

本期主题：削核辩论

- 中国核武器与多边核军控的前景
Frank G. Klotz 空军退休中将/高级研究员; Oliver Bloom 高级研究员
- 避险核威慑：储备核弹头还是建设快速响应核基础设施？
Dallas Boyd 高级研究员
- 重振联合作战环境下的核作战意识
Kelvin Mote 陆军中校
- 核威慑与网空互动概念初探
Stephen J. Cimbala 博士
- 陆军科曼奇人直升机项目对空军勒颈之结的启示
Michael W. Pietrucha 空军上校



本期导读

- 削核辩论 2

将帅视角

- 中国核武器与多边核军控的前景 4
Frank G. Klotz 空军退役中将 / 高级研究员; Oliver Bloom 高级研究员

军事变革

- 避险核威慑：储备核弹头还是建设快速响应核基础设施? 10
Dallas Boyd 高级研究员
- 重振联合作战环境下的核作战意识 23
Kelvin Mote 陆军中校
- 核威慑与网空互动概念初探 27
Stephen J. Cimbala 博士
- 从公共健康角度分析向太阳发射核废料的可行性 40
Murray R. Berkowitz 博士

作战研究

- 一个解释网空优势的概念模型 45
William D. Bryant 空军中校
- 虚空布兵：正确理解网空战争中的兵力集结和战斗力 56
John "Strider" Cobb 空军上尉

争鸣建言

- 走向中美网络关系共同安全平台 63
Panayotis A. Yannakogeorgos 博士 / 空军防务分析员
- 陆军科曼奇人直升机项目对空军勒颈之结的启示 72
Michael W. Pietrucha 空军上校
- 国防部的人员可靠性计划：皇帝的新衣 86
Jon Paul Mickle 空军中校

以史为鉴

- 正义事业锻造的友谊万古长青——纪念美国军事观察组访问延安七十周年 88
鲍世修，解放军退役大校 / 高级研究员（中国）
- 美国陆军航空队1946-47年在中国 94
Gordon K. Pickler 空军中校

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。



削核辩论

犹记得,《华尔街日报》在2007年1月突然发表基辛格、舒尔茨、佩里、纳恩合写的专栏文章“没有核武器的世界”。从此,这四位著名的冷战勇士华丽转身,站到无核世界运动的前列,不仅继续著文呼吁公众支持削核,更策划了可视中美俄2010年新战略武器削减条约之先声的纪录片《核倾点》(Nuclear Tipping Point)。然后,一如逻辑发展,正反阵营激烈辩论削减更多核弹头的可能性和可行性,其中,有关“多边核军控”和“多极核威慑”的讨论不绝于耳,有人甚至提出“战略海盗时代”已经来临。一言以蔽之,未来的削核谈判可能不再是两个超级核大国之间的“私事”。再者,先前几十年,冷战幸未酿成热战,一定程度上是热腾腾的核威慑帮助保持了冷冰冰的和平,许多专家相信核威慑的关键在于确保互相摧毁。但如今,多个国家开始大力发展冷战时代闻所未闻的网空攻击能力,如果这种攻击能力发展到可能破坏核作战体系中任何一个或多个环节,那么谁还敢确保互相摧毁或二次打击能力,甚至核安全本身?还有,美国维持核武库和核威慑所费不貲,在军费紧缩的大势之下,把威慑从实实在在的核弹头移建到“虚拟核武库”之上是否可行?有关新形势下削核的前景,本期发表几篇文章。

“多边核军控”意味着要求其他拥核国家加入削核谈判。“中国核武器与多边核军控的前景”一文指出,继新战略武器削减条约之后,美俄是否愿意继续推动削核谈判以及能再削减多少,在很大程度上取决于这两个核超级大国对中国核能力的认知。作者认为,鉴于中国刻意以“深藏不露”来实施核威慑,其“核能力和核原则的不确定性”使美俄两国政府难以达成进一步削核的意向,也难以获得各自政界和评论界广泛支持。因此继续削核和多边核军控仍然是一个遥远的前景。

“无武器威慑”或“虚拟核武库”(以及另一个相关概念“countervailing reconstitution”一指一个国家快速恢复核武器制造的复原重构能力)算不上最新理论,但在新战略武器削减条约签订之后成为削核辩论的焦点之一。“避险核威慑:储备核弹头还是建设快速响应核基础设施?”一文强烈批评弥漫在美国的一种以储存核武器快速制造能力取代维持现存核武库从而削减更多核弹头的思潮。作者把基于弹头的威慑和基于能力的威慑首先从形式上进行比较:弹头储备看得见摸得着,是实体存在;能力储备只是隐伏,属于虚构和假定。作者进一步警告:形式的区别和变更将带来颠覆性的后果:威慑基础动摇,延伸威慑失信,战略稳定倾斜。

“多极核威慑”正逐步形成,世界上拥核和有志拥核的国家确在增多,“战略海盗时代”的来临也许不全是危言耸听;更令人警觉的是,新拥核国更有可能轻率地跨过核门槛。“重振联合作战环境下的核作战意识”一文告诫美国国防部加强核作战意识教育,重新制定核作战准则,确保联合国部队做好准备,应对未来的多极核威慑挑战。

世界逐渐远离网空前核时代而进入网空核时代。在此背景下美俄通过新战略武器削减条约将各自部署弹头削减到1550枚,甚至有进一步削减到1000枚的可能。世界因此更安全了吗?“核威慑与网空互动概念初探”一文对此提出质疑。作者认为,网空武器将成为未来核常战争的第

一波先制打击武器，网空攻击能力和核攻击能力的同时并存更令人不安，且导致核危机管理更加脆弱。进一步，美欧反导和精确常规打击能力的发展威胁到对手对自身“最低威慑”的信心，从而可能破坏互相威慑下的平衡现状。因此，人们在建构网空核时代的威慑理论时，需要调整思维模式，把这些因素都考虑进去。

核科学带来核武器和核动力也带来核废料。人类目前可采用两种处置放射性核废料的办法：一是封存于地上/地下或葬入海洋深处（目前通行做法），二是送入太空。“从公共健康角度分析向太阳发射核废料的可行性”一文探讨把核废料射向太阳的利弊，认为这是经济可行的、公共健康风险最小的、一劳永逸根除隐患的最佳方案。

美军《国防部军语词典》对天空、陆地、海上、太空优势都给出定义，唯独缺失网空优势的定义，却又称全谱优势是“在陆、海、空、天领域及信息环境（包括网空）占据统治地位的累积效应”。那么，有所谓的网空优势吗，它与天空优势有哪些异同，它包含哪些特征和要素，攻防双方如何互动来构建或破解网空优势？“一个解释网空优势的概念模型”试图解决这些困惑。

网空攻击有针对性打击（如震网病毒攻击）和蔓延式打击（如分布式拒绝服务攻击）两大类，于前者，攻方可能需要集结大量人力物力；于后者，一小撮散兵游勇从世界各地出击就可能得手。那么防方在防守关键性大型网络和保护关键性小型系统方面，需要考虑哪些因素才能正确配置兵力？“虚空布兵：正确理解网空战争中的兵力集结和战斗力”一文就此提供看法。

如果说上篇文章仅从形式上对“震网病毒攻击”和“分布式拒绝服务攻击”加以区分的话，“走向中美网络关系共同安全平台”一文更从性质上对这两类攻击进行区别。作者认为，前者属于网络战争行为而后者属于网络犯罪行为，认清和认同这种区别对美中两国网络合作和共同安全具有重要意义。

美国空军尽管面临史无前例的预算紧缩，采购 1,763 架 F-35A 的决心坚定不移。该计划目前已进入初始生产阶段，100 多架 F-35 已经投用于训练和测试等用途。“就是 F-35，我们别无它选。”空军参谋长韦尔什将军的表述最简洁地说出空军的决心。然而时至今日，还有人敢“唱反调”。曾在本刊发表两篇力挺轻型作战飞机（见本刊 2011 年第 1 期“美国空军轻型攻击机未来十年想象”和 2013 年第 4 期“未来十年的新一代自主化轻型战斗机”）的同一作者，再次在本刊发表“陆军科曼奇人直升机项目对空军勒颈之结的启示”一文，批评 F-35 采购计划，认为该计划以应对假定的最高端威胁为唯一目标未免狭窄，空军应该组建以现有升级主战飞机和现代化轻型作战飞机构成的高/中/低搭配机群，才能成功应对更可能发生的各种强度和复杂度的全球威胁。

美中关系跌宕起伏，其实源远流长。值美国军事观察组访问延安七十周年之际，本刊发文两篇，其一“正义事业锻造的友谊万古长青”为中国学者撰写，作者从宏观视角回忆这段史实，缅怀曾为中美交往做出贡献的几位美国友人，希望两国人民珍惜战时情谊，继往开来。其二“美国陆军航空队 1946-47 年在中国”是一位美国空军军官 1973 年在本刊英文版发表的短文，作者选取了 1947 年美国空军帮助中共代表团撤离南京的一个历史片断，如实述史并配图。

《空天力量杂志》中文编辑姜国成



中国核武器与多边核军控的前景

China's Nuclear Weapons and the Prospects for Multilateral Arms Control*

弗兰克·克劳茨, 美国空军退休中将 / 对外关系委员会战略研究与军控高级研究员 (Lt Gen Frank G. Klotz, USAF, Retired, Senior Fellow for Strategic Studies and Arms Control Council on Foreign Relations)

奥利弗·布鲁姆, 对外关系委员会战略研究与军控高级研究员 (Oliver Bloom, Senior Fellow for Strategic Studies and Arms Control Council on Foreign Relations)

过去 40 多年里, 美国和俄罗斯就限制和削减各自核武库一直在举行谈判。2010 年成功签署的《新战略武器削减条约》(New START) 标志着这一进程取得最新进展, 用奥巴马总统的话说, 为更大的削减奠定了基础。¹ 在 2013 年 6 月的讲话中, 奥巴马实际上重申了他寻求进一步与俄罗斯磋商削减核武器的意图。

其它已宣布拥有核武器的国家——中国、法国、印度、巴基斯坦和英国——到目前为止没有在此削核谈判进程中发挥直接作用。因为美国和俄罗斯拥有最大和最多样化的核武库, 囊括了全世界核武器的将近 90%, 其它国家的有限核能力迄今对两个核超级大国之间的总体战略平衡和稳定概念影响极小。

然而, 这种情况可能会改变。如果美国和俄罗斯在未来几年中确实继续大规模削减核武器数量, 其它五个国家核能力的相对比例可能大大提高。这样的发展将产生两个方面的重大影响。首先, 人们会质疑: 最初在双边和冷战环境中发展起来的核威慑理论, 将如何适用于几个国家持有“数百枚”核武器的国际体系? 再者, 它意味着, 其它拥核国的核武库可能成为美俄间未来任何削核谈判中的一个重要因素。

美俄两国官员已经承认, 他们将最终需要以某种形式或方法解决其它国家的拥核问题。例如在美国, 国会授权研究美国战略态势的两党委员会于 2009 年提出: “为支持美国军备控制利益和更广泛的战略稳定利益, 美国应寻求一系列更广泛和更远大目标的战略对话, 不仅仅与俄罗斯, 而且还包括与中国, 以及美国在欧洲和亚洲的盟国的对话。”² 此外, 在批准《新战略武器削减条约》时, 美国参议院呼吁“其它拥核国家认真、尽早考虑相应削减自己的核武库”。³

俄罗斯方面在过去, 包括在促成 1972 年《削减战略核武器条约》(SALT I) 的早期谈判过程中, 已经提出了所谓第三国核力量的问题。⁴ 最近, 外交部副部长谢尔盖·里亚布科夫 2012 年 11 月 8 日在莫斯科告诉一次国际会议的与会者们说: “核军备裁减和限制领域的进一步措施必须是多边的。”⁵ 他的评论也显示, 美国和俄罗斯对在任何正式谈判中吸纳其它拥核国参与的时机可能有所分歧。华盛顿官员似乎认为, 两个核大国应再进行自身新一轮的削减。而莫斯科官员显然更愿意尽早将其它国家包括进来。

即使美国和俄罗斯最终在时机问题上达成共识, 其它拥核国家是否、并在多大程度

* Translated and reprinted with permission from Strategic Studies Quarterly, Winter 2013, Vol. 7, No. 4.

上已经准备好加入有关战略稳定的谈判，并且最终可能削减各自的核武库，这些问题仍然有待观察。人们可以想象，各拥核国有自己的政策，对自身国家安全的需要的认识亦不同，故而对以上问题的答案将各说各话，不可能一样。

中国核力量的不确定性

在美国和俄罗斯对未来威慑需求的评估中，以及对进一步削核之明智性的考量中，最担心的国家是中国。虽说这两个大国的核武器储存使中国相形见绌，但是中国仍拥有不容小觑且不断增长的核武库。进一步，美国和俄罗斯——出于非常不同的原因——都把中国看成是战略竞争对手，并且是对地区重要安全利益的潜在威胁。因此，无论是华盛顿还是莫斯科，都不喜欢看到中国在核武器方面与之平起平坐。显然，这两个国家都有意避免将自家的核武库削减到中国目前的水平，也不愿削减到中国通过继续发展甚至加速扩充自身能力最终能够达到的水平。

在评估以上任一种结果的可能性时，最主要的障碍是中国核力量的当前规模和计划规模的巨大不确定性。中国一向表示，它只需要足够的核武器来阻止核攻击和对抗核胁迫。根据中国的政策文件，此目标并不需要中国在武器方面与核大国对等。的确，中国已多次表示无意与其它国家进行核军备竞赛。按照泰勒·弗莱瓦尔和伊万·埃罗斯(Taylor Fravel and Evan Medeiros)的观点，中国的核准则似乎是遵循“确保报复”原则，据此，“保存少量的可生存武器，足以在报复攻击中施以不可承受的伤害，从而遏制核侵略。”⁶

中国目前核武库的规模乍看之下似乎与这种解释相一致。2013年五角大楼向国会提

交的中国军事能力报告估计，其陆基核能力由50-75枚井下发射和公路机动发射型洲际弹道导弹组成。报告还指出，中国“有可能继续投入大量的资源以维持有限、但是可生存的核力量……，以确保中国人民解放军能够实施具破坏性的报复核打击。根据该报告，为此，中国很有可能增加其移动式洲际弹道导弹的数量、开始其配置JL-2海上发射弹道导弹的晋级潜艇作战巡逻，并且开发针对美国和其它国家弹道导弹防御系统的对策。”⁷五角大楼的评估并没有提供中国核弹头实际储存规模的数据。然而，非政府分析师汉斯·克里斯丁森和罗伯特·诺里斯(Hans Kristensen and Robert Norris)估计，中国目前拥有大约250枚核弹头的总库存。⁸

不是所有人都同意这些数字。比如，俄罗斯专家阿列克谢·阿尔巴托夫和弗拉基米尔·德沃尔金(Alexei Arbatov and Vladimir Dvorkin)就断言：“国际社会明显低估了中国的核能力。”他们指出，一些俄罗斯专家估计中国当前核武器库存中，有800-900枚可快速部署，并且可能有相同数目的核武器用于储备，或者等待拆除。他们还援引外国的新闻报道，称中国庞大的地道系统可以用于存储大量的军事装备，包括核武器。⁹

关于“不首先使用”的辩论

除了对中国核力量当前和未来规模的疑问之外，另一个不确定因素涉及中国奉行的核原则。2013年早些时候，中国政府公布了最新版国防白皮书。不出所料，这份新文件着重阐述了北京直接关切的领域，其中包括广为宣传的美国亚太地区“再平衡”战略，以及该地区越来越可能失控的海洋争端。¹⁰尽管白皮书没有详细阐述中国的核武器政策，但是对这个主题的表达——或者更确切地说，

其中未言之处——立刻引起西方观察家的关注和反应。

中国自1964年首次成功试验核武器以来，一直公开宣称永远不对任何拥核国首先使用核武器，并且承诺永远不会向任何非拥核国或者无核区使用或者威胁使用核武器。这个所谓“不首先使用”的承诺已成为中国官方几乎所有关于核政策宣告的中一道必备菜。此外，中国官员经常批评美国和俄罗斯从未明确宣布不首先使用核武器的政策，并且指控这两国保持“核战”态势，包括实施第一次打击的能力。

然而值得注意的是，最新的中国国防白皮书中没有明确提及“不首先使用”政策。在《纽约时报》的评论专栏中，设在华盛顿的卡内基国际和平基金会的詹姆斯·阿克顿（James Acton）大胆设想，这一遗漏可能反映了中国宣称了50年之久的政策出现改变。他提出，北京经常提及的关于美国导弹防御系统和常规精确攻击武器项目对中国核报复部队构成潜在威胁的担心，可能会导致中国国防界重新思考不首先使用核武器的长期承诺。¹¹事实上，好几个学者认为，延着这种思路的内部辩论的确在2000年代中期的中国就已发生。¹²

其他研究者立刻挑战阿克顿的结论。或许最有趣的回应来自中国军事科学院的姚云竹少将撰写的一篇评论；姚云竹是广为人知的中国核政策官方发言人。¹³她驳斥阿克顿的结论，认为此白皮书与过去语言的偏离不是源于政策的改变，而是源于文件形式的改变。事实上，最新版本的标题不同，而且结构也和以前的六个版本（2000 - 2010年）不同。更重要的是，姚云竹辩称，最新白皮书中关于核政策的寥寥数语，与不首先使用核

武器原则是一致的；而且最近中国领导人在其它场合——包括2012年4月首尔核安全峰会——上所发表的言论，证实它继续是中国的官方政策。

这场辩论的双方都各抒己见。最新白皮书中关于中国核原则的语言大部分看上去是从较早版本，特别是2008年版本，照抄下来的。不过，阿克顿的质疑有其道理，他发问，既然最新文件照抄老文字，为什么却要剔除以往版本中明确提及的中国不首先使用核武器政策的文字。反过来说，姚云竹说的也对，她列举了中国最近多次承诺不首先使用核武器的例子，使那些怀疑中国政府突然和间接放弃其50年承诺的言论难以立足。

不管真相如何，这场辩论突显了美俄两国核相关部门对中国长远核计划的挥之不去的怀疑。如果中国的确因为担心美国常规军事能力的优势而重新考虑其不首先使用核武器的政策，它也就有可能思考其核力量向另一种方向，一种非常不同于其所宣称的只确保二次打击报复能力的方向发展。

多边核军控的前景

中国核能力和核原则的不确定性，对两个最大核强国未来军备控制措施有影响。除非美国和俄罗斯对中国核武库的现状和发展趋势更为确定，否则这两国的批评家们将会抵制进一步削减核武器，这三个国家之间的战略稳定仍将是值得关注的领域。

美国和俄罗斯专家多次呼吁，中国应该对其当前核能力和未来意图更加开放。同样，其他人则建议，中国应与法国和英国一道，自愿加入美国和俄罗斯的努力，按照《新战略武器削减条约》规定的方式，披露其战略

核力量的信息，作为加强透明度和建立信任的第一步。¹⁴

然而，中国历来不愿意讨论其核力量规模和特性，声称保密性是确保其相对较小报复性力量生存能力的关键。正如姚少将所说，“中国更多地依赖于不确定性——而不是确定性和透明度——来实施威慑……一定程度的不透明是中国不首先使用核武器政策的组成部分。”¹⁵ 因此，中国在短期内似乎不太可能同意以单方面披露或者多边合作的做法，透露更多的信息。

同样，中国目前不会有任何兴趣参与如何限制或削减其核武器的更正式的讨论。虽然中国官方声明展望了今后削减核武器的多边谈判，他们是附加了特定的先决条件的。例如，早期的国防白皮书（2010年）指出：“拥有最大核武库的国家对核裁军负有特殊和优先责任，应继续大幅削减其核武库，……为最终实现全面彻底核裁军创造必要条件。”并且，在全面彻底核裁军之前，“所有核武器国家应放弃以首先使用核武器为基础的核威慑政策”。¹⁶ 因为满足这些条件之中任何一条的可能性不大，中国参与削减核武器或战略稳定正式对话的前景（无论是双边或多边）目前似乎同样是遥不可及的。

一些令人鼓舞的迹象…

尽管如此，有迹象表明，面对其它国家要求中国对其核能力和政策更加公开化的压力，中国认为有必要至少以有限的方式作出反应。过去几年来，在美国国家科学院、战略与国际研究中心（CSIS）太平洋论坛、海军研究生院、卡内基基金会和其它非政府组织发起的几次“第二轨道”对话上，来自美中两国的前政府官员、技术专家，以及学者

已经见过面。虽然这些是非官方场合，但是它们在促进国家间更好地了解各自立场方面发挥了有益的作用，这反过来也使政策制定者更好地了解情况。例如，美国国际安全与军控委员会和中国军控科学家小组在2008年联合编制了一份英汉核安全词汇表。¹⁷ 这项活动期间开诚布公的讨论，进一步阐明了美中两国关于核威慑理论和实践基本概念看法的相似之处；在某些情况下也是阐明了两者之间的真正差异。

除了“第二轨道”的积极努力之外，在过去的两年间，正式访问和军方交流的次数显著上升。例如，2013年9月，马克·威尔什将军成为过去15年内首位访问中国的美国空军参谋长。¹⁸ 中国的官方代表还参加了一些高规格的核政策和军控主题国际会议，包括美国战略司令部首届威慑专题讨论会，以及2013年卡内基国际核政策会议。

再者，中国对在多边核军控讨论中扮演更加可见和建设性的角色，似乎显示出了更大的兴趣。2012年，中国同意领导一个联合国安理会五常任理事国（P5）工作组开发术语表，以便五常任理事国进一步就核问题展开讨论。¹⁹ 另在2013年8月，中国政府终于同意向设在维也纳的“全面禁止核试验条约组织”国际数据中心提供来自其监测站的有限数据——尽管中国尚未批准该条约。²⁰

…但远非理想

虽然这些都是令人鼓舞的发展，但是相比而言中国在其核能力和原则方面仍然不够透明。只要这种状态保持如此，那么美俄两国将继续对中国核计划的现状保持怀疑，对其未来方向更疑虑重重。因此，在这两个国家，

要想推动对各自核武库更大幅度削减的政治支持，都将难以做到。

同样，与中国展开关于战略稳定和核军备控制的正式谈判，这种可能性将遥遥无期，无论美俄两国政治家希望达成什么样的终局。问题是，中国不仅宣称只有在两个超级核大国把核武器削减到远远更低的水平之后，中国才会考虑参与多边核军备控制讨论；而且中国所采用的深藏不露的做法，将对有意义的会谈构成巨大障碍。美国和俄罗斯经过多年的实际交往，认识到，这一进程需要相

当程度的信息共享和透明度，无论是在谈判阶段还是在协议的实际执行中。中国显然没有准备好接受这样的做法。因此，如果核武器还会有更多削减，大概这些削减也只会发生在华盛顿和莫斯科新一轮双边谈判的框架之中。

而在目前，我们最多能期待的，就是中国以其更明显的意愿参与正式对话和军事交流，最终促使其核能力及原则更加开放和公开。但这远远不够，其它拥核国家应利用一切机会，提醒中国意识到这一事实。♣

注释：

1. White House Office of the Press Secretary, "Remarks by President Obama and President Medvedev of Russia at New START Treaty Signing Ceremony and Press Conference" [奥巴马总统和俄罗斯总统梅德韦杰夫在NewSTART条约签约仪式暨新闻发布会上的讲话], Prague, Czech Republic, 8 April 2010.
2. William J. Perry and James R. Schlesinger, *America's Strategic Posture: Final Report of the Congressional Commission on the Strategic Posture of the United States* [美国的战略态势：国会关于美国战略态势委员会的最终报告], (Washington: US Institute for Peace Press, 2009), xviii-xix.
3. US Department of State (DoS), "New START Treaty: Resolution of Advice and Consent to Ratification" [New START条约：意见决议和同意批准], 22 December 2010, <http://www.state.gov/t/avc/rls/153910.htm>.
4. DoS, *Foreign Relations of the United States*, [美国外交关系], 1969-1976, vol. 32, SALT I, 1969-1972, doc. 14, 3; *Ibid.*, vol. 14, Soviet Union, October 1971-May 1972, doc. 267, 1038, fn.3.
5. "Moscow Insists on Making Nuclear Arms Reduction Multilateral—DFM Sergei Ryabkov" [莫斯科坚持核裁军多边化——外交部副部长谢尔盖·里亚布科夫], ITAR-TASS, 8 November 2012.
6. M. Taylor Fravel and Evan Medeiros, "China's Search for Assured Retaliation: The Evolution of Chinese Nuclear Strategy and Force Structure" [中国寻求确保报复能力：中国核战略与力量结构的演变], *International Security*, 35, no. 2 (Fall 2010): 63. 有关中国思维演变的其它分析，参见江忆恩 (Alastair Iain Johnston), "Chinas New 'Old Thinking': The Concept of Limited Deterrent" [中国的新“旧思维”：有限阻遏概念], *International Security*, 20, no. 3 (Winter 1995/96): 5-42; 另参看 John W. Lewis and Xue Litai, "Making China's Nuclear War Plan" [制定中国的核战争计划], *Bulletin of the Atomic Scientists*, 68, no. 5 (2012); 另参看 Elbridge Colby and Abraham Denmark, co-chairs, *Nuclear Weapons and U.S.-China Relations: A Way Forward* [核武器与美中关系：未来方向], (Washington: Center for Strategic and International Studies, 2013).
7. DoD, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* [涉华军事与安全发展 2013 年报告], (Washington, DoD, 6 May 2013), 30-32.
8. Hans M. Kristensen and Robert S. Norris, "Global Nuclear Weapons Inventories, 1945-2013" [全球核武器库存，1945-2013], *Bulletin of the Atomic Scientists*, 65, no. 5 (2013): 79-80.
9. Alexei Arbatov and Vladimir Dvorkin, *The Great Strategic Triangle* [大战略三角], (Moscow: Carnegie Moscow Center, 2013), 10-11.
10. Information Office of the State Council of the People's Republic of China, "The Diversified Employment of China's Armed Forces" [中国武装力量的多样化运用], 16 April 2013.

11. James M. Acton, "Is China Changing Its Position on Nuclear Weapons?" [中国在改变其核武器立场吗?], *New York Times*, 18 April 2013. For an expanded discussion of China's concerns about conventional prompt global strike, see Acton, *Silver Bullet? Asking the Right Questions About Conventional Prompt Global Strike* [有关中国对常规快速全球打击关切的更多讨论, 请参看 James M. Acton, *Silver Bullet? Asking the Right Questions About Conventional Prompt Global Strike* [精准银弹? 就常规快速全球打击提出正确的问题], (Washington: Carnegie Endowment for International Peace, 2013).
12. Rong Yu and Peng Guangqian, "Nuclear No-First-Use Revisited" [再谈不首先使用核武器], *China Security* 1, no. 1 (Winter 2009): 85-86.
13. Yao Yunzhu, "China Will Not Change Its Nuclear Policy" [中国不会改变其核政策], *China-US Focus*, 22 April 2013; 另参看 M. Taylor Fravel, "China Has Not (Yet) Changed Its Position on Nuclear Weapons" [中国(还)没有改变其核武器立场], *Diplomat*, 22 April 2013; 另参看 Rachel Oswald, "China's New Defense Paper Causes Stir over No-First-Use Nuke Policy" [中国新国防白皮书引发对“不首先使用”核政策的热议], *Global Security Newswire*, 24 April 2013.
14. 例如, 可参看 Tamara Patton, Pavel Podvig, and Phillip Schell, *A New START Model for Transparency in Nuclear Disarmament* [核裁军透明化的 New START 模型], (Geneva: United Nations Institute for Disarmament Research, 2013), 12.
15. Remarks by Yao Yunzhu at the 2013 Carnegie International Nuclear Policy Conference [姚云竹在 2013 年卡内基国际核政策会议上的发言], Washington, DC, 8 April 2013.
16. Information Office of the State Council of the People's Republic of China, "China's National Defense in 2010" [2010 年中国的国防], 31 March 2011, 6.
17. National Research Council, *English-Chinese, Chinese-English Nuclear Security Glossary* [英汉、汉英核安全术语表], (Washington: National Academies Press, 2008).
18. "CSAF Begins Counterpart Visit in China" [空军参谋长开始在中国对口访问], *Air Force News Service*, 25 September 2013.
19. DoS, "Third P5 Conference: Implementing the NPT" [第三次安理会五常会议: 执行不扩散条约], 29 June 2012.
20. "China's Foreign Minister Wang Yi Reaffirms Commitment to the Comprehensive Nuclear-Test-Ban Treaty (CTBT): Progress on CTBTO Stations in China" [中国外长王毅重申对全面禁止核试验条约的承诺: 全面禁止核试验条约组织工作站在中国的进展], *CTBTO Preparatory Commission Press Release*, 17 August 2013.



避险核威慑：储备核弹头还是建设快速响应核基础设施？

Hedging Nuclear Deterrence: Reserve Warheads or a Responsive Infrastructure? *

达拉斯·博伊德，高级研究员（Dallas Boyd, senior policy analyst for Leidos [formerly SAIC]）

除非发生重大的全球动荡，美国安全政策自“后冷战”以来不再强调核武器，这种趋势将延续到可预见的未来。从美国的宣示性政策中我们看到，核武器的作用将进一步受限，更多的核弹头削减亦可能发生，把《新战略武器削减条约》所设的限量降至新低。¹ 尤其是，奥巴马总统表达了自己的意图，总统不仅要削减已部署战略武器、还要削减非部署储备核弹头。²

把这些储备武器作为未来的削减目标，将对美国的“避险”战略产生重大影响。当前的避险战略反映了美国的信念，这就是，美国必须拥有精密设计的强大保险，无论核武器储备发生技术问题或者地缘政治突发不利局面，美国都能安然无恙。如今，美国继续采用避防核武器技术出错或者地缘政治突发事件的原始手段，即能在相对较短时间内向运载系统添加或者“上载”大量的储备核弹头。³ 奥巴马总统意图对储备核力量进行砍削，是基于对另一种替代避险模式的信心，这种模式称为“快速响应核基础设施”，在此建议模式中，美国以核武器集成能力来替代当前的核弹头大量储备模式。⁴

“快速响应核基础设施”的概念最初出现在小布什政府时期的《2002年核态势审查报

告》中，担当核威慑“新三角”的一部分。在此概念之下，由陆-海-空发射核武器组成的老三角或传统三位一体核战略被统称为“进攻性打击系统”，仅仅作为新三角的一条腿；其它两条腿分别是“主动和被动防御”，以及“振兴防御基础设施”，这最后一条腿的主要部分就是具备快速响应能力的核武器部门。⁵ 虽然这个新三角模式后来被抛弃，但是对快速响应核基础设施的提及持续不断。在奥巴马政府的《2010年核态势审查报告》中，这个概念被描述为：“对关键基础设施加以恢复和现代化以后，将允许美国逐步偏离以保持大量非部署核弹头作为技术避险的策略，长久以往将允许美国进一步削减其非部署核武器库存。”⁶

根据这一设想，美国核威慑的终极后盾将是国家的科研能力、国家实验室等基础设施，以及核弹头生产能力，而不是真实的核弹头储备。然而，这种假定比《核态势审查报告》所用的平淡语言更有争议。首先，这种模式如何运作显得非常模糊。快速响应核基础设施的概念大致被理解为：一种能够对不可预见的技术问题或政治事件作出迅速反应的核武器集成能力；至于该核武器集成能力能提供哪些具体的能力，以及提供这诸般能力的时间框架，都语焉不详，含糊带过。

* Translated and reprinted with permission from Strategic Studies Quarterly, Summer 2014, Vol. 8, No. 2.

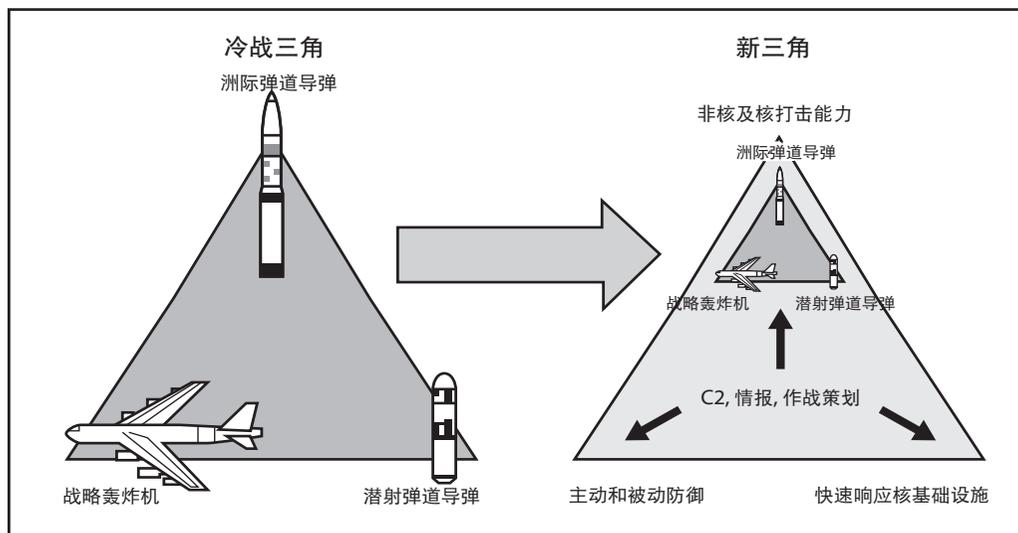


图 1:《2002 年核态势审查报告》提出,“新三角”的一条腿将由“快速响应核基础设施”组成(取自: Air Force Doctrine Document 2-12, Nuclear Operations [空军作战准则 AFDD 2-12:核作战], 7 May 2009, 6.)

概念上的含糊已然令人不安,更深层的担忧,是当我们把“快速响应”作为核武器集成能力之一项组织原则而追求时,我们需要付出多大的机会成本。即便我们能大幅提升响应速度,但是实现这一能力所需的投资,可能迫使我们牺牲更重要的能力——例如,维护美国已部署核弹头的能力。而已部署的核弹头与假设中的快速响应核基础设施所带来的收益有明显不同,这就是,前者对威慑的贡献没有疑问,但后者根本无法消除人们的疑虑,而且这种所谓的集成能力可迅速扭转过去二十年核弹头削减的推断更是难圆自说。构建这种能力在于迎合一种纯假设的需要——例如,迅速重整军备,或者快速研发新弹头——而置其他需要依靠该集成能力的数项现存要求于不顾。的确,本届政府核日程表中的其它事项,从拆解退役弹头到打击核恐怖主义,都依赖于已不堪重负的核基础设施。在目前的预算环境下,大量投资于核基础设施建设几乎不可能,如果再对快速响

应能力进行投入,势必占用对其它使命的预算。

除了上述这些实际的考虑之外,快速响应核基础设施构想还基于另一个更深层的想法,这就是以隐伏的核技术能力储备替代已建成的核武器。这种深层思路极具争议,也是在过去几十年间呼吁裁军的主要支撑观点。但是这种模式对战略稳定的冲击,一直令人深切担忧,特别是当拥核国之间关系破裂时。例如,如果一个国家随着对立升温开始重构其核储备力量,其对手可能会采取对等措施,从而使安全环境更加恶化,而不是改善。至于当前美国政府如何应对这些担忧,我们无从知晓,因为有关建设快速响应核基础设施的蓝图从来没有连贯展现出来。

此外,依靠所谓隐伏能力来体现核威慑的思路,可能有朝一日会从对目前核储备力量的压缩向外蔓延,进一步成为削减已部署部队的理由,因此,我们必须认真审察这种

思路的潜在缺陷。担任核生化武器防御规划助理国防部长的安德鲁·韦伯（Andrew Weber），曾在2013年重申了基础设施投资和核弹头削减之间的联系，但是没有对储备武器和已部署武器做出区分。他作证说：“快速响应核基础设施，将使我们能以规模远小于当前的武器储备，为美国解决武器储备中的技术问题，并应对未来地缘政治的负面挑战。”⁷

虽然一些官员坚持认为对核基础设施投资能够促成武器储存的大规模削减，但是这种思路并没有经过任何严密分析，也无历史案例可资借鉴。在国家威慑战略还没有开始这番根本性转变之前，提出这样一种选项，或能激发起坚定信念。不过奇怪的是，核政策观察人士居然没有把批判分析矛头指向这种构想，而让其倡导者逍遥于指责之外，这样的轻易过关，在核武器政策辩论场上也算绝无仅有。然而，预算压力之下，人们终究越来越强烈要求核武器集成能力模式必须具体列举其一系列功能，证明这些功能的确经过严格论证，而容不得敷衍了事或含混的使命陈述。因此，对快速响应核基础设施的概念，应予彻底的重新审察，对其追求的未来核弹头削减的前提条件，也应加以同样的关注。这个审察过程的第一步，应该是辨明这种核武器集成能力能具备哪些具体功能，并确定这些功能对核威慑是否真正至关重要。

“快速响应”的定义前后矛盾

在早期鼓吹快速响应核基础设施构想的人中，时任国家核安全管理局局长的林顿·布鲁克斯（Linton Brooks）将“快速响应”定义为“一种确保我们的核武器体系能应对意外事件或新现威胁的生存韧性，一种使我们能预见对手的创新并及时加以反制以防自身威

慑被降格的能力。”⁸ 时任国家核安全局官员的约翰·哈维（John Harvey）则解释得更具体些，他至少列出了快速响应核基础设施的可辨识要素，包括一支训练和管理有素的队伍，获得加强的科研基础，高效的、现代化的、“规模适中”的制造设施，获得改进的经营做法，以及检验主要能力的频繁的“端至端”的演练。⁹ 然而，这些要素和核武器集成能力的具体产出之间有什么关联，却难以捉摸，而且其后续的表述更加令人困惑。¹⁰ 例如，国家核安全局提出重新配置核集成的综合计划——“核武器集成能力2030”时，将快速响应能力定义为“了解需求，并且有能力以一整套明确的能力与实力满足这些需求。”¹¹

应该指出，这些描述并不是对同一个主题的不同描述，而是对未来核武器集成能力概念的一堆杂乱无章的不连贯的远景期待。此外，凡为实现这些要求设定的具体期限，都看上去缺乏严谨的论证。例如，在以量化方式确定需求的为数不多的几次尝试中，有一次，布鲁克斯列出了一组几乎不能算作快速响应的功能和相应的时间框架，如下：¹²

- **修复储备问题（1年）。**核武器集成能力依赖于严格的武器储备管理程序，以评估武器中的问题，并寻求修复的办法。为此进程设立典型的时间间隔是很困难的，因为大多数情况下，已得到解决的储备问题仍然属于机密。然而，有理由相信这一进程需要的时间远不止一年，何况识别储备问题并且找到解决方案也许只是整个进程中费时最少的一步。再者，我们还要对部署在洲际弹道导弹、潜艇和轰炸机中的大量核弹头进行维护，它们分布在不同的地理位置，后勤需求巨大，需要相当长的时间才能完成。

- **改装武器（18个月）。**按新使命或变动使命需要改造旧武器，例如改变其爆炸特点，这个进程所需时间很可能超出时间表。不妨回顾在B61-7型弹头的基础上研发B61-11改进型钻地弹头的案例，这项开发在1990年代中期花费了接近两年的时间。¹³需注意，这项努力是发生在冷战结束之后不久，当时的核武器集成能力远比现在坚实得多。再看看最近的“弹头延寿项目”的进度，就可知道，核武器集成能力将很难在预算内按时完成正在进行的工作（例如B61和W78/W88-1弹头的延寿），更遑论承接新的重大挑战。¹⁴

- **设计、开发和生产一种新弹头（3-4年）。**及时生产新核弹头，包括完成全面联合核武器寿期的程序，是国家安全长期以来的一项必需能力。¹⁵正如劳伦斯利弗莫尔国家实验室的一项研究早在1987年指出：“为了避免新科技带来的措手不及，我们必须保持开发新[武器]的能力，以应对我们对手的新发展。”¹⁶但是，开发新武器所必需的速度，仍然模糊不清。三到四年的时间目标，表明了自冷战时代以来响应能力的急剧下降。1945年至1992年期间，美国生产了超过65种不同类型的弹头，平均每九个月推出一项新设计。¹⁷尽管如今生产一种新武器所需的时间不清楚，但是肯定要以年计。根据全国研究委员会2012年的研究，“开发具有新军事特色的武器将花费远远长于24-36个月的时间。”¹⁸最近为W88核弹头所开展的裂变核生产的过程，似乎加强了这项评估。第一个W88钚核替换件是2006年才通过验证的，花费了足足11年的努力。¹⁹2000年代中期的“可靠替换弹头”即RRW计划也表明，开发期相当

漫长，仅项目的设计阶段就消耗了大约10个月时间。²⁰

- **保持地下核试验就绪状态（18个月）。**从当前的地下核试验就绪状态来看，美国需要两至三年才能着手这种试验。²¹即使把这个时间大幅度缩短，一旦真出现要求迅速响应的情形——一种情形是平时修复核储备问题，另一种情形是全球安全环境突变——这样的就绪状态也难有作为。于前者，对地下核试验的禁令使我们不可能进行这类试验来验证储备武器；于后者，如果全球形势的突变严重到我们必须置禁令于不顾，那么这样的突变一定是快得迫使我们根本无法考虑用试验来验证储备武器的有效性。

关于快速响应核基础设施，还有两项附加能力已被列出但并没有指定时限：一个是批量生产新核弹头的能力，再一个是增强核力量的能力。

- **新弹头的批量生产。**在快速响应核设施概念下，批量生产新核弹头的能力，类似于一种被称为“基于生产能力的威慑”或“无武器威慑”的模式。在这个概念之下，国家能够以核武器的生产能力，而不是依靠维持现成的武器储备，来展示威慑。约瑟夫·C·马茨（Joseph C. Martz）是洛斯阿拉莫斯国家实验室的核材料科学家，根据他的说法，就基于生产能力的核威慑而言，实质问题在于“时机（灵活性）和能力。”他提出：“目前就这些问题没有达成任何共识，至于武器或其组成部分在一旦需要而重建需要“多快”和“多少”这样的问题，也没有现成的答案。”²²此外，即使已经知道这些数量，美国仍然严重缺乏生产新核弹头的能力。美国战略司令部前司令理查

德·梅斯海军上将 (ADM Richard Mies) 在 2012 年一篇关于二十一世纪威慑的论文中指出：与俄罗斯相比，美国“在过去二十年已经几乎没有生产弹头的能力，也几乎没有在未来十年间开发出坚实生产能力的可能。”这种能力的缺乏导致梅斯得出结论：“快速响应核基础设施的承诺基本上未能兑现。”²³

批量生产新核弹头能力的核心问题，是钚裂变核的制造能力。自洛基弗拉茨工厂于 1989 年关闭，美国失去这种大规模生产能力已将近二十年。从 2007 年开始，国家核安全局再次开始生产钚核，用以替代在测查过程中被毁掉的部分，洛斯阿拉莫斯国家实验室每年为 W88 弹头生产大约 10 个钚核。²⁴ 提高钚核的生产率应该是基础设施现代化的关键因素——能源部/国防部对钚核生产的长期需求是，每年生产 50-80 个新制的钚核。然而，鉴于洛斯阿拉莫斯国家实验室中化学和冶金研究更换核设施项目的推迟，国家核安全局在今后五年内如有能力每年制造 20 个钚核就谢天谢地了。²⁵ 为弥补钚核生产能力的下降，各种选项正在探索之中，其中包括在未来的“弹头延寿项目”中重新使用储备的钚核。然而，这些都是权宜之计，并非快速响应核基础设施模式所设想的能力。

- **增强核部队。**美国官员经常夸大避险储备弹头安装到已部署核发射装置上的速度，比如前国防部长威廉·佩里在作证时说：美国有“向我们的战略部队迅速安装数以千计的核弹头的的能力，如果国家决定这样做的话。”²⁶ 美国战略态势委员会也做过类似暗示：“在国际局势迅速恶化的情况下，非部署武器储备可以迅速安装就绪。”²⁷ 但在现实中，由于后勤方面的各种限制（例如，

执行此安装任务所需的合格人员、车辆和设备数量有限），避险储备弹头能否迅速安装上架，对发展速度以数周或数月计的国际危机能否产生有意义的影响，实在值得怀疑。²⁸

无论不可预见的事件是技术性的或地缘政治性的，即使核基础设施得到大幅增强，也未必能够及时做出响应，从历史借鉴中，我们很难想象这种及时响应的可能性。前面提到的布鲁克斯说过：如果美国能够“以地缘政治威胁可能出现的时间表”生产出新的核弹头，美国就能够更多地削减核储备。²⁹ 这一论断与《核态势审查报告》一致；该政策文件指出：将把“飙升式生产”能力落实到位，以应对“重大地缘政治的‘意外’。”³⁰ 然而，具有世界历史意义的危机可能以惊人的速度展现，二十世纪发生的许多事件就是证明。举例来说，纳粹德国和苏联从 1939 年签订互不侵犯条约并联合肢解波兰，到两国之间全面爆发战争，这种过渡只用了 20 个月的时间。对于持续笼罩在低等级敌意状态下的国家，比如冷战时期的美国和苏联，关系的恶化可能远更迅速。

古巴导弹危机也是验证这种现象的适当案例。美国从 1962 年 8 月开始怀疑苏联在古巴建设弹道导弹基地，此后于 10 月 14 日第一次从空中拍摄到这些基地的图像。仅仅一星期后，肯尼迪总统公布了这一发现，并且明确表示该事件可能引发核战争。依此类推，美国只要发现其潜在敌人正在秘密囤积核武器，这个发现就会成为美国必须激增核能力的最明显的理由。但是眼下，美国只有极早获得此类情报才能这样做，因为需要太多的时间才能建成充分响应的能力。

对依靠快速响应核基础设施来响应地缘政治突发事件的另一担忧，是种种不确定性对决策的影响。前面提到“快速响应”的定义，它强调的是“一种使我们能预见对手的创新并及时加以反制以防自身威慑被降格的能力。”此说法想当然地以为，所谓的地缘政治事件总是明确无疑的。然而，历史告诉我们，政府的任何一个部门，都可能在评估外国威胁上产生重大分歧，何况一个庞大的官僚政府。³¹ 我们需要多大程度的确定性，才能同意启动核武器集成能力来开始做出昂贵的、甚至可能破坏国家稳定的响应？是绝对肯定还是几乎肯定，抑或只要合理怀疑？以冷战为先例，那时候的“最坏情况规划”似乎在暗示以后者为准。但如果这次的响应决策证明是虚惊一场，虚惊后的政府领导人可能走向两个极端，要么再不肯重新松弛战备，要么比先前松弛得更厉害。

然而，即使地缘政治事件不存在含混，即使核武器集成能力的响应速度得到大幅度改进，我们仍然有大量的理由质疑这种模式的依据。其中最主要的质疑是，一个部分基于隐伏技术储备能力的威慑模型，能否像完全由真实弹头组成的核武库那样提供战略稳定性。

与“无武器威慑”理论的相似之处及其缺陷

“无武器威慑”概念一直是核裁军运动的理论核心，历经了不止一代人的时间。这一概念也称为“复原重构”和“虚拟核武库”。此概念认为，一个国家或许能够以快速生产核武器的隐伏储备能力来威慑对手，而不一定需要拥有已构建的“现存武库”。想起一位鼓吹者的名言：目前这种“导弹威慑导弹、轰炸机威慑轰炸机、潜艇威慑潜艇”的模式，

将被一种“工厂威慑工厂、蓝图威慑蓝图，方程威慑方程”的模式所取代。³²

谈到“无武器威慑”从1980年代到目前的理论沿袭，马茨认为：“为支持‘全球零核’愿景，[2010年核态势审查报告]接受了这样的观念：核力量的复原重构能力可以在核储备削减环境下成为核威慑中更大的一部分。”³³ 虽然这份核态势审查报告没有明确提到基于储备能力的威慑，这个已经存在几十年的旧概念与政府的快速响应核基础设施构想仍有明显的类似。这两种模式都企图用基于基础设施的能力取代真实存在的弹头，只是程度有别而已。³⁴ 两者之间的明显区别是，在“无武器威慑”概念中，核武器集成能力代表一个国家战略威慑的整体，而在奥巴马政府的愿景中，核基础设施仅是已部署核武库的补充。尽管如此，两个模式之间有足够的相似性，就是说，曾经对“无武器威慑”的种种质疑，同样适用于此概念的现今修正版。在这些质疑中，最重要的一点是担忧基于能力的威慑可能颠覆战略稳定。其它的质疑中，有的怀疑这样的威慑模式无力向盟国提供延伸威慑，有的认为这种模式可能使对方壮胆而出手（而不是以实力威慑使之缩手）；再一个质疑是，这种隐伏的核重构能力是否具有足够的生存能力，而成为有价值的威慑。

战略稳定

美国官员频繁地提到快速响应核基础设施在应对全球喧嚣中的作用。例如，时任国家核安全管理局负责国防项目的副局长托马斯·达格斯蒂诺（Thomas D'Agostino）认为：“地缘政治威胁环境的不利变化，可能会要求我们在相对较快的时间内制造并且部署额外弹头。”³⁵ 然而，即使我们能够具备这项能力，其鼓吹者可能根本没有意识到曾经导致原始

的“无武器威慑”理论备受争议的一项担忧，这就是，以迅速建立核军备来应对全球动荡的做法，本质上可能就在颠覆稳定。

为说明这一担忧，乔治·珀科维奇和詹姆斯·阿克顿（George Perkovich and James Acton）描述了这样一种情景：一个虚拟的核国家因为自认受到威胁，“可能会通过重构其核武库来展示决心，于是可能激起另一个有能力的对手或者一个好战国家的保护伞国起而效之，以尽快夺回平衡。”³⁶ 这种假设场景和在快速响应核基础设施模式下可能发生的任何情况之间，固然有明显差别：前者意味着实施行动只需几周或几个月，后者若想做出响应，可能需要几年时间。此外，核武器从零向有过渡，其所引发的后果，可能远比简单地向已经相当可观的核武库添加一些弹头要严重得多。尽管如此，珀科维奇和阿克顿假设的情景，与核武器集成能力将快捷投入运作的设想之间，确有明显的相似。这两种情况都可能导致一种经典的“安全困境”，在此困境中，一个国家为提高自身安全采取行动，可能诱发其对手采取对应措施，双方的不明行动呈螺旋形恶性升级，增大了双方都不情愿看到的冲突几率。³⁷ 废除数以千计的储备弹头的行动无论可获得什么效果，都不可以牺牲战略稳定为代价。因此，政府在负责任地实施这个计划之前，必须实实在在地消除人们对此计划可能破坏战略稳定的担忧。

延伸威慑和胁迫

另一个考虑因素是，快速响应核基础设施模式除了必须阻遏敌人对美国的直接攻击以外，是否能够执行美国核武器的其它两项功能。其一，美国需向盟国提供延伸威慑，

此已广获认可；其二，实施核“胁迫”，此已在国家宣示性政策中不言自明。

在大量削减美国弹头数目之前，美国政策制定者必须证明，无论采用其它任何替代方案，美国都能向盟友和伙伴提供“核保护伞”。在此安排中，美国必须承诺，美国愿意为保护盟友而甘愿本土遭受攻击的风险。核战略家一直纠结于延伸威慑的可信性，即便手中拥有庞大的核武库。讽刺的是，安抚盟友的安全承诺无论如何真诚，总是比不上向对手展示决心更有说服力。一位欧洲领导人有句名言：延伸威慑与信誓旦旦的区别在于，“在美国承诺报复的信用努力中，为威慑俄罗斯只占 5%，为安抚欧洲却占 95%。”³⁸

因此，人们有理由相信，如果美国的核力量大多由虚拟武器而非真实武器组成，美国的安全承诺就更加令人怀疑。美国在欧洲保持一定数目的前沿部署核武器，部分原因就是强调了其对北约的承诺。³⁹ 美国及其盟国似乎更看重这些武器的实体存在，更愿意选择这种实在的安排，而非美国战略武器支撑下的安全承诺。欧洲对实际武器如此重视，也间接说明以虚拟核能力来实现延伸威慑的想法难树公信力。

对快速响应核基础设施模式能否奏效的另一项质疑是指向其核胁迫功能。核胁迫与“中央”威慑是两种不同的概念。威慑属于被动性威胁，即威胁对手不得采取特定行动（例如：攻击某国本土），否则将施以惩罚；胁迫则属于主动性威胁，即压服对手采取某项行动（例如，从被占领土撤出），否则不会取消威胁。⁴⁰ 核胁迫也是核武器的一种意料之中的“用途”，虽然从历史上看，这种用途不如犯我必报的威胁更常见。⁴¹ 但是，一般认为胁迫要比“中央”威慑更难奏效。隐伏核能

力模式或许能威慑对手不敢贸然直接攻击我本土，但是它可能不足以实施胁迫，部分原因是这种快速响应核基础设施模式不能充分地迅速地响应，来对快速发展的事态产生影响。

生存能力

以快速响应核基础设施模式取代现成武库的思路，还需面对一个最大的挑战，这就是如何确保这些基础设施——像我们保护当前核武库一样——不会被对手先发制人的攻击所摧毁。构成快速响应核基础设施的那些具体设施，其实只是为数寥寥的几个“瞄准点”，成为第一次打击目标的几率很高。这些设施的位置，和美国洲际弹道导弹发射井一样，已经被对手掌握；为确保生存，将需深埋于地下，其设计必须满足两个看似矛盾的要求：必须能抵御最先进钻地弹头的渗透，同时必须能向国际视察开放。（第二个要求背后的逻辑是，无论是美国还是它的对手，都不能单方面采取隐伏威慑的姿态；这种模式将被视为国际协定的一部分，此协定对各方可能拥有的已建成武器数量实施严格限制。这样一种协定系统将需要辅之以严格的核查规程，于是要求各方的敏感地点充分开放。）

然而，即使这些要求得到满足，人们仍然有理由怀疑，将核基础设施埋入地下是否就提供了充分的解决办法。正如克里斯托弗·福特（Christopher Ford）指出，国家的需求将要求此核武器集成能力体系既能生存也能发挥作用，而不只是“一些分离的组成元素，埋葬在各自孤立的深洞之中。”⁴² 此体系应包括“全部必需的能力……且完整无损，一旦国家要求重建、部署，以及有可能使用核武库，就能运作起来，这些能力包括：生产和组装设施、弹头组件和裂变材料储存库、运载系统及其弹头加载、管理和运作的机构

和程序、以及重构这些武器系统并保障其发挥作用的后勤和通信链接。”⁴³ 其每一项能力都必须得到保护。

未予深究的其它问题

还有一类问题，是质疑快速响应核基础设施模式的实际运作机制，尤其涉及到与俄罗斯的双边关系。具体而言，美国削减储备弹头会要求俄罗斯采取对等行动吗？美国的核政策似乎很重视在弹头数量上与俄罗斯大体相当，《2010年核态势审查报告》明确指出：“[美俄之间]的核能力如有巨大差距……可能不利于维持稳定、长期的战略关系，特别是在核力量大幅度削减的情况下。”⁴⁴ 奇怪的是，快速响应核基础设施模式的鼓吹者们似乎忽视了单方面削减核库存会破坏稳定的可能性。⁴⁵ 当军备控制辩论中提及俄罗斯非战略性弹头的数量优势时，美国官员便经常提到美国在非部署战略武器上的优势，言外之意是这些力量无非是彼此消长。⁴⁶ 那么，美国减少其避险性核力量会让俄罗斯在非战略性武器上占据可能打破稳定的优势吗？

另一个问题是关于核查。快速响应核基础设施模式的鼓吹者所设想的核武器集成能力具备能实现各种伟大壮举的高度敏捷。然而这种愿景又与完全消除核武器的雄心壮志伴生同存。只是，秘密和迅速重建核武装的潜在能力可以说是核裁军的最大障碍，因此，当这些鼓吹者在呼吁构建此能力时，其实别人可能听不出其中的音调。就是说，尽管此模式的本意在于通过加强核基础设施能力，尤其是生产新核武器的快速能力，来最终促成实际弹头的削减，美国的对手不一定听得明白。也许正好事与愿违。

于是，美国可能有必要允许外界对其核武器集成能力设施开展侵入式核查，才能避免俄罗斯和其它国家出于敌意而以牙还牙地加大投资。根据当前的美俄双边条约，只有已部署武器必须接受核查。然而，如果采用快速响应核基础设施模式，核武器集成能力设施可能与已部署武器一样，必须接受同等严格的核查。这种前景，显然不是美国核武器机构所乐见的。

弹头削减与核基础设施现代化相挂钩

要关注的最后一点是，如何把战略核弹头的削减与核设施的现代化建设捆绑在一起考虑。核武器削减的拥护者和反对者，在过去十年间出于各种原因，都将两者联系在一起。奥巴马政府与其前任一样，可能也是出于政治原因这样做。决策者们向公众保证，快速响应核基础设施可以弥补核武库的压缩，由此为其削减核弹头的意图提供某种程度的遮掩。与此同时，国会共和党人促成了以批准《新战略武器削减条约》作为交换，承诺对核集成设施进行现代化。他们的动机，有人认为是设定一个昂贵的“价格标签”，从而终将抬高削减核弹头的政治成本；也许他们只是希望在废核思潮汹涌的年代加固现存核体系。然而，这种方法对双方来说都存在着一个关键的缺陷。

决策者早就认识到对核武器集成能力投资和威慑力量之间的关系，许多人预测，如果美国不对其核基础设施进行现代化，后果将不堪设想。例如2008年，时任国防部长罗伯特·盖茨认为：“毫无疑问，[美国]如果不恢复检验我们的核武库，或者启动核设施现代化改造计划。就绝对无法做到既维持可信核威慑，又削减核武库弹头数量。”⁴⁷话已至此，如果再不做出投资，这些把两者捆绑

起来的表述势将对美国核武库的技术可信度造成自残。的确，自从盖茨发表了这种不当言论以后，基础设施现代化建设的步伐已大大减慢，新设施建设被推迟了好几年。这一转变引发了一个问题：决策者们现在会愿意接受盖茨关于美国核武库可信度已经开始下降的逻辑推论吗？

美国领导人自己设置了一个站不住脚的立场：他们不可能将削减核弹头与基础设施现代化脱钩而不损害核威慑的可信度；与此同时，他们无法找到可行的机制来强行重振核基础设施。于是，一再提及的未来核武器集成能力，离现实越来越远。

结语

随着美国武器不断老化，维护越来越困难，从中长期来看，广义而言的核基础设施现代化肯定有其必要。然而，如果把核基础设施现代化蜕变成替代核避险力量的选择，又可能意味着偏离更迫切的国家使命，这种偏离将十分昂贵、不可行，并具有颠覆战略稳定的潜在可能。核武器集成能力的思路，应该着眼于既能维持目前的旧核武库，同时也能支持美国政府核议程上的其它使命，包括弹头拆除、核不扩散、条约核查、核反恐以及核取证。

鉴于总统已经承诺，只要核武器在任何地方存在，美国将继续保持核弹头，那么这些使命中的第一项，即维持旧核武库，已经不证自明。进一步，因为任何超过《新战略武器削减条约》水平的额外削减，可能需要美国加固对已部署核武库的信心，因此，确保这些武器的健康——而不是撤除这种避险力量——才是废核主义阵营最应关注的优先。其它核使命都需要依赖坚实的核基础设

施，或许这种依赖关系不太明显，但事实上每项使命都依赖于专业科研与开发的有限资源。平衡这些使命的轻重缓急需要熟练的管理，资源的日益稀缺将导致我们面临的挑战更加严峻。总之，对于整个核武器集成能力，我们必须排列出完整的全部需求，从而做到正确评估这些需求的可取性和可行性。

快速响应核基础设施构想不仅表象令人困惑，它与生俱来的内在矛盾更令人费解。鼓吹大幅度削减美国核武库的呼声来自多元的，常常令人意外的群体，这种呼声将其前提建立在两项发展之上：其一是冷战结束后安全局势有所改善，其二是自“核武库管理计划”出台以来民众对美国陈旧武库的信心增强。⁴⁸ 然而，快速响应核基础设施模式的鼓吹者们一直在争辩说——或许出于无心——以上两项发展都太过脆弱，因而需要

把核武器集成能力建设成能迅速逆转弹头削减造成的劣势。这种说辞对已经发生的削减尚且没有说服力，对未来削减已部署或储备力量而言更是站不住脚。

避险核威慑——亦即对核武库内技术问题或地缘政治发展突变保持响应的能力——是核武器体系当仁不让的职能。至于如何能最有效地承担起这种责任，无论是基于大规模避险力量，或者弹头储备与核基础设施相结合，或者基于其它替代模式，我们还难以确定。但是，如果想实质性偏离现状，任何此类企图都必须能证明在成本、效用和对战略稳定的影响方面具备明显的优势。做出这样的确定，要求我们必须放弃投机性质的股票术语，代之以用批判性思维来考察核武器集成能力模式应该是什么样子，以及它应该产出怎样的结果。♣

注释：

1. Sustaining U.S. Global Leadership: Priorities for 21st Century Defense [维持美国全球领导地位：21 世纪国防优先], (Washington: Department of Defense [DoD], 5 January 2012), 5.
2. Remarks by President Obama at Hankuk University [奥巴马总统在韩国外国语大学的讲话], Seoul, Republic of Korea, 26 March 2012.
3. 此弹头上载能力是克林顿政府的“领先与避险”战略的遗产。这一战略在《1994 年核态势审查报告》中首次引入，它呼吁美国率先削减其部署部队，并且鼓励军备控制，同时通过维护相当规模的未部署核弹头库存，以对冲不利的发展。参看 Samuel W. Bodman and Robert M. Gates, “National Security and Nuclear Weapons in the 21st Century” [国家安全与 21 世纪核武器], US Department of Energy/Department of Defense, September 2008, i. 关于利用未部署核弹头来对冲技术问题或地缘政治突发风险的讨论，请参看 Nuclear Posture Review Report [核态势审查报告], (Washington: DoD, 2010), 38.
4. 此术语有各种不同说法，包括快速响应核基础设施、快速响应国防基础设施、快速响应工业基础设施等。
5. Nuclear Posture Review Report [2002 年核态势审查报告], (Washington: DoD, 2002), i-iii.
6. 《2010 年核态势审查报告》没有将快速响应核基础设施的愿景局限于仅仅“技术避险”；它在其它场合提出，现代化“将会通过允许我们在不需要大量非部署库存的情况下规避未来的威胁，以启动进一步裁减军备。参看 Nuclear Posture Review Report [2010 年核态势审查报告], (Washington: DoD, 2010), 40.
7. Andrew Weber, testimony before the Senate Armed Services Subcommittee on Strategic Forces [在参议院军事委员会战略力量小组委员会的证词], 17 April 2013. 能源部和美国国防部虽然一直（至少在口头上）承诺支持快速响应核基础设施模式，他们同时也赞同另一种明显允许削减避险核力量的策略。2012 年 11 月，核武器理事会批准了核武库延寿计划，该计划将实施所谓的“3 + 2”愿景，即核武库将被整合为三枚弹道导弹弹头加两枚空投弹头。此愿景被吹捧为启动了“通过平衡潜射弹道导弹和洲际弹道导弹部分的部署，削减技术避险所需要的核弹头的数目。”参

- 看 Fiscal Year 2014 Stockpile Stewardship and Management Plan [2014 财年库存管理计划], (Washington: DoE, June 2013), 2-16.
8. Linton F. Brooks, testimony before the Senate Armed Services Committee [在参议院军事委员会的证词], 24 March 2004.
 9. John R. Harvey, “How Can the Nuclear Weapons Enterprise Itself Reinforce ‘Assurance’ and ‘Dissuasion?’” [核武器体系如何自我加强“保障”和“劝阻”力度], Presentation to 36th Annual IFPA-Fletcher Conference, Washington, DC, 15 December 2005.
 10. 时任国家核安全局副局长托马斯·达格斯蒂诺也确定了一些快速响应核基础设施的具体职能：确保核弹头可用来补充作战部署力量；确定和解决核武库的技术问题；设计、开发、认证和生产翻新或更换弹头；保持设计、开发并开始生产新型弹头的能力；生产所需数量的弹头；拆解弹头；以及保持进行地下核试验的就绪状态。然而在他发表这通讲话的时候，他提及的这些功能与核武器集成能力概念下的功能没有明显差别。参看 Thomas P. D’Agostino, testimony before the House Armed Services Committee, Subcommittee on Strategic Forces [在众议院军事委员会战略力量小组委员会的作证], 5 April 2006.
 11. Complex 2030: An Infrastructure Planning Scenario for a Nuclear Weapons Complex Able to Meet the Threats of the 21st Century, [核武器集成能力 2030：能应对 21 世纪威胁的核武器集成能力基础设施规划], DOE/NA-0013 (Washington: DoE/NNSA, 23 October 2006), 9.
 12. 见注释 8 中 Brooks 证词。
 13. Greg Mello, “New Bomb, No Mission” [新炸弹，无使命], Bulletin of the Atomic Scientists, 53, no. 3 (May/June 1997): 28-32.
 14. D’Anne Spence 概括了国家核安全局在“以每年大幅度削减的维护资金，维护日益破旧的武器集成和核武库”所面临的挑战。参看 D’Anne E. Spence, “Zero Nuclear Weapons and Nuclear Security Enterprise Modernization” [零核武器与核安全体系现代化], Strategic Studies Quarterly, 5, no. 3 (Fall 2011): 124.
 15. 见 Appendix D: “U.S. Nuclear Weapons Life-Cycle” in The Nuclear Matters Handbook [核物质手册附件 D：美国核武器生命周期], (Washington: Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs, 2011), 181-93.
 16. George H. Miller, Paul S. Brown, and Carol T. Alonso, “Report to Congress on Stockpile Reliability, Weapon Remanufacture, and the Role of Nuclear Testing” [向国会提交的核武库可靠性、武器翻新与核检验作用报告], Lawrence Livermore National Laboratory, UCRL-53822, October 1987.
 17. 见注释 11 中 Spence 文。
 18. National Research Council, The Comprehensive Nuclear Test Ban Treaty: Technical Issues for the United States [全面禁止核试验条约：美国的技术问题], (Washington: National Academies Press, 2012), 30.
 19. Joseph C. Martz, “Reconstitution as Deterrence: Advantages and Challenges of the Strategy” [作为威慑的重构：战略优势和挑战], Actinide Research Quarterly, no. 1 (May 2011): 1-9. “核”是内爆武器的核心——含有裂变材料和与之粘结的中子反射体。在 20 世纪 50 年代试验的一些核武器使用的是只用 U-235 或者与钷合成的钷核。参看 “Restricted Data Declassification Decisions 1946 to the Present (RDD-7)” [受限数据解密决定，1946 年至今 (RDD-7)], DoE, 1 January 2001.
 20. 设计阶段包括洛斯阿拉莫斯国家实验室和劳伦斯利弗莫尔国家实验室之间的竞争，这两者间的竞争开始于 2005 年 5 月。次年 2 月，各个团队都对自己的设计充满信心；2006 年 3 月，他们完成了任务。参看 Jonathan Medalia, “The Reliable Replacement Warhead Program: Background and Current Developments” [可靠替换弹头计划：背景和当前的发展], Congressional Research Service report RL32929, 27 July 2009, 16-17.
 21. Department of Energy, “Nuclear Test Readiness: Report to Congress” [核检验就绪状态：提交国会的报告], May 2011.
 22. 见注释 19 中 Martz 文。
 23. Richard Mies, “Strategic Deterrence in the 21st Century” [21 世纪战略威慑], Undersea Warfare 48, (Spring 2012): 12-19.
 24. Marisa Sandoval, “Pit Perfect: LANL Meets Plutonium Pit Production Goal” [完美钷核：洛斯阿拉莫斯国家实验室完成钷核生产目标], National Security Science, issue 3 (2011): n.p., http://www.lanl.gov/science/NSS/issue3_2011/story3full.shtml.

25. Frank Kendall and Neile L. Miller, letter to the Honorable Howard P. McKeon, chairman, House Committee on Armed Services [致众议院军事委员会主席霍华德·麦肯阁下的信], 8 April 2013. 根据美国国防部和美国能源部协议备忘录, 最初要求国家核安全局在 2022 年的时间框架内, 达到每年 50-80 个钚核的产能。
26. William Perry, testimony before the Senate Committee on Foreign Relations [在参议院外交关系委员会的证词], 29 April 2010.
27. William J. Perry and James Schlesinger, co-chairs, America's Strategic Posture: The Final Report of the Congressional Commission on the Strategic Posture of the United States [美国的战略态势：国会美国战略态势委员会最终报告], (Washington: US Institute of Peace Press, 2009), 24.
28. 根据美国国防部《核物质手册》, “非活跃近期避险弹头”作为技术避险或地缘政治避险的一部分, 可以在 6 到 24 个月内作为活跃就绪弹头; “延伸避险弹头”作为技术避险或者地缘政治避险的一部分, 可以在 24 到 60 个月内作为活跃就绪弹头。参看 Nuclear Matters Handbook: Expanded Edition, Section 3.4.1: Configuration Management. 参看《核物质手册：扩大版》第 3.4.1 条：配置管理。
29. 见注释 8 中 Brooks 证词。
30. 见注释 3 中“2010 年核态势审查报告”第 43 页。
31. 以 1976 年“竞争分析”演练 B 团队的案例为例, 在此案例中一个独立小组受命审查美国对苏联军事威胁的情报评估。该小组编制了苏联实力和战略意图的评估, 此评估与当时常规情报评估大相径庭。参看 Anne Hessing Cahn, “Team B: The Trillion-Dollar Experiment” [B 团队：万亿美元试验], Bulletin of the Atomic Scientists, no. 3 (April 1993): 22-27.
32. Jonathan Schell, The Abolition [废核], (New York: Alfred A. Knopf, 1984), 119.
33. 见注释 19 中 Martz 文。另外, 前布什政府官员克里斯托弗·福特也认为, 《2010 年核态势审查报告》“积极地赞同”无武器威慑的基本要素。参看 Christopher A. Ford, “Nuclear Weapons Reconstitution and its Discontents: Challenges of ‘Weaponless Deterrence’” [核武库重构及其不足：“无武器威慑”的挑战], Hudson Institute, November 2010.
34. 几份政策文件更加明确地指出了这种关联。例如, 国家核安全局文件《核武器集成能力 2030》称, 快速响应核基础设施“促进了核武库规模的削减, 以及对能力威慑更多的依赖。”请参阅美国能源部/国家核安全局发布的《核武器集成能力 2030》。2008 年国家核安全局战略文件《核武器集成能力转型》也提及了通过基础设施的威慑：“可靠、高效快速响应核基础设施的目的, 是要阻遏对手寻求优势, 即寻求优势的企图被快速响应发现并被排除。更加快速响应的基础设施将促成核武库的进一步削减。”参看“Final Complex Transformation Supplemental Programmatic Environmental Impact Statement” [最终核武器集成能力转型补充程序环境影响评价声明], National Nuclear Security Administration, DOE/EIS-0236-S4, October 2008, S-15. 截至 2014 年, 国家核安全局网站证实, “国家核安全局继续保证现有核武库的安全、安保以及可靠性, 国家核安全局正朝着《2001 年核态势审查报告》中‘核集成转型’所要求的新型快速响应核基础设施的方向转型。 <http://nnsa.energy.gov/aboutus/ourprograms/defenseprograms/futurescienceandtechnologyprograms/productiontechnology>。”
35. 见注释 10 中 D'Agostino 的证词。
36. George Perkovich and James M. Acton, eds., Abolishing Nuclear Weapons: A Debate, [废除核武器：一场辩论], 收录于 Adelphi Paper 396 [阿德尔菲论文 396], (London: International Institute for Strategic Studies, 2009), 120-24.
37. Robert Jervis, “Cooperation under the Security Dilemma” [安全困境下的合作], World Politics 30, no. 2 (January 1978): 167-74.
38. Keith Payne, “Future of Deterrence: The Art of Defining How Much Is Enough” [未来威慑：确定多少才算够的艺术], Comparative Strategy 29, issue 3 (2010): 220.
39. 美国还在大陆各州储备核武器, 以支持延伸威慑时用于全球部署。参看《2010 年核态势审查报告》第 27 页。
40. Thomas Schelling, Arms and Influence [武器与影响], (Cambridge, MA: Yale University Press, 1966).
41. 关于已公布的核威胁实例不完全清单, 参看 Samuel Black, The Changing Political Utility of Nuclear Weapons: Nuclear Threats from 1970 to 2010 [核武器不断变化的政治效用：1970 年至 2010 年间核威胁], (Washington: Henry L. Stimson Center, August 2010).
42. 见注释 33 中 Ford 文。
43. 见注释 33 中 Ford 文。
44. 见《2010 年核态势审查报告》第 xi 页。

45. 例如，战略态势委员会的报告指出，“大量减少储存需要与俄罗斯进行双边行动。”然而，该报告还建议，“非部署武器的一些潜在削减，不需要等待俄罗斯。美国若翻新核基础设施，可以降低其对储备弹头的依赖，因此也可以减少储备弹头的供应。参看注释 27 中 Perry and Schlesinger 文，第 25 页。
46. 例如，前国防部长威廉·佩里曾指出，“战术核武器的不对称主要是俄罗斯占上风，但是战略储备武器的不对称主要是美国占上风，而且对我所接触过的俄罗斯人来说，这是一个很难咽下的一口气。”参看注释 26 中 Perry 的证词。
47. Robert M. Gates, remarks at the Carnegie Endowment for International Peace [在卡内基国际和平基金会的演讲], Washington, DC, 28 October 2008.
48. 以最少的库存弹头数目维持核威慑，是核政策界很流行的原则。这一立场的一些更令人吃惊的倡导者包括：前美国战略司令部司令官、退休上将詹姆斯·卡特莱特，他在 2012 年概述了仅由 450 枚已部署核弹头组成的建议核态势。参看 James Cartwright, chair, “Modernizing U.S. Nuclear Strategy, Force Structure and Posture” [美国核战略、部队结构与态势的现代化], 收录于 Global Zero US Nuclear Policy Commission Report [全球零核美国核政策委员会报告], May 2012. 与此同时，空军大学学者 Gary Schaub Jr. and James Forsyth Jr. 认为：“美国的核安全能够轻易地依赖数量相对较少的反击和对等武器，总数略超过 300 件即可。”参看 James Wood Forsyth Jr., et al., “Remembrance of Things Past: The Enduring Value of Nuclear Weapons” [追忆过去:核武器的不朽价值], Strategic Studies Quarterly 4, no. 1 (Spring 2010): 74-89. 最后，在 2013 年 6 月，奥巴马总统宣布，他相信美国能将其已部署核武器储存减少三分之一，同时仍能维持美国威慑的可信度，并且确保美国盟友的安全。参看 “Remarks by President Obama at the Brandenburg Gate” [奥巴马总统在布兰登堡大门前的讲话], Berlin, Germany, 19 June 2013.

达拉斯·博伊德 (Dallas Boyd)，现任 Leidos (前称 SAIC) 公司资深政策分析员，致力于核武器政策和反恐研究，著述见于《防扩散评论》、《华盛顿季刊》、《原子科学家公报》及《冲突与恐怖主义研究》等刊物。他自哈佛大学肯尼迪政府学院获公共政策硕士学位。

As we continue to implement the NPR, we are focused on maintaining and improving strategic stability with both Russia and China.

— FACT SHEET: Nuclear Weapons Employment Strategy of the United States (<http://www.whitehouse.gov/the-press-office/2013/06/19/fact-sheet-nuclear-weapons-employment-strategy-united-states>).

我们在继续定期编制国家核态势审查报告的同时，重点关注如何保持和改进与俄罗斯及中国的战略稳定。

——美国的核武器运用战略，美国白宫网站，2013/06/19

重振联合作战环境下的核作战意识

Revitalizing Nuclear Operations in the Joint Environment

凯文·摩特，美国陆军中校（LTC Kelvin Mote, USA）

联合作战规划专家在思考美国面临的未来威胁时，必须考虑多种情况。

对手的武器库中有许多选择，包括改良的末端制导弹道导弹、网空作战能力，以及太空相关武器系统。而美国，经过长达 13 年的平叛作战，已经忽视了对我军构成持久威胁的核武器。正如各种文献和威慑专题讨论会所强调，现在已经到了必须严肃讨论和思考敌人动用核武器的可能性以及我方规划如何在限制性环境中开展作战的时候了。因此，国防部必须教育规划核作战的有关人员，重新编写核作战准则，提高意识，确保联合部队做好应对未来挑战的准备。

战略背景

如今，在美军有关如何应对明天战争的描述中，“网空作战”是个“时髦”词。但网空作战只代表我们在 2025 年可能面对的场景中潜在敌人对多个作战领域发挥影响的一部分。根据《全球趋势 2025》报告，“未来 20 年间使用核武器的风险尽管非常低，但是很可能高于当今的风险水平”。¹ 敌人既然有使用这些武器的可能性，我联合部队就要认真备战，确保打赢。正如参谋长联席会议主席在《联合作战顶层概念》中所言：“全球经济中先进技术的扩散，意味着中量级军队和非国家行为者现在可以获得曾由超级大国独占的武器。”² 当今世界包括七个公开的核国家，一个隐秘的核国家（以色列），以及至少三个有志拥核的国家（伊朗、朝鲜和叙利亚），核现象比以往任何时候更加全球化。³ 奥巴马总统在 2009 年布拉格演讲中承认：“全球核

大战的威胁已经减弱，但是核攻击的风险却在增加。”⁴ 这些条件形成未来核世界的基准线，并产生了一个自然的假设：发展中国家不会遵守《核不扩散条约》。

扎卡里·戴维斯（Zachary Davis）将此现象称作“战略储存”，意思是，那些能构成军事（或经济）优势的技术暂时保持在未开发状态，等待安全需求驱动这些技术武器化的时机来临。⁵ 例如，在伦敦《泰晤士报》最近的一篇文章中，沙特一位高级官员称：“目前没有寻求单边军事核项目的意图，但是如果伊朗人发展自己的核能力，这种态势会立即改变……伊朗拥核而沙特无核，从政治上讲，这完全不能接受。”⁶ 许多国家现在感觉到，随时开发这些储存技术符合其最高利益。美国军队一直享有的核优势在未来可能减弱。技术的扩散、超级大国减少战略核武器储备的趋势，以及多国行动者相互威慑的复杂性，促使许多国家寻求核能力。《全球趋势 2030》重申了多极世界的威胁，并指出，遏制朝鲜和伊朗核野心的努力，将决定《核不扩散条约》的未来。⁷ 与之平行，这些行动还将确定美军联合作战参谋班子如何策划核能力及如何编写核作战准则。战略规划专家需要准确预见未来，并调整我们的核能力，以应对美国可能面临的新现威胁。

历史借鉴

美国的核能力源于 70 多年的智力和作战应用开发。在冷战高峰时期，美国科学家和联合作战规划专家同时进行武器开发和武器应用之效应的作战艺术开发。审视对手将

在未来制造的复杂环境，我们认识到，美军必须重振核作战意识，以威慑那些核武器追求者，并且重新编制核环境中的作战准则。《二十一世纪核威慑》一书或许是对这种现象的最佳研究之一，该书的作者泰雷兹·德尔佩奇（Thérèse Delpech）指出：“只要核武器存在，即使数量很少，威慑是应对核武器的最安全做法。此原则理论上比较容易接受，而实践起来则比较难。在冷战时期是这样，今天似乎更加如此。”⁸

“理论”和“实践”这两个词汇与“概念”和“准备”相对应。如何做好准备在未来冲突中实施威慑，途径很多。更重要的是，无论计划如何周密，我们不能假设危机中的每一项行动都不出所料。用德尔佩奇的话说：“一个**战略海盗时代**可能正在展开，在这里，海盗是指蔑视法规和欺瞒诈骗者横行无忌。”（粗体强调来自原文）⁹作为一个国家，我们没有做好准备，不足以应对核追求者的增多和这些国家的核作战准则不透明甚至根本没有核作战准则的现实。能否保持有效的威慑，难度在于如何应用作战艺术发挥威慑效应。

对作战艺术的理解，如许多中级军官教育课程中所描述，起源于作战准则。然而大多数情况下，作战规划专家看不到核武器的现行作战准则。首先，核武器的使用是由总统控制的。自苏联解体以来，美国一直处于重新界定核武器作战政策的状态中。冷战时期的核战争准则来自国家战略指南，其原则精神贯穿体现于联合作战和军种作战出版物。现在，国防部已经有了如何运用核武器的国家战略指南，但还没有制定出相应的作战指导准则，因此我们正处于一个关键时期。联合出版物 JP 3-12《联合核作战准则》作为纲领性的联合作战指导文件，为核作战提供了框架。此文件初版于1995年12月15日，

但在2006年作废。修订版的发布日期至今尚未确定。或许更值得关注的是，陆军相应的出版物，战地手册100-30《核作战》公布于1996年，目前仍作为现役战地文件保留；而引领陆军编制战地手册和指导陆军作战规划专家的战略指导文件，不复存在已17年有余。这种出版期久远的出版物和联合作战规划文件的缺失，是我们的军官队伍核战争艺术和技能不断下跌的原因之一。

军官们必须了解核武器的效应。美军长达十三年的平叛作战，美国国家核政策的改变，加上新技术的兴起，损耗了我们的核作战概念，削弱了我们的危险意识，使我们对美军面临的国际核武器威胁不太在意。展望未来冲突，我们必须知道对手可能及如何使用核武器，了解我们的作战部队必须克服哪些核作战效应。

作战考量

目前，大多数年轻一代的军事规划人员已不熟悉核武器的威胁。在1980年代长大的人，很容易联想到核武器的毁灭性，那个时代的电影描述了核武器的巨大威力，里根总统的“战略防御计划”推动了军队以新的军事战略取代同归于尽战略。然而，在“后X代”军界，军官们对美国“冷战”遗产的经验非常有限，眼下的军事作战只关注于如何开展平叛和民心战，而常常忽视全频谱军事行动的更多内容。

虽然核战争处在作战频谱的最右端，我们必须了解如果敌人使用核武器会发生什么。核武器的性质，决定了一枚核弹引爆后，其所产生的效应要比常规炸弹强大得多。大规模爆炸加大规模杀伤，核爆炸要比常规爆炸的威力高出数百万倍。如《核物质手册》

所示，当前的作战准则没有准确反映典型地面核爆炸所产生的效应。¹⁰

我们在查阅核作战效应时有必要注意，除了指导生化核放射及高能炸药等的部队作战保护的文件或章节之外，联合作战准则中还有哪些地方谈及了核作战。核作战概念在 JP 3-0《联合作战》中出现过一次，在 JP 5-0《联合作战规划》中出现过两次。在总共超过 468 页的两部文件中，此概念只占不足区区一页。¹¹

这些文件中不讨论核作战环境中的核作战效应，暴露出我们缺乏与拥核对手对抗所需的作战策划和部队运筹的作战艺术。联合出版物对武器运用和策划着墨不多，没有为联合作战规划专家提供如何对抗拥核敌人的指导框架。虽然是否使用核武器由总统定夺，联合作战规划专家必须做好准备，引导我军在未来战略背景下的抗衡环境中打赢拥核对手，尤其要注意以下几点：

1. 敌人的核武器、甚至其首先使用核武器的可信威胁，都将对整个军事行动范围产生影响。美国国家领导人需要在此种背景下考虑未来作战行动的战略目标和预期的终局。

2. 敌人可能会考虑凭借有限的核打击，即借助核弹的速度、生存能力（渗透能力），以及对部署的美军关键目标实施核打击（即针对部署部队的弹道导弹攻击）而可能增加成功几率的侥幸，来获得快速战术胜利。

- a. 快速攻击可能导致美国决策周期延误。
- b. 可能需要导弹防御能力来应对威胁。

3. 敌人使用高空爆炸核武器可能降低美国的指挥控制能力。

4. 作战规划专家应审查使用密集编队的风险。敌人使用核武器以及核武器的后续效应，对美国密集型作战编队和前方固定作战基地形成较高风险。

5. 在对拥核敌人作战的环境中，目标选择是控制冲突升级的一个关键考虑因素。对联合作战一体化优先目标列表中的每一个目标，需要做仔细的目标分析，包括其对威慑的影响。作战规划专家们应做好思想准备，应估计到高层领导在战略危机中为保持稳定，可能不批准对大型目标的打击。

把核效应对拥核对手作战的机动艺术纳入思考，为我们增强作战效果提供了一个途径。在未来的冲突中，我们不能假定新兴对手将把作战行动控制在核武器门槛之下；相反，我们必须通过控制冲突升级和抑制升级来管理冲突。在未来作战准则的编写中如能包括这些观点，如能就这些话题开展理性讨论，将为联合作战参谋专家们提供正确信息，为联合部队作战提供更好的指导。

结语

联合作战规划专家在思考美国面临的威胁时，需要考虑多种情形。对手的武器库中有多样武器选择，包括改良的弹道导弹、网空作战能力、太空相关武器系统，以及核武器等。各种讨论表明，敌人有可能使用这些武器，我们不可再拖，必须严肃对待，认真讨论，制定出在核环境中作战的计划。这种形势还要求国防部对相关人员进行核作战意识教育，重新制定核作战准则，以确保联合部队做好准备，应对未来的挑战。♣

注释:

1. National Intelligence Council, Office of the Director of National Intelligence, Global Trends 2025: A Transformed World [全球趋势 2025 : 变换的世界], (Washington, DC: National Intelligence Council, Office of the Director of National Intelligence, 2008), 67, <http://www.aicpa.org/research/cpahorizons2025/globalforces/downloadabledocuments/globaltrends.pdf>.
2. Chairman of the Joint Chiefs of Staff, Capstone Concept for Joint Operations: Joint Force 2020 [联合作战顶层概念 : 联合部队 2020], (Washington, DC: Chairman of the Joint Chiefs of Staff, 10 September 2012), 2, http://www.defenseinnovationmarketplace.mil/resources/JV2020_Capstone.pdf.
3. Thérèse Delpech, Nuclear Deterrence in the 21st Century: Lessons from the Cold War for a New Era of Strategic Piracy [二十一世纪核威慑 : 冷战之鉴与战略海盗新时代], (Santa Monica, CA: Rand Corporation, 2012), 3, http://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1103.pdf.
4. “Remarks by President Barack Obama, Hradcany Square, Prague, Czech Republic” [奥巴马总统在捷克布拉格城堡广场的演讲], (Washington, DC: White House, Office of the Press Secretary, 5 April 2009), http://www.whitehouse.gov/the_press_office/Remarks-By-President-Barack-Obama-In-Prague-As-Delivered.
5. Zachary S. Davis, “Strategic Latency and World Order” [战略储存与世界秩序], Orbis 55, no. 1 (January 2011): 72.
6. Hugh Tomlinson, “Saudi Arabia Threatens to Go Nuclear 'within Weeks' If Iran Gets the Bomb” [沙特威胁 : 如果伊朗获得核弹, 沙特将在“几周内”造出核武器], Times (London), 10 February 2012.
7. National Intelligence Council, Office of the Director of National Intelligence, Global Trends 2030: Alternative Worlds [全球趋势 2030 : 另类世界], (Washington, DC: National Intelligence Council, Office of the Director of National Intelligence, 2013), 57, http://www.dni.gov/files/documents/GlobalTrends_2030.pdf.
8. 见注释 3, 第 1 页。
9. 见注释 3, 第 6-7 页。
10. Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs, Nuclear Matters Handbook [核物质手册], expanded ed. (Washington, DC: Office of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs, 2011), 211-37, <http://www.fas.org/man/eprint/NMHB2011.pdf>.
11. Joint Publication (JP) 3-0, Joint Operations [联合出版物 JP 3-0 : 联合作战], 11 August 2011, III-34, V-58, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf; and JP 5-0, Joint Operation Planning, 11 August 2011, IV-51, http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.



凯尔文·摩特, 美国陆军中校 (LTC Kelvin Mote, USA), 田纳西大学文学士, 马里兰大学理科硕士, 现任内布拉斯加州奥佛特空军基地的美国战略司令部全球打击联合功能组成部队司令部联合作战规划官, 负责为实现国家目标而制定慎密、可调适、高时敏性计划提供必要的作战专业知识。他曾作为装甲部队军官及信息作战规划官部署支援“南方守望”和“伊拉克自由”行动超过 48 个月, 其后服务于堪萨斯州利文沃斯堡的合成武器中心使命指挥训练计划。摩特中校是美国陆军指挥总参学院和美国海军陆战队指挥参谋学院的毕业生。

核威慑与网空互动概念初探

Nuclear Deterrence and Cyber: The Quest for Concept

斯蒂芬·森巴拉博士 (Dr. Stephen J. Cimbala)

核威慑自是今非昔比。理论家、政策制定者和军事策划专家已经踏入著名物理学家弗里曼·戴森 (Freeman Dyson) 称之为“概念探索”的地界。¹ 之所以需要探索，一个原因是：核武器无论用于威慑或是其它使命，从今往后必须在后互联网时代或者说网空就绪环境中进行。现今的国际体系，是由政治哲学专家和科技专家共同界定。政府及其武装部队必须调整其官僚结构，方能适应更快及更灵活制定国家决策和兵力应用的形势要求。在此过程中，政府和军队也将越来越深地进入网空、依赖网空，并受制于网空弱点。²

美军已经意识到这样的趋势，国防部组建了美国网空司令部，作为战略司令部以下的二级统辖司令部，负责协调美军所有相关军事单位（陆军网空司令部、美国舰队网空司令部/美国第十舰队、第24空军、海军陆战队网空司令部、海岸警卫队网空司令部）。网空司令部与国家安全局在同一地点工作，由同一总监领导。³ 然而在大部分情况下，核威慑和网空战还是被视为互相独立的问题分开处理。这种核/网分离意识和做法从专家分工角度可以理解，但是它对核威慑现实或当今浓厚网空环境下的危机管理投下了阴影。

在下文的讨论中，让我们首先为主修国家安全政策与战争的学生解说核/网交织的一些泛性理论影响。接着，我们评论网空和信息战的显著重要性，列出一些可能未受关注的警示。然后，我们探讨导弹防御建设——其本身就面临着网空挑战——如何有可能使

美俄两国的政治关系和削核努力陷入更复杂的局面，这并非想暗示美俄互相威慑关系也是其他军备控制和扩散问题的缩影，其实如本文所示，情况发展正好相反。尽管如此，当我们逐步远离网空前的核时代而进入网空核时代的时候，核力量交战的一些长久现实值得我们回味。第四，我们分析核进攻能力建设与更先进导弹防御能力建设相结合，如何可能影响未来的威慑稳定，尤其是在美俄继续争斗的背景下。最后，我们联系未来军备控制、防扩散和威慑的前景，对核/网互动做出相关结论。

核与网：相合还是分开？

网空战概念或实践与核威慑之间的潜在叠接具有什么意义？⁴ 看起来，网空战和核武器好像风马牛不相及。但网空武器对那些崇尚非核或甚至认为军事技术进入后核时代的人具有特别的吸引力，因为数字领域的战争（至少在理论上）有可能在不需要动能打击、在可将物理破坏降至最低的情况下，严重破坏或瘫痪敌人的资产。⁵ 相比之下，核武器简直就是“大规模”毁灭的缩影，故而人们宁愿通过对风险的操纵，用核武器来威慑或避免战争，而不愿动真格发射核武器。不幸的是，无论是核威慑还是网空战，在近期或遥远的未来都不可能存在于互不相干的政策世界里。

核武器，用于威慑摆设也好，一怒射出也罢，都必须被纳入指挥、控制、通信、计算机、情报、监测、侦察 (C4ISR) 系统。对核武器及其 C4ISR 系统必须严加保护，防止

遭受动能打击和数字化打击。再者，那些必须在危机期间管理核力量的决策者，需要保持最高程度的态势感知，既了解己方核军和网军以及指挥系统的状况，也了解潜在攻击者的部队及其 C4ISR，以及潜在对手的大概意图和风险接受程度等。简而言之，管理核危机要求清晰的思维和良好的知情。但是如果双方在危机的初级阶段就使用网空武器，可能对网空和依赖网空的决策行动渠道造成混乱而妨碍清晰的评估。⁶ 这表明网空先发制人打击确有其诱惑力，并可能“成功”，致使核危机管理更脆弱而非更强大。

讽刺的是，自冷战结束以来，美国和俄罗斯战略核武库规模逐渐缩小，虽然从核武器控制和防扩散方面看是积极的发展，但网空攻击能力和核攻击能力的同时并存更令人警觉不安。冷战时期，美苏两国超大规模部署导弹和轰炸机互相抗衡，至少有一点好处，这就是，各自准备了足量的冗余，足以承受第一次打击，于是，遭受袭击之时或之后用于核袭击预警、指挥控制，及报复发射的系统虽然相对单薄，却已足够。并且，在冷战时代，用于军事网空破坏的工具还很原始，远不及现在的水平。而且那个时候，国家及其武装部队在保障国家安全方面对信息系统提供真实信息的依赖也远不如现在那么紧密。如此，美国、俄罗斯、可能还有其它国家武装力量如果缩减到“最低威慑”规模，在以网空攻击先行、动能打击随后、或两者并举的战争形势下，国家的核能力可能失去灵活性及生存韧性。⁷

攻防信息战以及其它网空相关的活动，显然是美军领导人和美国及盟国国家安全机构中其它人非常关心的问题。⁸ 俄罗斯也明确表示了对相关网空问题的担忧。普京总统在 2013 年 7 月初敦促俄罗斯安全会议加强

国家安全防御网空攻击。⁹ 俄罗斯安全专家弗拉基米尔·巴丘科 (Vladimir Batyuk) 在高度评价 2013 年 6 月美俄两国关于保护、控制、审计核材料的协定 (继承最近过期的纳恩-卢格减少核风险协议) 的同时，也警告说，普京和奥巴马总统对网空安全合作的承诺甚至更为重要：“核武器是二十世纪的遗产。二十一世纪的挑战是网空安全。”¹⁰ 另一方面，网空军备控制不易推行，即使双方在这类敏感问题上达成了政治互信，仍有可能碰到严峻的安全和技术问题，尤其是，网空军控谈判代表们如何才能证明本国能充分控制黑客活动和保持透明。

网空领域还贯穿和影响着陆海空天这四个地缘战略领域的作战。但与这四个领域相比，网空无历史可作借鉴，因而更难探究。有作者指出：网空领域“建设时间短，故而对其的研究远不及对其他作战领域那样透彻。”¹¹ 这种状态对网/核交汇意味着什么，目前尚不清楚。以下表 1 根据专家们的看法，归纳了核威慑和网空战的一些主要区分属性；但是，这里列出的核/网之间的差别与上述的认知——即网空与核领域在实际运作中的互动不可避免——并不矛盾。正如美国空军研究所两位研究员雅纳科乔戈斯博士和洛瑟博士 (Panayotis A. Yannakogeorgos and Adam B. Lowther) 所言：“当空军飞向未来时，兵力结构——因而还有兵力发展计划——必须改变，将更加重视有人机和无人机、太空及网空力量投送能力的一体化。”¹²

网空攻击和信息战：重要性有多大？

国防部和政府其它机构，还有军事和信息技术专家们都预期：未来的国家间冲突将包括网空攻击和信息战。¹³ 但是“网空战”这个术语也许会产生误导，因为对计算机和

表 1：网空战和核威慑的属性对比

| 网空战 | 核威慑 |
|--|---|
| 攻击源不明——有可能是伪装成其它参与者的第三方侵扰。 | 攻击源——如果攻击者是一个国家——几乎可以肯定能被找到，甚至恐怖分子匿藏的核材料也可能被追查。 |
| 主要破坏信息系统、网络及其通信内容，但其溢出效应可能影响军事作战系统、经济和社会基础设施。 | 威慑一旦失效，可能导致史无前例的社会大灾难，即使按冷战标准为“有限”核战争，情况亦如此。 |
| 可以阻止攻击者实现目的——如果防御足够坚固，并且 / 或者及时修补漏洞的话。 | 想以威胁作为手段来阻止攻击者实现目的，这种威慑的可信度较低，莫如以确保报复作为惩罚性威慑更加可信（尽管各方企图通过强化导弹防御来改变）。 |
| 网空攻击的目的通常是中断运作或引发混乱，而不是摧毁。 | 核威慑在很大程度上依赖于以大规模瞬间摧毁物理资产和人口作为可信的威胁。 |
| 网空战和信息攻击能持续很长时间而不被察觉，有时也不造成明显或重大破坏，有些甚至在被发现之后也不报告。 | 自 1945 年以来，核武器首次由一个国家或非国家行为体出于敌对目的（而非试验）而使用，这是世界政治上一个改变游戏规则的事件，无论爆炸规模和直接后果如何。 |
| 进入游戏场打网空战的入门费相对较低，从个体黑客到国家实体都可参与。 | 建设和运作二次打击核威慑能力需要有国家支持的基础设施、大量科技知识和长期财政投入来支撑。 |

此表由笔者自制。另参看 Timothy L. Thomas, *Three Faces of the Cyber Dragon: Cyber Peace Activist, Spook, Attacker* [网龙三面：网空和平主义者、幽灵、攻击者], (Ft. Leavenworth, KS: Foreign Military Studies Institute, 2012), 60–66; 另参看 Martin C. Libicki, *Cyberdeterrence and Cyberwar* [网空威慑和网空战], (Santa Monica, CA: RAND Corporation, 2009), 27–28. 该书各处都有相关论述。

网络的攻击只是达到瘫痪敌人关键基础设施目的的一种手段。¹⁴ 乔尔·布伦纳 (Joel Brenner) 如此说：

美国海军耗费了 50 亿多美元开发了一种静音电气传动系统，使潜艇和舰船能悄然航行而难被发现，中国间谍偷了去。海军又花了几十亿美元为其顶级“神盾”巡洋舰开发了新雷达，中国间谍又偷了去。中国和俄罗斯的电子情报部门对我们无孔不入——利用我们漏洞百出的网络和对安全的漠不关心偷窃了我们价值几十亿的军事和商业机密。我们的某些同盟国，如法国和以色列，也试图这样做过。¹⁵

国防部称之为信息和基础设施作战的活动目的，不是大规模杀伤（尽管有可能发生破坏性次级效应），而是大规模和 / 或精确“破坏”。¹⁶ 按照罗伯特·米勒、丹尼尔·库尔和欧文·莱褚 (Robert A. Miller, Daniel T. Kuehl and Irving Lachow) 三人的说法，信息和基础设施作战的目的是“破坏、扰乱、削弱士气、分散精力、最终削弱另一方的能力”。¹⁷ 这个概念可启发我们对基于常规或核报复可信威胁的威慑使命进行思考。但我们务必记住：核武器具有其独特和迅速致命的性质，因而产生了一套打核战争的独特规则，即使这种战争迄今继续留在战略逻辑推理的界限之内。¹⁸ 正如科林·格雷 (Colin Gray) 警告说：

首先，网空力量的破坏效果限制在网空之内，极少有例外。这并不是要低估网空攻击可能造成的问题，而是要坚决断言：网空可能造成的那种破坏和扰乱无法与核武器肯定会造成的直接而更持久的伤害相提并论。¹⁹

值得强调的是：网空战或主要在网空实施的威慑所针对的重心主要是在认知方面。要使网空战（或网空威慑）引起战略家的重大关注，就必须也找到其有价值的应用，即能否有助于解决分析家和作战将士面临的战略性及战术性问题。在这点上，网空战或网空威慑理论引发了与核威慑理论曾经引起的同样担忧。在这两种情况下，理论家都可能走调，高谈阔论地提出优雅的理论概念结构，却不在乎这些理论究竟有无任何可见的实用性。我们必须警惕施里芬计划（译注：Schlieffen Plan——一战前德国一项对东西两条战线开战的战略计划，意图利用速度差，在西线快速击溃法国，然后东移，在俄国未完成集结的情况下再打败俄国，但最终失算）在核领域或网空领域的翻版将我们的注意力引向歧途。

导弹防御：是预示还是问题？

技术不确定性

核威慑与网空相交互动的部分主要涉及到导弹防御。导弹防御，如果可以成功的话，是向攻击方展示两种威慑，一是有能力实施令攻击方难以承受的报复，二是有能力阻止攻击方实现其攻击目的，且后一种威慑加固前一种威慑。²⁰ 如今，导弹防御在技术上和政治上仍有争议。俄罗斯对美国 and 北约实施的欧洲分阶段调适反导计划的反对，至今坚定不移，甚至传闻的国防部秘密研究报告也质疑建议的欧洲弹道导弹防御系统组成部分

的技术熟练程度。²¹ 美国国家科学院在一份关于导弹防御技术的研究中，对奥巴马政府和美国导弹防御局一些关于某些任务的优先排序和弹道导弹防御技术提出疑问。²² 也有一些权威科学专家批驳上述研究，认为其中包含了“众多的错误假设、分析性疏忽和自相矛盾，”从而导致“报告中许多最重要研究结果和建议完全错误，”由此严重削弱了其科学可信度。²³ 与冷战高峰时期把重心放在两极对抗和物理竞赛的背景相比，未来导弹防御的发展和部署面临的技术挑战，会更更多地涉及到软件工程设计中针对多重突发事件和众多参与者的“无常复杂性”。²⁴ 总之，学术和政策界将就导弹防御建设的可行性和可取性继续争论，伴随争论的，则是自里根政府“战略防御倡议”启动以来研究与发展资金继续朝这个方向流动的惯性引力。²⁵

政治陷阱

如果说美国和北约的欧洲导弹防御计划与美俄两国削减战略核武器谈判进展之间的关联还算不上是一种绑架关系的话，至少也是一种问题重重的关联。²⁶ 新削减战略武器条约并不妨碍美国部署未来的导弹防御，尽管俄罗斯在谈判过程中努力限制美国在这方面的自由。²⁷ 不过，当时的俄罗斯总统梅德韦杰夫及其前任和继任者普京都明确表示：俄罗斯的地缘战略观是把美国和北约的导弹防御与在其它武器控制问题上的合作挂钩。同时，美国和北约自2011年开始了欧洲分阶段调适反导计划四阶段部署的第一阶段。²⁸ 2013年3月，美国防部长哈格尔宣布修改此计划的原始方案，放弃原定2022年之前在波兰部署SM-3IIB拦截导弹的计划。然而，这一步没能说服俄罗斯怀疑者相信美国和北约声称其区域及全球导弹防御并不针对俄罗斯的说辞。俄罗斯官员屡次要求美国和北约作

出有法律约束力的保证，保证俄罗斯的战略核力量不会成为该系统的打击目标或受其影响。²⁹ 以下表 2 总结了截至 2013 年秋欧洲分阶段调适反导计划建设的状况。

在写本文之际，美俄之间或北约与俄罗斯之间在欧洲导弹防御方面能否谈妥仍充满

变数，但美国与欧洲盟国及欧洲以外的伙伴在区域导弹防御方面的合作前景态势良好。导弹防御的潜在“牛市”可能出现在亚洲，刺激原因包括来自中日之间的对抗，北朝鲜的威胁及导弹试验，印巴之间的威慑挑战等。从军事现代化（包括常规与核武器）以及未来战争的角度看，与动荡的亚洲相比，欧洲

表 2：欧洲分阶段调适反导计划

| | 阶段 I | 阶段 II | 阶段 III | 阶段 IV (2013 年 3 月被取消) |
|---------|---|---|--|--|
| 期限 | 2011 | 2015 | 2018 | 2020 |
| 能力 | 部署当前能力 | 加强中程导弹防御 | 加强中远程导弹防御 | 对 MRBM/ IRBM/ ICBM 的早期拦截 |
| 威胁 / 使命 | 应对区域弹道导弹对欧洲及美国派驻人员的威胁 | 扩大设防区，防御对南欧的短 / 中程导弹威胁 | 应对短 / 中 / 中远程导弹对整个欧洲的威胁 | 应对美国面临的 MRBM/IRBM/ 和未来 ICBM 的潜在威胁 |
| 组成部分 | 土耳其 Kurecik AN/TPY-2 (FBM)、德国拉姆斯泰因 C2BMC、西班牙海岸附近宙斯盾 BMD 舰 (SM-3 1A) | 土耳其 Kurecik AN/TPY-2 (FBM)、德国拉姆斯泰因 C2BMC、西班牙海岸附近宙斯盾 BMD 舰 (SM-3 1B)、罗马尼亚 Aegis Ashore (SM-3 1B) | 土耳其 Kurecik AN/TPY-2 (FBM)、德国拉姆斯泰因 C2BMC、西班牙海岸附近宙斯盾 BMD 舰 (SM-3 1A)、罗马尼亚和波兰 Aegis Ashore (SM-3 1B / IIA) | 土耳其 Kurecik AN/TPY-2 (FBM)、德国拉姆斯泰因 C2BMC、西班牙海岸附近宙斯盾 BMD 舰 (SM-3 1IA)、罗马尼亚和波兰 Aegis Ashore (SM-3 1IB) |
| 技术 | 现有 | 测试中 | 正在开发 | 在概念阶段取消 |
| 地点 | 土耳其、德国、西班牙海岸附近的舰船 | 土耳其、德国、西班牙海岸附近的舰船、罗马尼亚的岸上 | 土耳其、德国、西班牙海岸附近的舰船、罗马尼亚和波兰的岸上 | 土耳其、德国、西班牙海岸附近的舰船、罗马尼亚和波兰的岸上 |

来源：Karen Kaya, “NATO Missile Defense and the View from the Front Line” [北约导弹防御和来自前线的观点], Joint Force Quarterly, issue 71 (4th Quarter 2013): 86. 涉及目标捕捉、识别、拦截和数据网络的相关技术挑战，参看 Steven J. Whitmore and John R. Deni, NATO Missile Defense and the European Phased Adaptive Approach: The Implications of Burden Sharing and the Underappreciated Role of the U.S. Army [北约导弹防御和欧洲分阶段调适反导计划：分承负担的影响和美国陆军被忽视的作用], (Carlisle, PA: US Army War College, October 2013), 11-17.

注：荷兰和法国宣布对欧洲弹道导弹防御另拨国家捐助

Aegis Ashore -- “宙斯盾”弹道导弹防御系统的陆基组成部分

AN/TPY-2 (FBM) -- 陆海军 / 移动式雷达监视 2 型 (前进基地模式)

BMD -- 弹道导弹防御

C2BMC -- 指挥、控制、作战管理、通信

ICBM -- 洲际弹道导弹

IRBM -- 中远程弹道导弹

MRBM -- 中程弹道导弹

是一个相对和平的安全社区。如果威慑失败，导弹防御也许会吸引亚洲国家，因为它可以阻止敌人实现攻击目的而加固自身的威慑，也可以限制对方攻击的毁伤程度。美国一些盟国和伙伴的导弹防御也有可能加强基于美国核保护伞的美国安全保证，并因此减少这些国家发展本国核武库的积极性。³⁰

军备裁减：分析

兵力交战模型

2010 年的新削减战略武器条约规定适量减少部署的战略武器和发射装置，该协议建立在早前小布什执政期间美国和俄罗斯之间达成的削减进攻性战略武器条约的基础之上。奥巴马总统在其 2013 年 6 月 19 日的柏林讲话中表明了美国有意在新削减战略武器

条约的基础上，进一步将俄罗斯和美国部署的洲际武器数量再削减约三分之一。³¹

美国和俄罗斯能够安全地迈开这一步吗？即能否从新削减战略武器条约规定的 1550 枚最大限额裁减到大约 1000 枚作战部署在洲际导弹和战略轰炸机上的核弹头，而同时继续保持威慑和军备控制的稳定性？下面的分析使用归纳数字来质疑这个问题。³²模型中对新削减战略武器条约和更低限额兵力结构的预测是根据各方专家的评估，模型进一步测试了双方核交战的结果。³³

图 1 和 2 总结了美 / 俄战略核交战的结果，其假设按照新削减战略武器条约的限额，即每个国家在洲际发射装置上作战部署 1550 枚或 1000 枚核弹头。图 1 显示每个国家在 1550 枚武器部署限额之下，可以生存并用于

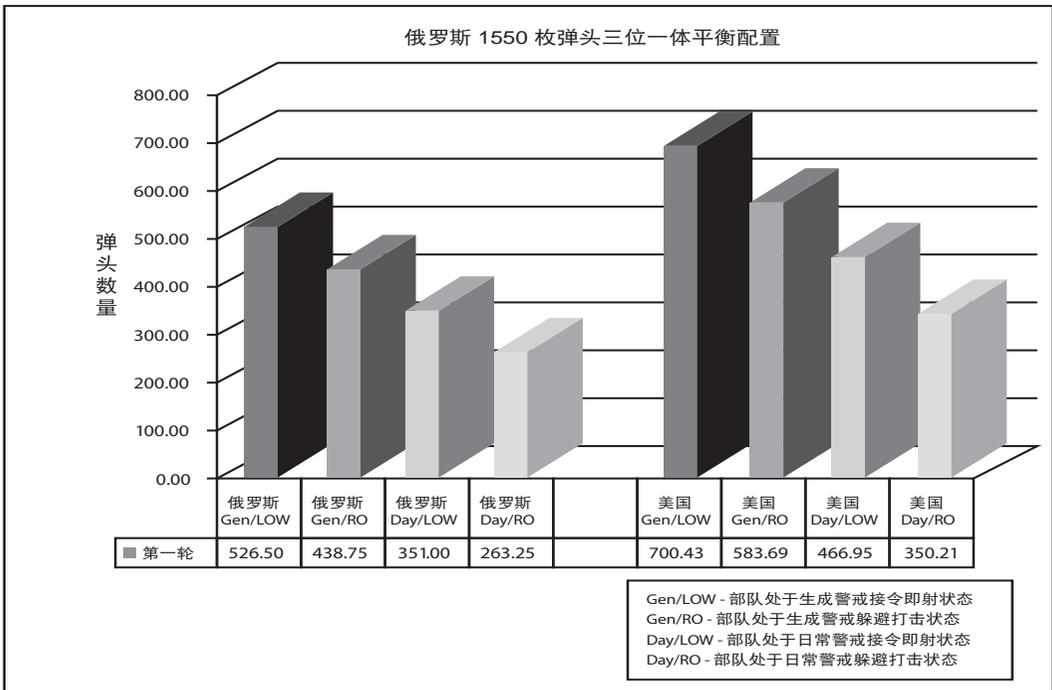


图 1：美 / 俄各自生存报复弹头数量 (1,550 枚部署限额)

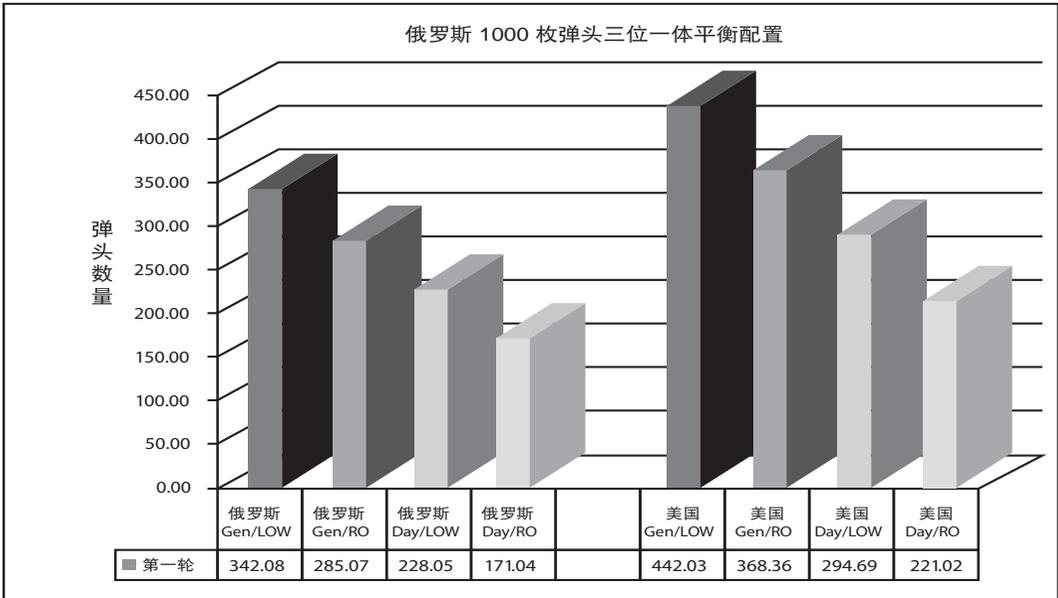


图 2：美 / 俄各自生存报复弹头数量 (1,000 枚部署限额)

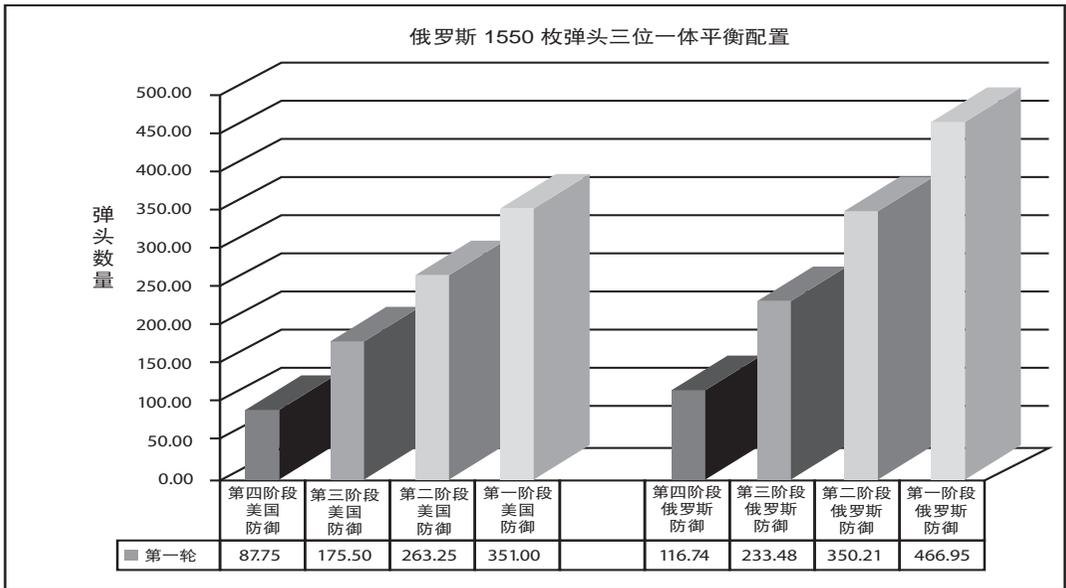


图 3：美 / 俄防御状态下各自生存报复弹头与防御对照 (1550 枚部署限额)

二次打击和报复的弹头数量。图 2 表现 1000 件部署武器限额下的类似数据。在图 3 和图 4 中，我们分别把反导和防空（结合起来）

能力引入每个国家的等式中，从而得出四个防御阶段拦截二次打击报复武器的表现范围及其变化：对于二次打击报复弹头，第一阶

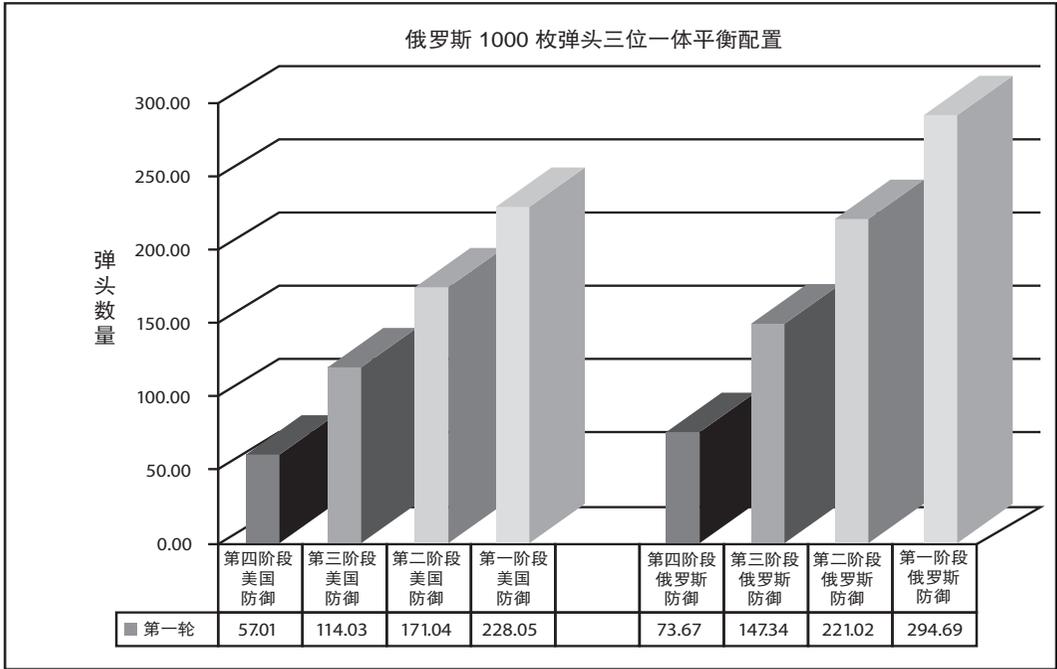


图 4：美 / 俄防御状态下各自生存报复弹头与防御对照 (1000 枚部署限额)

段成功拦截至少 20%；第二阶段至少 40%；第三阶段至少 60%；第四阶段至少 80%。

结果和影响

以上各图似乎表明：每个国家拥有的生存报复武器的数量，足可达到二次打击造成“无法承受的损失”这个按传统的美国政治和军事标准界定的标杆。³⁴ 然而，传统威慑模型赖以为基础的逻辑性或合理性原本属于假设，而这种假设可能误导。基斯·佩恩 (Keith B. Payne) 在为一种更经验主义的威慑法辩护时指出：

我们企图熟悉外国领导人的决策思维方式和变化，并企图在知情基础上建立威慑结构来胁迫他们就范，这项努力绝非易事。并且，我们必须认识到，即使我们付出了大量努力来获取有关对手决策

所依据的种种因素的情报，也不能排除对手基于各种我们并不熟悉或全然费解的动机、目的或价值观而不按常理出牌，做出种种无法预测的行为。³⁵

例如有些专家已经提出：提高投送核武器和常规武器的精确度，也许会导致美国 and 俄罗斯之外的其他一些国家，包括拥核国家，重视建设反击军事力量的战略。³⁶ 另一些研究人员则警告说：即使发生了规模上完全达不到美俄核大战的小型核战争，例如未来以色列和伊朗之间的核冲突，也能对双方造成史无前例的、社会上无法收拾的后果（此外还有对该区域其它各方的不确定的附带后果。）³⁷

如此，包括网空武器在内的非核武器对在攻击者的吸引力，部分源自对这些武器的推定能力，即“精算欺骗”和“精确杀伤”

相结合的能力。对于这一点，俄罗斯副总理罗戈津警告说：信息武器正成为打击敌人政治、军事和工业中心的第一波攻击武器。他并声称：五角大楼的计算机推演表明，由大约 3000-4000 枚精确制导武器发起的攻击能摧毁俄罗斯多达 80-90% 的核潜力。³⁸ 当然，美国对俄罗斯的这种规模的攻击和俄罗斯可能做出的反应，将破坏欧洲和欧亚中部大部分地区的政治稳定和经济生存能力，更不必说对这两国领土分别造成的破坏。威慑失败仍然是一条要全力避开的死胡同；所谓相对优势只是一个残忍的骗局。

对奥巴马政府的另一个挑战，是其追求的目标之间可能发生冲突：即一方面想实现全球无核化并减少核武器在美国军事战略中的作用；另一方面又鼓吹提升自身先进常规武器，包括导弹防御和用于全球精确打击的进攻性武器。比如，中国据称奉行最低威慑，其部署的战略武器在数量上是假定能相对于美国确保最小程度的二次打击能力，但如果美国加强了导弹防御和 / 或全球精确打击武器，中国的假定最低二次打击态势就会感到威胁。³⁹ 再者，如前所述，俄罗斯也警告说，名义上针对伊朗的美国导弹防御最终可能对俄罗斯的战略核威慑构成威胁。⁴⁰

结语

核武器如今成为后冷战时代的怪物，因为它们已经游离在美苏全球对抗竞争的初衷之外。这些武器，以其瞬间大规模杀伤并引发长期致命效果的独特能力，仍然令人敬畏。然而，制定国家战略和开展核威慑、武控和裁军政策分析的环境，已经发生了深刻变化——并且将继续出现更大变化。最明显的变化是在技术领域，但是其影响超出技术本身。进攻性打击平台的多样化、反导和防空

能力的改进，以及网空重要性的不断提升，包括进攻性和防御性信息战的重要性等，交织汇聚，可能促成思维模式的转变，引发对先进国家之间大型战争的重新思考。以上讨论最多也只是涉及了这种建构性变化的表面。

核 / 网时代的一个悖论是：核大国拥有互相威慑对方的强大能力，于是无来由地沾沾自喜，而忽视下一层级的地区性核威慑，尤其是中东、南亚、东亚地区的拥核国或有志拥核国之间。⁴¹ 欧洲以外的多极拥核国体系正产生潜在不稳定性，它将挑战当前威慑观所依据的推理逻辑以及防扩散体系的持久性。美国和盟军制定核危机应对计划时，将不得不考虑以往战争推演中没有描述过的但可能出现的设想情景，包括无法确定某些国家究竟是否已经动“核”。⁴² 由于这些原因，本文提供的二维分析，即对美俄两国的核互动分析，不可避免且必然地搭接到也是这种互动之一部分的新兴的多极拥核国体系。不过，现在美国和俄罗斯已经不同于冷战中的美国和苏联，现在的这两个国家有激励因素也有机会来追求多层次的系统危机管理和共同的防扩散目标，而不必自缚于臆想的敌对意识形态。该系统“预设”为鼓励各相关地区更积极参与禁核努力，以及（希望如此）多边武器削减，其成就将超越新削减战略武器条约和所有后续协议所取得的成果。

进攻性核力量裁减和导弹防御（无论有或无网空参与）之间的关系是复杂的。导弹防御技术和上世纪相比已然更加先进。然而专家的研究表明：反弹道导弹防御系统只对地区性敌对国家的小型攻击更加有效，作为战略对抗手段来应对大规模远程导弹攻击则远谈不上有效。⁴³ 北约和俄罗斯在导弹防御方面有安全合作的空间，以共同对付可能由中东或其它核国家构成的威胁。但是，核武

器在中东的传播或在亚洲的进一步扩散，其影响不可能仅仅靠导弹防御或者甚至只靠军事反应来排除。灵巧外交和有限区域导弹防

御并用，也许能争取一些时间，以利推动扩散和反扩散努力的更宏大目标，并收到成效。⁴⁴ ♣

注释:

1. Freeman Dyson, *Weapons and Hope* [武器与希望], (New York: Harper and Row, 1984), 223-38.
2. 据信息安全及情报专家 Joel Brenner 说，美国军工体系是世界上“最肥的间谍靶子”，而且外部对我们国家防务机构的攻击是“持续不断、不屈不挠、来自四面八方、且新老手段并用。”参看 Brenner, *Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World* [玻璃房：透明世界里的隐私、保密和网空不安全感], (New York: Penguin Books, 2013), 73.
3. Thomas M. Chen, *An Assessment of the Department of Defense Strategy for Operating in Cyberspace* [国防部网空作战战略评估], (Carlisle Barracks, PA: Strategic Studies Institute, US Army War College, September 2013), 第 9-10 页及通篇各处。
4. 有关这一主题富有洞察力的分析包括 Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* [明白网空力量的战略意义：天为什么没有塌?], (Carlisle Barracks, PA: Strategic Studies Institute, US Army War College, April 2013); 另参看 Kamaal T. Jabbour and E. Paul Ratazzi, “Does the United States Need a New Model for Cyber Deterrence?” [美国需要新的网空威慑模型吗?], 收录于 *Deterrence: Rising Powers, Rogue Regimes, Terrorism in the Twenty-First Century* [威慑：二十一世纪的新兴大国、流氓政权和恐怖主义], ed. Adam B. Lowther (New York: Palgrave-Macmillan, 2012), 33-45; 另参看 Martin C. Libicki, *Cyberdeterrence and Cyberwar* [网空威慑与网空战], (Santa Monica, CA: RAND, 2009). 关于这个主题的其他引用资料在后面的注释中继续列明。有关网空和美国国家安全战略的重要政府文件的年表，以上注释 3 中 Chen 文的附录即第 45-46 页里有很好的总结。
5. 关于主要大国的信息作战概念，见 Timothy L. Thomas, *Cyber Silhouettes: Shadows over Information Operations* [网空剪影：笼罩信息作战的阴影], (Ft. Leavenworth, KS: Foreign Military Studies Office, 2005), 第 5-6、10、14 章以及全文各处；另参看 Pavel Koshkin, “Are Cyberwars between Major Powers Possible? A Group of Russian Cybersecurity Experts Debate the Likelihood of a Cyberwar Involving the U.S., Russia or China” [主要大国间有无网空战可能？一组俄罗斯网空安全专家辩论有美、俄、中卷入的网空战的可能性], *Russia Direct*, 1 August 2013, <http://russia-direct.org>, 收录于俄罗斯信息集锦 -2013, 143 (6 August 2013), davidjohnson@starpower.net.
6. 网空武器并不一定能有效地用作产生战役战术或战略效果的使能工具。参看 Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* [网空中的征服：国家安全和信息战] (Cambridge, UK: Cambridge University Press, 2007), Chaps 4-5.
7. 批评美国最低核威慑建议的专家文章见 Dr. Keith B. Payne, study director, and Hon. James Schlesinger, chairman, Senior Review Group, *Minimum Deterrence: Examining the Evidence* [最低威慑：审查证据], (Fairfax, VA: National Institute for Public Policy, National Institute Press, 2013). 赞成最低威慑前景的专家评论评见 James Wood Forsyth Jr., Col B. Chance Saltzman, and Gary Schaub Jr., “Remembrance of Things Past: The Enduring Value of Nuclear Weapons” [回忆往事：核武器的持久价值], *Strategic Studies Quarterly* 4, no. 1 (Spring 2010): 74-90.
8. 美国网空司令部为抵抗对计算机网络和其它目标的攻击而计划建造的相当于“星球大战”的网空防御，可能会在国家安全局监视做法上的政治争议所耽误或转向。参看 David E. Sanger, “N.S.A. Leaks Make Plan for Cyberdefense Unlikely” [国家安全局的泄露可能使网空防御计划泡汤], *New York Times*, 12 August 2013, <http://www.nytimes.com/2013/08/13/us/nsa-leaks-make-plan-for-cyberdefense-unlikely.html>.
9. “Putin Calls to Strengthen Protection against Cyber Attacks” [普京呼吁加强对网空攻击的防御], *Itar-Tass*, 5 July 2013, 收录于 *Johnson's Russia List 2013* [俄罗斯信息集锦 -2013], no. 122, 5 July 2013, davidjohnson@starpower.net.
10. Jonathan Earle, “U.S. and Russia Sign New Anti-Proliferation Deal” [美俄签署新反扩散协议], *Moscow Times*, 19 June 2013, 收录于 *Johnson's Russia List 2013* [俄罗斯信息集锦 -2013], no. 111 (19 June 2013), davidjohnson@starpower.net.
11. Clifford S. Magee, “Awaiting Cyber 9/11” [等待网空 9/11], *Joint Force Quarterly*, issue 70 (3rd Quarter 2013): 76.
12. Dr. Panayotis A. Yannakogeorgos and Dr. Adam B. Lowther, “Saving NATO with Airpower” [以空中力量拯救北约], *Royal Canadian Air Force Journal* 2, no. 1 (Winter 2013): 70.

13. 例如, 参看注释 3 中 Chen 文, 10-11; 注释 2 中 Brenner 文, 尤其是第 6-7 章; 另参看 Timothy L. Thomas, *Three Faces of the Dragon: Cyber Peace Activist, Spook, Attacker* [网龙三面: 网空和平主义者、幽灵、攻击者], (Ft. Leavenworth, KS: Foreign Military Studies Office, 2012); 另参看 Timothy L. Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology through Toughness* [重塑红星: 以坚韧锻造的俄罗斯传统和技术], (Ft. Leavenworth, KS: Foreign Military Studies Office, 2011); 另参看 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), <http://www.defense.gov/news/d20110714cyber.pdf>; 另参看 White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* [国际网空战略: 联网世界的繁荣、安全和开放], (Washington, DC: White House, May 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; 另参看注释 4 中 Colin S. Gray 文第 8 页; 另参看 Robert A. Miller, Daniel T. Kuehl, and Irving Lachow, "Cyber War: Issues in Attack and Defense" [网空战: 攻击和防御方面的问题], *Joint Force Quarterly*, issue 61 (2nd Quarter 2011), 18-23; 另参看注释 4 中 Libicki 文; 另参看 P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century* [联网作战: 第 21 世纪的机器人革命与冲突], (New York: Penguin Books, 2009); 另参看 John Arquilla, *Worst Enemy: The Reluctant Transformation of the American Military* [顽敌: 阻力重重的美军转型], (Chicago: Ivan R. Dee, 2008), 主要在第 6-7 章; 另参看注释 6 中 Libicki 文, 主要在第 15-31 页。
14. 见注释 13 中 Miller, Kuehl, and Lachow 文。
15. 见注释 2 中 Brenner 文, 第 3 页。
16. 以 Stuxnet “震网” 病毒攻击伊朗核计划之一部分的离心机, 这就是此类攻击的一个例子。据报道, 伊朗 5000 台离心机之中大约有 1000 台受到美国和以色列网空攻击而短时瘫痪, 这是被称作“奥运会”的美国计划的一部分, 该计划在小布什执政时开始并继续到奥巴马政府。参看 David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran" [奥巴马命令加速针对伊朗的网空攻击浪潮], *New York Times*, 1 June 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0.
17. 见注释 13 中 Miller, Kuehl, and Lachow 文, 第 19 页。这些目标中有些也许还可能通过网空中的“友好征服”而非“敌对征服”来实现。参看注释 6 中 Libicki 文关于对立的定义, 第 125-26 页; 相关的讨论还可见第 6 章的其它部分。
18. Patrick M. Morgan, "The State of Deterrence in International Politics Today" [当今国际政治领域的威慑状况], *Contemporary Security Policy* 33, no. 1 (April 2012): 85-107, 作者尤其在 101-103 页中讨论了重申威慑理论与实践与网空安全之间的关系。
19. 见注释 4 种 Gray 文, 第 36 页。
20. Adam B. Lowther 认为, 威慑可以被概念化为由三部分组成的连续频谱: 以劝阻威慑、以拒止威慑、以威胁威慑。行使威慑的国家从频谱的一端移向另一端, 从劝阻到拒止又到威胁, 逐步提高威慑行动的级别。见 Lowther, "How Can the United States Deter Nonstate Actors?" [美国能如何威慑非国家行为体?], 具体讨论参看注释 4 中 Lowther 主编的论文集 163-182 页, 尤其是 166-167 页。
21. Desmond Butler, "Flaws Found in U.S. Missile Shield for Europe" [在美国的欧洲导弹防御系统中发现缺陷], *Army Times*, 9 February 2013, <http://www.armytimes.com/article/20130209/NEWS/302090305/Flaws-found-in-U-S-missile-shield-for-Europe>; 另参看 "US Missile Defense Shield Flawed—Classified Studies" [美国导弹防御系统存在漏洞—机密研究], *Russia Today*, 11 February 2013, <http://rt.com/usa/us-missile-defense-flaws-811/>.
22. National Research Council, *Making Sense of Ballistic Missile Defense: An Assessment of Concepts and Systems for U.S. Boost-Phase Missile Defense in Comparison to Other Alternatives* [确立弹道导弹防御的意义: 评估美国助推段导弹防御概念和系统并与其他选择相比较], (Washington, DC: National Research Council, National Academy of Sciences, National Academies Press, 2012), <http://www.nap.edu>.
23. George N. Lewis and Theodore A. Postol, "The Astonishing National Academy of Sciences Missile Defense Report" [令人惊讶的国家科学院导弹防御报告], *Bulletin of the Atomic Scientists*, 20 September 2012, <http://thebulletin.org/astonishing-national-academy-sciences-missile-defense-report-0>.
24. Rebecca Slayton, *Arguments That Count: Physics, Computing, and Missile Defense, 1949-2012* [有意义的争论: 物理、计算和导弹防御, 1949-2012], (Cambridge, MA: MIT Press, 2013).
25. Steven J. Whitmore and John R. Deni, *NATO Missile Defense and the European Phased Adaptive Approach: The Implications of Burden Sharing and the Underappreciated Role of the U.S. Army* [北约导弹防御和欧洲分阶段调适反导计划: 责任分担和美国陆军被低估的作用之影响], (Carlisle Barracks, PA: Strategic Studies Institute and US Army War College Press, October 2013), 作者在这篇文章中较好地论述了美国和北约欧洲导弹防御计划面临的技术、政治和经济挑战。

26. 关于美国和北约导弹防御计划, 参看 LTG Patrick J. O'Reilly, USA, director, Missile Defense Agency, "Ballistic Missile Defense Overview" [弹道导弹防御概观], 12-MDA-6631 (briefing presented to the 10th Annual Missile Defense Conference, Department of Defense, Washington, DC, 26 March 2012), <http://mostlymissiledefense.files.wordpress.com/2013/06/bmd-update-oreilly-march-2012.pdf>.
27. Treaty between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms [美国和俄罗斯就进一步削减和限制战略进攻性武器措施的条约], (Washington, DC: Department of State, 8 April 2010), <http://www.state.gov/documents/organization/140035.pdf>.
28. 奥巴马政府主导的导弹防御分阶段调适方案将保留并提高小布什执政期间部署的某些技术, 但会把重点转向其它由改进的作战管理指挥、控制、通信 (BMC3) 系统和发射检测与跟踪所支持的拦截器。参看 Karen Kaya, "NATO Missile Defense and the View from the Front Line" [北约导弹防御和来自前线的看法], Joint Force Quarterly, issue 71 (4th Quarter 2013), 84-89; 另参看 John F. Morton and George Galdorisi, "Any Sensor, Any Shooter: Toward an Aegis BMD Global Enterprise" [任何传感器、任何发射器: 向宙斯盾弹道导弹防御全球体系发展], Joint Force Quarterly, issue 67 (4th Quarter 2012), 85-90; 另参看 Frank A. Rose, deputy assistant secretary, Bureau of Arms Control, Verification and Compliance, "Growing Global Cooperation on Ballistic Missile Defense" [弹道导弹防御领域的全球合作不断发展], (remarks as prepared, Berlin, Germany, 10 September 2012), <http://www.state.gov/t/avc/rls/197547.htm>.
29. 例如, 可参阅 "Moscow Needs More 'Predictability' in NATO Missile Defense Plans" [莫斯科需要北约导弹防御计划中更大的“可预测性”], RIA Novosti, 23 October 2013, 收录于 Johnson's Russia List 2013 [俄罗斯信息集锦 -2013], no. 191 (24 October 2013), davidjohnson@starpower.net.
30. 相关的讨论, 参看 Dr. Adam Lowther 主编的 The Asia-Pacific Century: Challenges and Opportunities [亚太世纪: 挑战和机遇], (Maxwell AFB, AL: Air University Press, Air Force Research Institute, April 2013).
31. Peter Baker and David E. Sanger, "Obama Has Plans to Cut U.S. Nuclear Arsenal, if Russia Reciprocates" [奥巴马计划削减美国核武库, 如果俄罗斯也这样做的话], New York Times, 18 June 2013, http://www.nytimes.com/2013/06/19/world/obama-has-plans-to-cut-us-nuclear-arsenal-if-russia-reciprocates.html?_r=0; 另参看 Roberts Rampton and Stephen Brown, "Obama Challenges Russia to Agree to Deeper Nuclear Weapon Cuts" [奥巴马挑战俄罗斯同意进一步削减核武器], Reuters, 20 June 2013, 收录于 Johnson's Russia List 2013 [俄罗斯信息集锦 -2013], no. 212 (20 June 2013), davidjohnson@starpower.net.
32. 图 1-4 是以 Dr. James J. Tritten 最初研发的一个模型为基础改动而成, 笔者特致感谢。对本文插图或文字的任何争论或意见, Dr. James J. Tritten 不承担任何责任。
33. 该分析中的兵力结构是概念性的, 并非一定能预测实际部署。关于专家鉴定, 参看 Hans M. Kristensen, Trimming Nuclear Excess: Options for Further Reductions of U.S. and Russian Nuclear Forces [修剪过剩核力量: 进一步缩减美俄核力量的备选方案], Special Report no. 5 (Washington, DC: Federation of American Scientists, December 2012), <http://www.fas.org/programs/ssp/nukes/publications1/TrimmingNuclearExcess.pdf>; 另参看 Gen James Cartwright, retired, chair, Global Zero U.S. Nuclear Policy Commission Report: Modernizing U.S. Nuclear Strategy, Force Structure and Posture [美国核政策委员会全球零核报告: 使美国核战略、兵力结构和态势现代化], (Washington, DC: Global Zero, May 2012), http://www.globalzero.org/files/gz_us_nuclear_policy_commission_report.pdf; 另参看 Pavel Podvig, "New START Treaty in Numbers" [新削减战略武器条约中的数字], Russian Strategic Nuclear Forces (blog), 9 April 2010, http://russianforces.org/blog/2010/03/new_start_treaty_in_numbers.shtml; 另参看 Joseph Cirincione, "Strategic Turn: New U.S. and Russian Views on Nuclear Weapons" [战略转变: 美国和俄罗斯关于核武器的新观点], New America Foundation, 29 June 2011, http://newamerica.net/publications/policy/strategic_turn; 另参看 "U.S. Strategic Nuclear Forces under New START" [新削减战略武器条约约束下的美国战略核力量], Arms Control Association, July 2013, <http://www.armscontrol.org/factsheets/USStratNukeForceNewSTART>.
34. 某些专家认为, 美国只需要在洲际发射架上部署不足 400 枚弹头就能满足战略核威慑需要。参看 James Wood Forsyth Jr., B. Chance Saltzman, and Gary Schaub Jr., "Minimum Deterrence and Its Critics" [最低威慑及其批评言论], Strategic Studies Quarterly 4, no. 4 (Winter 2010), 3-12. 反驳意见参看注释 7 中 Payne and Schlesinger 文, 尤其是第 65-70 页。
35. Keith B. Payne, The Fallacies of Cold War Deterrence and a New Direction [冷战威慑的悖论和新方向] (Lexington: University Press of Kentucky, 2001), 101.
36. 例如, 可参看 Keir A. Lieber and Daryl G. Press, "The New Era of Nuclear Weapons, Deterrence, and Conflict" [核武器、威慑和冲突的新时代], Strategic Studies Quarterly 7, no. 1 (Spring 2013): 3-14.

37. Cham E. Dallas et al., “Nuclear War between Israel and Iran: Lethality beyond the Pale” [以色列和伊朗之间的核战争：难以承受的致命打击], *Conflict and Health*, 10 May 2013, <http://www.conflictandhealth.com/content/7/1/10>; 另参看 Anthony H. Cordesman, *Iran, Israel, and Nuclear War: An Illustrative Scenario Analysis* [伊朗、以色列、核战争：一种说明性情景分析], (Washington, DC: Center for Strategic and International Studies, 19 November 2007), http://csis.org/files/media/csis/pubs/071119_iran.is&nuclearwar.pdf; 另参看 US Congress, Office of Technology Assessment, *The Effects of Nuclear War* [核战争的后果], (Washington, DC: Government Printing Office, May 1979), 其中 27-44 页包含单一城市遭受核打击的案例研究。此报告部门警告说, 即使一场小型或有限的核攻击也会造成“巨大的”后果 (p.4)。
38. Ilya Maksimov and Sergey Kuksin, “Russia Will Not Be a Bystander in the Arms Race” [俄罗斯不会是军备竞赛的旁观者], *Rossiyskaya Gazeta*, 28 June 2013, 收录于 Johnson's Russia List 2013 [俄罗斯信息集锦 -2013], no. 122 (5 July 2013), davidjohnson@starpower.net.
39. Lora Saalman, “How Chinese Analysts View Arms Control, Disarmament, and Nuclear Deterrence after the Cold War” [中国分析家如何看待冷战之后的军备控制、裁军和核威慑], 收录于 *Engaging China and Russia on Nuclear Disarmament* [推动中国和俄罗斯参加核裁军], Occasional Paper, no. 15, ed. Cristina Hansell and William C. Potter (Monterey, CA: James Martin Center for Nonproliferation Studies, April 2009), 47-71.
40. 关于奥巴马核裁军目标与先进常规武器现代化目标之间可能出现的冲突, 进一步讨论参看 Andrew Futter and Benjamin Zala, “Advanced US Conventional Weapons and Nuclear Disarmament: Why the Obama Plan Won't Work” [美国先进常规武器与核裁军：奥巴马计划为何行不通?], *Nonproliferation Review*, 20, no. 1 (2013): 107-22, <http://dx.doi.org/10.1080/10736700.2012.761790>.
41. Paul Bracken, *The Second Nuclear Age: Strategy, Danger, and the New Power Politics* [第二个核时代：战略、危险和新强权政治], (New York: Henry Holt, 2012), 主要在 215-220 和 267-270 页。关于第二个核时代的更多辩论, 参看注释 4 中 Adam Lowther 主编的 *Deterrence: Rising Powers* [威慑：崛起的大国]; 另参看 Paul K. Davis, *Structuring Analysis to Support Future Decisions about Nuclear Forces and Postures* [以结构性分析支持核力量与核态势的未来决定], Working Paper WR-878-OSD (Santa Monica, CA: RAND National Defense Research Institute, September 2011); 另参看 Michael Krepon, *Better Safe Than Sorry: The Ironies of Living with the Bomb* [小心为妙：与炸弹共存的讽刺], (Stanford, CA: Stanford University Press, 2009), 94-132; 另参看 Colin S. Gray, *The Second Nuclear Age* [第二个核时代], (Boulder, CO: Lynne Rienner Publishers, 1999).
42. 关于这方面一些有意思的可能性, 参看 George H. Quester, *Nuclear First Strike: Consequences of a Broken Taboo* [第一次核打击：打破禁忌的后果], (Baltimore: Johns Hopkins University Press, 2006), 24-52, 尤其是第 25-30 页。此文作者正在撰写另一篇文章“Anticipatory Attack” [预防性攻击], 其中展现对一些多极拥核强权模型的路试发现。
43. 见注释 22 中 National Research Council 文。
44. 第二个核时代中的不稳定性来源将包括主要强国、次级强国和一些团体, 它们在多极核系统之内大国竞争的覆盖下, 有时创造性地在战争边缘政治性玩弄核武器。参看注释 41 中 Bracken 文, 主要在第 93-126 页; 另参看 James E. Goodby, “The End of a Nuclear Era” [一个核时代的终结], *New York Times* 14 August 2013, http://www.nytimes.com/2013/08/15/opinion/global/the-end-of-a-nuclear-era.html?_r=0; 另参看 C. Dale Walton and Colin S. Gray, “The Geopolitics of Strategic Stability: Looking Beyond Cold Warriors and Nuclear Weapons” 战略稳定的地缘政治：超越冷战勇士和核武器看问题], 收录于 *Strategic Stability: Contending Interpretations*, [战略稳定性：多元观点汇总], ed. Elbridge A. Colby and Michael S. Gerson (Carlisle Barracks, PA: Strategic Studies Institute and US Army War College Press, 2013), 85-115.



斯蒂芬·森巴拉博士 (Dr. Stephen J. Cimbala), 宾夕法尼亚州立大学文学士, 威斯康星大学麦迪逊校区文科硕士、哲学博士, 现为宾夕法尼亚州立大学 Brandywine 校区政治学杰出教授, 在美国国家安全、核武器控制及其它领域著述颇丰。他是宾夕法尼亚州立大学获奖教师, 最新出版著作有《应对不确定性的武器: 美国与俄国安全政策中的核武器》(Ashgate, 2013 年) 及与 Sam C. Sarkesian 和 John Allen Williams 合著的《美国国家安全: 政策制定者, 过程与政治》(Lynne Rienner, 2013 年)。

从公共健康角度分析向太阳发射核废料的可行性

Public Health Considerations of Launching Nuclear Waste to the Sun

默里·贝科威茨博士 (Dr. Murray R. Berkowitz)

本文从保护公共健康的角度出发，分析把放射性核废料射向太阳的处置方案。自2010年4月20日英国石油公司在墨西哥湾发生漏油事件以来，所引起的环境和生态问题激起了关于寻找替代能源的讨论。2010年5月11日，时任马萨诸塞州民主党参议员约翰·克里 (John Kerry) 和康涅狄格州独立党派参议员约瑟夫·利伯曼 (Joseph Lieberman) 提出了一项立法议案，即“美国能源法”，旨在“确保美国的能源未来，奖励国内清洁能源技术的开发，实现意义深远的污染减排。”¹ 核能，作为许多替代能源形式的一种，重新唤起了人们更大的兴趣。然而，2011年3月15日发生的九级地震以及随后的海啸对日本福岛第一核电站造成的破坏，还有报道称“艾琳”飓风引发的美国东海岸几处核电站的问题，都加剧了人们对核电安全与健康的担忧。此外，在2012年10月29日“桑迪”超级风暴袭击美国东海岸之后造成停电灾难后，媒体发表了一系列有关核电厂危及公共健康的文章。

核废料释放“电离辐射”，因此对公众健康构成一种危害，危害程度取决于辐照持续时间的长短、距离辐射源的远近、辐射的类型 (α , β , γ 射线等)，以及是否有任何形式的防辐射保护等情况。² 放射性核废料的来源包括：核武器、核发电厂、用于诊断或治疗的医用放射性核素、产生辐射的机器、放射性金属和各种元素的放射性同位素（通常发现于“背景辐射”中）。³

辐照的威胁主要产生于导致放射性核物质泄漏（即“核泄漏”）的核事故或事件，它通常危及不到（未受保护的）普通人群。目

前通行的处置方法是把放射性核材料收集并封存于安全地点，它要求安全的运输及配有特殊安全设施的存放地。这些存放地必须远离人口居住区，存放设施外有可靠的物理安全保护，擅自（有意或无意）进入设施的可能性极小，也极容易被发现（例如尤卡山核废料贮存库，2010年弃用）；这些存放地还需选在极少有地震、火山爆发等地质不稳定现象的地区。

另一种处置方法是将放射性核废料掩埋在大洋底下，尤其是大洋中山脉的深缝隙里，或像马里亚纳海沟等极深的地质层中。显然，任何深海埋藏方案都要求远离海洋构造板块接合部——较易发生火山、地震或其他地质活动的部位。按查尔斯·霍利斯特 (Charles Hollister) 和史蒂夫·纳迪斯 (Steven Nadis) 的说法，海洋科学家们认为：这样的地方在过去五千多万年内未曾经历过地质活动，那么未来也不太可能会发生这种情况。⁴

过去已有人提出把放射性核废料射向太阳的处置建议，认为这种方法能消除存储设备泄漏或核废料被核恐怖分子盗走而引发的辐射威胁。⁵ 该建议所依据的原理是：任何物质进入太阳的引力场，就会在其强大的向心压力下解构，在抵达太阳之前“分裂”。而且，所有物质在抵达日冕之前都将被高温焚化并彻底消耗掉。⁶ 具体而言，物质随着温度升高而膨胀，其结构完整性被打破，热能造成分子键断裂。在太阳上，凡是原子序数超过二（即氦）的元素，其原子完整性都不存在。⁷ 本质上，极热使这些元素都分解成了构成这些元素的亚原子粒子（如电子、质子、中子，等等）。⁸ 如此，放射性核废料绝不会

影响到太阳,对其“生态系统”没有任何影响,因此不可能“损害”太阳。

问题的严重性

然而,就公共健康风险而言,人们必须考虑到发射的事故可能性,比如运载火箭在脱离地球引力之前爆毁,或者在发射后不久爆炸而散落放射性碎片。回顾美国的无人航天计划历史,应能了解发生此类事故的可能性有多大。宇宙神、半人马座、德尔塔、德尔塔 II、土星 5 等运载火箭,已执行过一千多次任务,也发生过事故,事故产生的残骸碎片尺寸从几厘米到几米不等,但都不是放射性物质。在无人航天器发射历史中,涉及运载火箭事故的概率不到百分之三。⁹ 这个概率风险虽低,但确实存在。

我们很早就认识到了电离辐射对健康的危害。在日本广岛和长崎上空爆炸的原子弹、美国及前苏联在 1946 年到 1964 年期间进行的原子弹和氢弹大气层试验、1979 年三里岛核反应堆事故、1986 年切尔诺贝利核电站事故,等等,其所造成的短期和长期健康问题都历历在案。载运放射性废料的运载火箭所涉及的风险,可以与在《禁止核武器试验条约》签订之前大气层核爆炸试验中观察到的核物质散落所涉及的风险相比。

主要决定因素

上面谈到,造成潜在公共健康问题的原因已为公众所熟知。具体说,就是放射性核废料环境对生命有机体的生物效应。电离辐射会破坏维持所有生命的生化、分子及细胞结构。人类行为对这个问题没有直接影响;但是在当前的国际地缘政治环境中,它可能会间接地影响到人们对于处理或封存放射性核废料的安全和/或防护的担忧。也就是说,我们必须考虑这种可能性,即这种物质也许

会落入恐怖组织之手,他们可能会用这些材料来制造和部署低当量“肮脏”核武器(即核恐怖主义)。

制定政策并确定优先顺序

重述一下,我们可以有两种处置放射性核废料的办法:(1)送入太空;(2)收集、隔离、封存于地面之上/之下或葬入海洋深处。如果把废物送入太空,尤其是射向太阳(废物会在抵达日冕之前焚化),就能一劳永逸地根除隐患。虽然,如前所述,这一选择会造成运载火箭发射费用,其本身也存在发射事故的风险;一旦发生事故,放射性碎片可能散落在广大地区上空且无法预测。把放射性核废料进行收集、隔离、并封存于地球的陆地之内或之上,这种方法在初始运作和后勤保障方面简单易行且费用低廉,但是需要持续的监控和保安,以防恐怖组织盗窃并用于邪恶目的。再者,放射性废物的封存可能遭受自然灾害(例如地震、火山爆发等)的破坏,从而渗入地下水中,污染地面和/或水源。而把核废料葬于海洋深处的做法,可能和送入太空一样耗资。海洋事故可能会使近人口居住区的海洋、捕鱼区等地区容易遭受放射性污染。此外,虽说大洋深处比陆基封存设施更难抵达,但恐怖分子仍有可能威胁其安全并盗出这些放射性物质。再者,这样的设施也将需要持续监控和保安。

无论如何,我们拥有实施上述各种处置方法的科技能力,包括能把核废料载荷发射到太空中的任何目标。¹⁰ 实施中遇到的政治和社会行为障碍,产生于公众对核能生产、使用、副产物等相关风险的认知;事实上,这种风险并非像多数民众想象的那样大。¹¹ 没有发布的研究结果能证明,在遵守适当保护措施的前提下,核业界人员的健康亚于普通大众;但是,如果不遵守安全操作措施、

或发生了涉及核材料的事故或事件，公众健康就会遭到损害，尤其是在致癌方面。

至于经济方面的考虑，向太空发射有效载荷的成本约为每磅 1 万美元。¹² 向太空每发送 100 吨放射性核废料要花费 22 亿美元，而将其封存于尤卡山设施的费用大约是每年 2 亿美元。¹³ 如此算来，11 年的费用就可以完全抵消一次太空发射的费用，而一次太空发射所能处置的核废料要比在地球上一个地点的存放量大得多。

太空处置放射性核废料的方法有益于全球范围的个人、社区和整个社会，因为这种做法消除了这些物质在地球上封存期间发生事故 / 事件或被恐怖分子盗用的可能性。如前所述，太空发射的附带风险，涉及在发射之际或紧随发射、或者过后在离开大气层之前可能发生的事件。显然，在发射之际或稍后发生的事故会影响发射地点下风处的邻近社区（例如佛罗里达州墨尔本、卡纳维拉尔角附近和帕特里克空军基地），放射性碎片在这些地区会迅速积聚并危及公众健康。据约翰霍普金斯大学的一份新闻发布稿说：

由事故或恐怖主义所产生的核放射微粒沉降含有可致甲状腺癌的放射性碘，它尤其会危害婴儿和 18 岁以下的儿童。碘化钾片能防止甲状腺吸收放射性碘，从而保护腺体。

“由核事件引发的甲状腺癌历来是个重大公共健康问题，这些事件包括对日本长崎的轰炸和乌克兰切尔诺贝利核事故，”约翰霍普金斯大学内分泌及代谢科主任保罗·莱迪逊（Paul W. Ladason）医学博士如是说。¹⁴

防护计划呼吁对住在核事件地点 20 英里范围内的居民发放碘化钾片。

如果核事故发生在高层大气，高空风和喷气流会将放射性碎片吹散，并影响到人口居住区域，受影响区域的数量和位置取决于事故是发生在北半球还是南半球。此外，核碎片会扰乱海洋生物和商业。现实地说，这种不太可能发生的事故所产生的影响，不会比前面提到的任何大气核弹试验的结果更糟糕——一次大气核弹试验势必要引爆有数百万吨级爆炸力的核武器，这些武器产生大量尘埃形式的放射性碎片。而我们在此讨论的核废料总量并不属于“百万吨级”范畴。

相关风险评估

多项风险评估（又称环境评估）都直接关系到核材料的收集和运输，其中包括安全问题、对潜在事故 / 事件所造成的威胁的分析、公共健康考虑等。美国能源部的国家核安全管理局（NNSA）进行了多次这种评估。在 2004 年 1 月，它完成了一项对可裂变核材料的收集和运输的调研。该项调研假设把高浓缩铀从俄罗斯空运到美国田纳西州诺克斯维尔附近的一个安全地点，并评估由此引发的潜伏癌症导致人口死亡的风险。NNSA 的评估考虑了这么几种情况：“无事故 / 事件”发生、飞机在飞行中解体或毁坏、飞机在地面坠毁（即“着陆失事”）、地面运输这种材料的车辆撞毁（例如卡车事故）、“不采取行动”，等等。NNSA 确定，在所有设想情景中，最坏的情形是一个人在地面交通事故现场“最大程度地遭到”放射性物质的照射，估计这种潜伏癌症死亡几率为“ 1.4×10^{-10} ，或者说低于十亿分之一。”对于负责把高浓度铀包装箱从飞机上转移到卡车上的工作人员来说，其几率低于十四万分之一。¹⁵ 因此 NNSA 的评估结果是：“没有显著影响。”得出相同结论的类似风险评估报告还有：查理顿山谷生物发电项目风险评估、芝加哥附近阿贡国家实验室的核反应堆设施清污和退役工程风险评估、南

卡罗来纳州艾肯附近的核反应堆燃料设施建设项目风险评估, 等等。¹⁶

1997年做出的发射“卡西尼”号探测器探访土星的决定意义非凡, 也与本文建议的概念密切相关。首先, 这项使命涉及到把一个有效载荷发射到地球轨道以外的目的地; 其次, 该航天器(即“卡西尼”轨道飞行器)采用的是核动力; 第三, 它的有效荷载, 即“惠更斯”(Huygen)探测器, 包含核部件。跨部门核安全审查小组为国家航天局进行的风险评估审视了这样几种设想情况: 发射事故、运载火箭和有效载荷意外重返地球大气层而解体或毁坏事故、航天器为提高行星际航行的惯性速度而进行“秋千式摇摆”机动时由于地球引力导致意外重返地球大气层事故。在“卡西尼”号使命报告的最终环境影响陈述中, 所评估的癌症死亡率中值为“ 1.4×10^{-6} ”。¹⁷ 这个值的变化范围在“130亿分

之一”到“2800亿分之一”之间。¹⁸ 该报告所设想的事故/事件及分析值得注意, 因为它们和向太阳发射核废料的建议中可能发生的情况颇为相似。

结论及建议

本文发现, 把放射性核废料射向太阳的处置方法对公众健康的危害风险甚微。具体说, “卡西尼”号小组(根据在此建议的发射情景可能发生的类似情况)所报告的癌症死亡率中值为38亿分之一, 而且这种情况也只有在发生运载火箭事故时才会出现, 此值显著小于一般人群的癌症死亡率(五千分之一)。鉴于对公共健康的风险极其微小, 同时考虑到上文提到的尤卡山核废料封存设施已被弃用的事实, 本文建议, 美国应重新考虑向太阳发射核废料这一经济可行的核废料处置方案。♣

注释:

1. Senate, A Bill to Secure the Energy Future of the United States, to Provide Incentives for the Domestic Production of Clean Energy Technology, to Achieve Meaningful Pollution Reductions, to Create Jobs, and for Other Purposes [参议院议案: 保障美国的能源未来、奖励清洁能源技术的国内生产、取得意义重大的污染减排、创造就业机会及实现其他目标], 111th Cong., 2nd sess., 11 May 2010, [1], <http://www.kerry.senate.gov/imo/media/doc/APAbill3.pdf>.
2. Francis W. Sears and Mark Waldo Zemansky, “Radioactivity and Nuclear Physics,” in University Physics [大学物理教程中“放射性与核物理”], 2nd ed. (Reading, MA: Addison-Wesley Publishing, 1962), 901-16.
3. C. L. Cheever, “Ionizing Radiation,” in Fundamentals of Industrial Hygiene [工业卫生基本原理教程中“电离辐射”], 5th ed., ed. Barbara A. Plog and Patricia J. Quinlan (Itasca, IL: National Safety Council Press, 2002), 257-80.
4. Charles D. Hollister and Steven Nadis, “Burial of Radioactive Waste under the Seabed” [海底埋葬放射性废物], Scientific American 278, no. 1 (January 1998): 60-65.
5. A. V. Zimmerman, R. L. Thompson, and R. J. Lubick, Summary Report of Space Transportation and Destination Considerations for Extraterrestrial Disposal of Radioactive Waste [关于地球外处置放射性废物的空间运输及目的地考虑的总结报告], NASA TM X-68211 (Cleveland, OH: Lewis Research Center, April 1973), http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19730012836_1973012836.pdf.
6. Markus J. Aschwanden, Physics of the Solar Corona: An Introduction [日冕物理导论], New York: Springer, 2004), 26-29.
7. Mark Waldo Zemansky, “Change of Phase” and “Applications of Thermodynamics to Special Systems,” in Heat and Thermodynamics [热与热力学教程中“相变化”和“热力学对特别系统的应用”], 4th ed. (New York: McGraw-Hill, 1957), 317-38; 280-316.
8. Francis W. Sears and Mark Waldo Zemansky, “Spectra and Atomic Physics,” in University Physics [大学物理教程中“光谱与原子物理学”], 2nd ed. (Reading, MA: Addison-Wesley Publishing, 1962), 884-900.
9. Chuck Walker with Joel Powell, Atlas: The Ultimate Weapon by Those Who Built It [宇宙神运载火箭: 建造者的终极武器], (Burlington, Ontario: Apogee Books, 2005), 265-78; 另参看 Roger D. Launius and Dennis R. Jenkins, To Reach the High

- Frontier: A History of U.S. Launch Vehicles [抵达高边疆：美国运载火箭历史], (Lexington: University Press of Kentucky, 2002), 102-46, 148-87; 另参看 Ed Kyle, “2013 Space Launch Report” [2013 年太空发射报告], 21 January 2013, <http://www.spacelaunchreport.com/log2013.html>.
10. Edward M. Purcell, “Space Travel: Problems of Physics and Engineering” [太空旅行：物理与工程问题], 收录于 Models of the Atom [原子模型], ed. Richard P. Feynman (New York: Holt, Reinhart and Winston, 1968), 221-44; 另参看 Curtis D. Cochran, Dennis M. Gorman, and Joseph D. Dumoulin, eds., Space Handbook [航天手册], (Maxwell AFB, AL: Air University Press, 1985).
 11. Eric Aakko, “Risk Communication, Risk Perception, and Public Health” [风险沟通、风险认知和公共健康], Wisconsin Medical Journal, 103, no. 1 (2004): 25-27, https://www.wisconsinmedicalsociety.org/_WMS/publications/wmj/pdf/103/1/25.pdf.
 12. “Advanced Space Transportation Program: Paving the Way to Space” [先进太空运输计划：铺设太空之路], Marshall Space Flight Center, National Aeronautics and Space Administration, <http://www.nasa.gov/centers/marshall/news/background/facts/astp.html>; 另参看 David Kestenbaum, “Spaceflight Is Getting Cheaper, but It’s Still Not Cheap Enough” [航天飞行成本趋低但仍不够便宜], National Public Radio, 21 July 2011, <http://www.npr.org/blogs/money/2011/07/21/138166072/spaceflight-is-getting-cheaper-but-its-still-not-cheap-enough>; 另参看 Frank Sietzen Jr., “Spacelift Washington: International Space Transportation Association Faltering; the Myth of \$10,000 per Pound” [太空运输华盛顿：国际太空运输协会踌躇不前；每磅 1 万美元的神话], SpaceRef, 18 March 2001, <http://www.spaceref.com/news/viewnews.html?id=301>; 另参看 R. L. Thompson, J. R. Ramler, and S. M. Stevenson, Study of Extraterrestrial Disposal of Radioactive Wastes, Part 1 [放射性废物地球外处置的研究，第一部分], NASA TM X-71557 (Cleveland, OH: Lewis Research Center, May 1974), 35, 37, http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19740014663_1974014663.pdf. (说明：1974 年的成本按照 2012 年 12 月的通货膨胀做了调整。)
 13. “Defense Nuclear Waste Disposal: Proposed Appropriation Language” [国防核废物处理：建议的拨款说明], in FY 2000 Congressional Budget, (Washington, DC: Congressional Budget Office, 2000).
 14. Karen Blum, “Johns Hopkins Conference to Study Prevention of Thyroid Cancer during Nuclear Events” [约翰霍普金斯大学——关于预防核事件期间甲状腺癌的研讨会], press release, Johns Hopkins Medical Institutions, 26 February 2003, <http://esgweb1.nts.jhu.edu/press/2003/FEBRUARY/030226.HTM>.
 15. Department of Energy (DOE) / Environmental Assessment (EA)-1471, “EA for the Transportation of Highly Enriched Uranium from the Russian Federation to the Y-12 National Security Complex” [关于从俄罗斯联邦运送高浓缩铀到美国橡树岭国家实验室的环境评估], 15 January 2004, v, http://energy.gov/sites/prod/files/nepapub/nepa_documents/RedDont/EA-1471-FONSI-2004.pdf.
 16. DOE/EA-1475, “Finding of No Significant Impact for the Chariton Valley Biomass Project Environmental Assessment” [查理顿山谷生物发电项目环境评估没有发现严重影响], 10 July 2003, http://energy.gov/sites/prod/files/nepapub/nepa_documents/RedDont/EA-1475-FONSI-2003.pdf; 另参看 DOE/EA-1483, “Environmental Assessment for Decontamination and Decommissioning of the Juggernaut Reactor at Argonne National Laboratory—East Argonne, Illinois” [伊利诺伊州东阿贡——阿贡国家实验室 Juggernaut 核反应堆的清污及退役环境评估], March 2004, http://energy.gov/sites/prod/files/nepapub/nepa_documents/RedDont/EA-1483-FEA-2004.pdf; 另参看 DOE/EA-0170, “Finding of No Significant Impact, Fuel Materials Facility, Savannah River Plant, Aiken, South Carolina” [对南卡罗来纳州艾肯萨凡纳河电厂核燃料设施的调查结果没有发现重大影响], July 1982, http://energy.gov/sites/prod/files/nepapub/nepa_documents/RedDont/EA-0170-FONSI-1982.pdf.
 17. Solar System Exploration Division, Final Environmental Impact Statement for the Cassini Mission [对卡西尼号使命的最终环境影响陈述], (Washington, DC: Office of Space Science, National Aeronautics and Space Administration, June 1995), 4-97 through 4-98, <http://saturn.jpl.nasa.gov/spacecraft/safety/chap4.pdf>.
 18. 同上, 4-100 到 4-101.



默里·贝科威茨博士 (Dr. Murray R. Berkowitz), 纽约大学理工学院理学学士, 哥伦比亚大学文理硕士, 约翰霍普金斯大学 Bloomberg 公共卫生学院公共卫生硕士, 德莫因大学骨科医学中心骨科医学与外科学院骨科医学博士, 现任费拉德尔非亚骨科医学院乔治亚校区终身副教授及防治和社区医学主任, 兼任德州沃思堡骨科医学研究中心研究员。他在马里兰州健康与心理卫生部接受普通防治医学和公共卫生实习医师训练。他是医学委员会认证的神经肌肉骨科医学、骨科干预医学及预防医学与公共卫生专科医师, 并拥有职业医学证书。他曾在美国陆军作为医疗兵团军官服役, 进入医学院之前在陆军和空军担任过多项任命。他是美国骨科医学院学报科学编辑 (主编), 发表过 100 余篇手稿、论文及讲演。贝科威茨博士毕业于装甲军官高级教程、海军陆战队指挥参谋学院、空军指挥参谋学院和空军战争学院。



一个解释网空优势的概念模型

Cyberspace Superiority: A Conceptual Model

威廉姆·D·布赖恩特，美国空军中校（Lt Col William D. Bryant, USAF）

空军追求空中优势，海军追求海上优势。那么是否有网空优势？这个问题目前还没有明确共识。有些作者，比如兰德公司网空问题专家马丁·利比基（Martin Libicki）认为：“网空绝对优势没有意义，因此不是网空战士所追求的合适目的。”¹ 美国空军不同意这种观点，它把网空优势定为一个关键概念。根据空军作战准则文件 AFDD 3-12《网空作战》的定义：网空优势代表“在网空、经网空、从网空在指定时间和指定领域开展行动而不受过度干扰的优势”。² 联合作战准则采取折中立场，联合出版物 JP 1-02《国防部军语词典》对天空、海上、太空优势都给出定义，惟独没有列出网空优势这个词条。然而这部文件将问题进一步复杂化，它指出：全谱优势是“在陆、海、空、天领域及信息环境（包括网空）占据支配地位的累积效应”。³ 关于网空优势的困惑，大部分是因为网空难以直观看到和把握。本文试图克服这一困难，提出一个解释网空优势的概念模型。

模型就本质而言，并非实物本身，而是一种极其精减的归纳，是以帮助理解和分析。然而，模型必须足够保真才能有用，任何战略模型都必须考虑战略的动态性质，即模型中需要考虑“敌人的投票”，双方都视对方的举动而作出相应决定。克劳塞维茨把这种互动比作两名摔跤手在比赛，互相拼命想制服对方。⁴ 战略模型也必须做到这一点。

还请注意：本文讨论的网空优势是以国家之间的冲突为背景。尽管黑客团伙和网络犯罪分子可能使用和国家行为者相同的一些工具和技术，但其目的有着本质的不同，他们的行动与“政治以另一种方式的继续”无关。⁵ 在国与国的冲突中，网空一般被认为是全球公域，就像海洋一样，其正常状态不受任何一方的指挥或控制。⁶

网空优势本身不是目的；赢得网空优势并不一定等于打赢整个冲突——但是夺得这种优势肯定有助于在冲突中取胜。对网空优势带来的最重大效应，网空战士的感受肯定不如在其他作战领域那么深刻。在陆、海、空、天领域，战士们严重依赖网空来执行任务，现代军队如果没有其信息系统，就很难有效地开展作战行动。为了说明网空优势的意义所在，以及控制网空如何会在其他领域产生预期的效果，本文首先建立一个能反映生成天空领域优势的模型。

领域控制模型

由于难以理解像网空这种非纯物理的现象，所以我们首先比较熟悉的环境中建立一个领域控制模型，见图1。具体说，文献资料包含大量关于空中优势的讨论，我们也可通过众多战争和实例研究来归纳出属于天空领域的特征、元素，和互动。本文建立的模型只涉及“手段”（是什么产生该领域的优势）和“方式”（这些手段在该领域之内之外能做什么）。手段即工具，方式即用这些工具

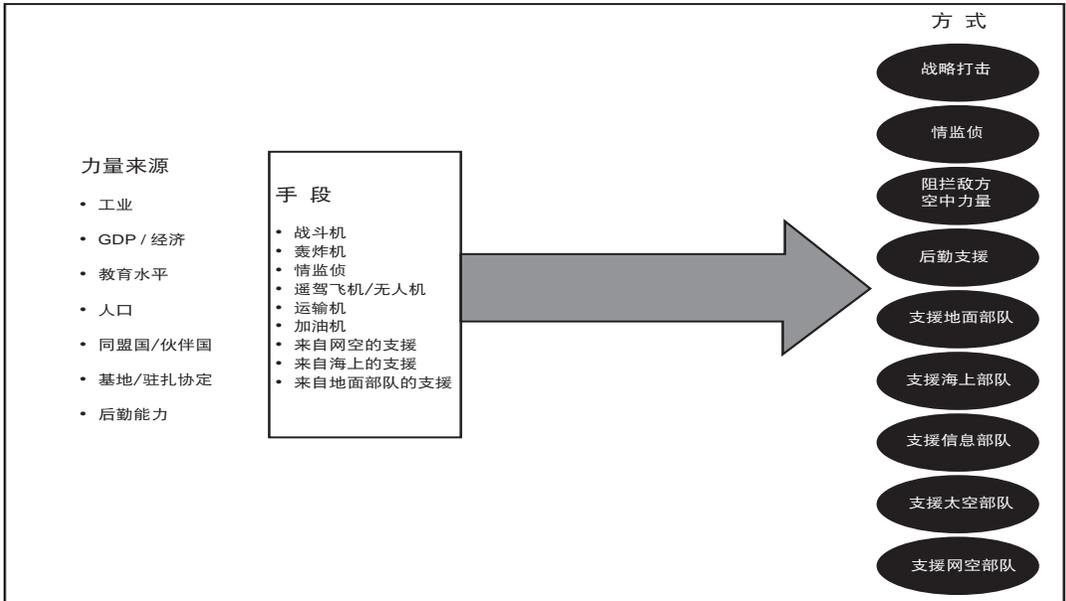


图 1：空中优势的手段和方式

能做什么事。至于这些方式如何能或者不能促成总体战略目的，该模型不予置评。

一个国家的力量来源，比如工业和人口，产生其空中力量的手段（战斗机、轰炸机、加油机等）。国家然后使用这些对付敌人的手段生成空中力量的方式——空中力量能做的事——比如实施战略打击或支援地面部队。然而，如克劳塞维茨所观察：“在战争中，意志是针对能起反应的有生命物体而言”。⁷ 敌人不会坐等攻击，而是会尽力阻止对手使用手段。图 2 描述了敌人可以用来阻拦空中力量的一些常用方式。

然而，战略的动态性质（即每个行动都会引起敌方的反应）还没有到此完结。行动发起方也能通过使用一系列大家熟悉的潜在有效的措施对敌方的行动作出反应。图 3 是空中优势的完整模型，展现进攻方一些可用的降低风险的战略。

当然，反应可能又引起反应，循环反复，没完没了；但是，只要上升两级就足以显现抗衡的动态性质。该模型示出发起方需要加强的元素，敌人拥有的阻拦发起方的选项，发起方削弱对方阻拦的选择和可使用的方式。所有这些，在天空领域相对而言几乎没有争议；但是网空领域因其独有特征，导致该模型的元素大为不同。

网空领域的独有特征

建造网空优势模型需要考虑网空领域的鲜明特征。因为该领域是人造的（第一特征），所以其地理位置总是随着作战员或第三方而变化。《网空中的战略战争》的作者格雷戈里·拉特瑞（Gregory Rattray）评论说：“网空是独特的，其互动受制于人造硬件和软件，所以网空的‘地理’比其它环境远更易变换。移山挪海不易，但手指一拨开关就能开启或关掉部分的网空。通过在路由器或交换机里

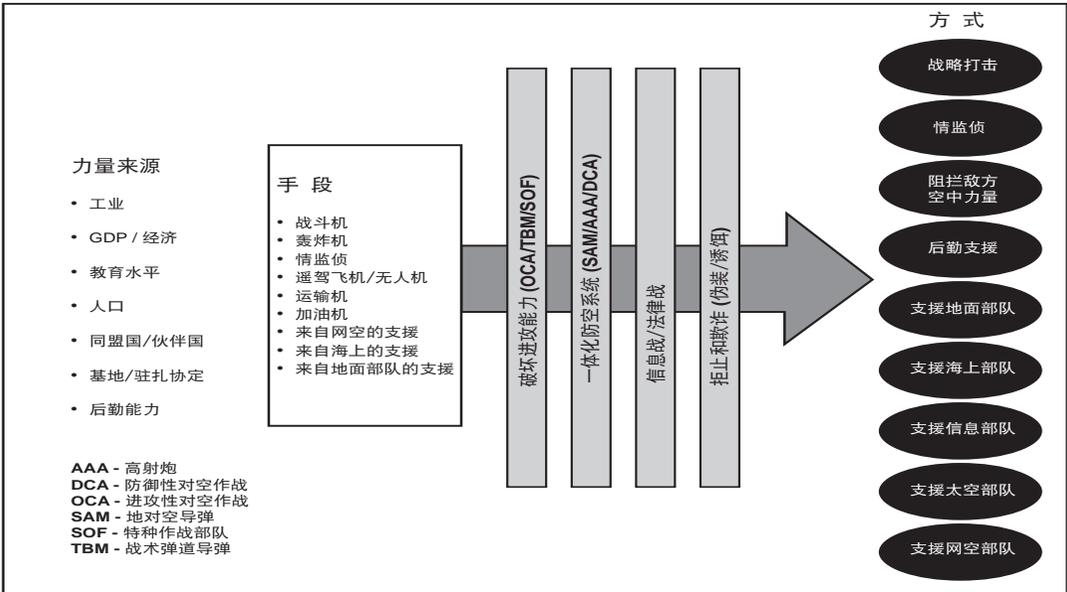


图 2：空中优势的手段和方式及对手的阻拦

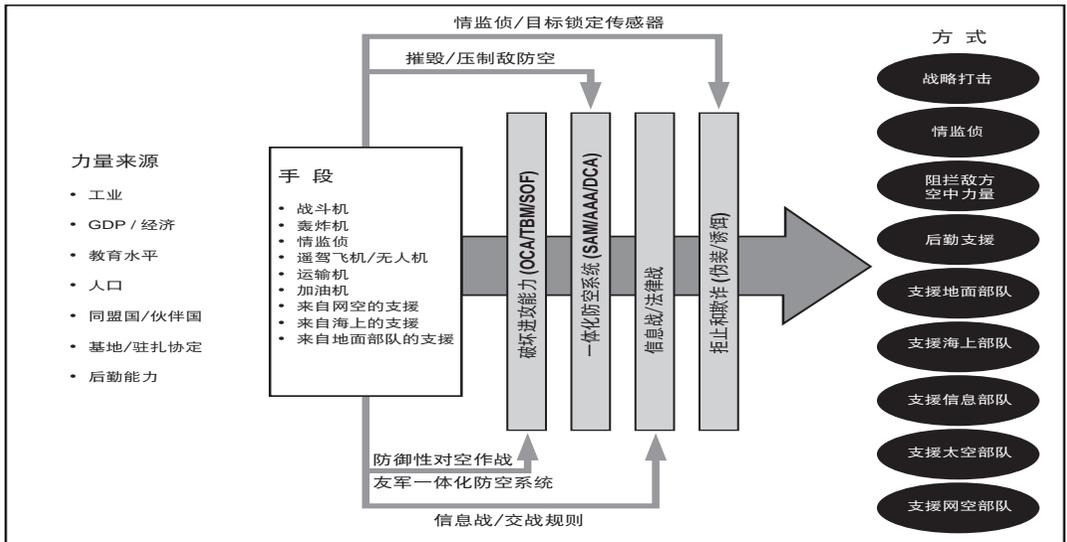


图 3：空中优势模型

增加新编码指令就能把它们建成或者‘移除’。⁸这种易变性不只是移动“地理”特征的能力，我们也能复制网空的河流、山脉、和海洋，随意把它们储存起来，日后如有必要再加进去。随着数据储存成本一路降低，

网空战士可以对每样东西拥有多个副本。利比基称：网空既可复制，便可修复——此概念对网空的持久效果有重大影响。⁹

如同天空和海洋领域的情况一样，作战员借助技术进入网空，不过成本要小得多。

海洋领域的港口和船只，天空领域的飞机和机场，都需要通常只有国家实体才拥有的巨额资源开支。相比之下，网空的港口或机场近在眼前，距离不过是最近的因特网服务提供商或网吧；用于攻击的载体可能是以不足500美金就几乎随地可购的便携式电脑。重大网空能力可能需要巨额资源，而且需要多年的开发，但是进入的最初成本始终非常低。进一步，成功所需的资源，主要是人，是经过高度培训的能干人才，而不是花费在基础设施和装备方面的大笔费用。

我们也必须承认，控制网空本身未必就能赢得战争。虽然敌人知道对手能够操纵其信息系统而产生严重不确定性，但敌人不会因此而放弃战斗和目标追求。占据土地固然意义重大，占据网空就未必如此。然而，网空优势使我们能利用网空的信息而开展其他行动，通过网空在其他领域产生效果。比如，敌人能进入美国后勤系统这一事实就值得注意，因为敌人可能获取部队的动向信息，也可能操纵该系统，故而通过减少对这些部队的补给而降低他们在其他领域的作战效能。对手侵入发电厂控制系统也意义重大，因为他能够通过网空破坏发电厂而对其它领域产生效应。

网空的另一特征，即进攻和防御之间的不对称，在某种程度上也适用于天空，因为现代空战中进攻性空中力量和地面防御力量之间存在着不对称。现代一体化防空系统利用的是地对空导弹、高射炮、战斗机、和与指挥和控制相整合的监视资产。除多用途战斗机之外，这些防御能力不能执行进入敌方领土的进攻性任务；它们只能攻击入侵的飞机。网空的防御和进攻之间存在着相似的不对称，在网空，防御和进攻系统既不相似也不能互换。这种非对称性与海战中的情况相

反，在海战中，驱逐舰可攻可防，很像坦克或步兵。防火墙和蠕虫病毒(网空的重要元素)在本质上不同，且不可互换，如同爱国者导弹与B-52轰炸机分属不同类别一样。

因为网空武器依赖欺诈达到入侵的目的，所以它不堪一击。它犹如一把玻璃剑，其锋虽利，足可致命，但稍折即断。防御方一旦发现有人窃取信息，就会设计补丁阻止对方利用同样的漏洞继续攻击。另外，就像玻璃剑那样，网空武器也难以被发现。针对未知破绽发起的网空攻击被称为“零日”攻击，因为当初次攻击发生时，漏洞的计时器从零开始，然后在软件工程师仓促制作补丁的同时递增上升。防御方在没有发现己方系统的具体漏洞之前，只能依靠寻找通识标志的系统，其成功率只在中等之间。如此，防御方认为敌人窥探零日漏洞的探哨码很重要，一经发现立刻加防。根据这些特征，我们现在可以建造一个网空优势模型。

网空优势模型

本文运用来自其他领域的一些概念以及网空的特性，通过图4展示网空的手段和方式。

网空攻击手段

一个国家的网空力量来源产生目前可供在网空使用的能力或手段。借助于社会工程，进攻方诱导用户不知不觉地采取某种行动而放他进门。进攻方也能开发“特洛伊木马”软件或攻击敌人的供应链，在防御方使用的软件或硬件中设置某种访问端口或能力。此外，进攻方也许会利用“拒绝服务”攻击，即向防御方的系统发送铺天盖地的巨量虚假信息请求，致使其服务器资源耗尽而不能有效工作。他也许会使用某些动能手段（无论

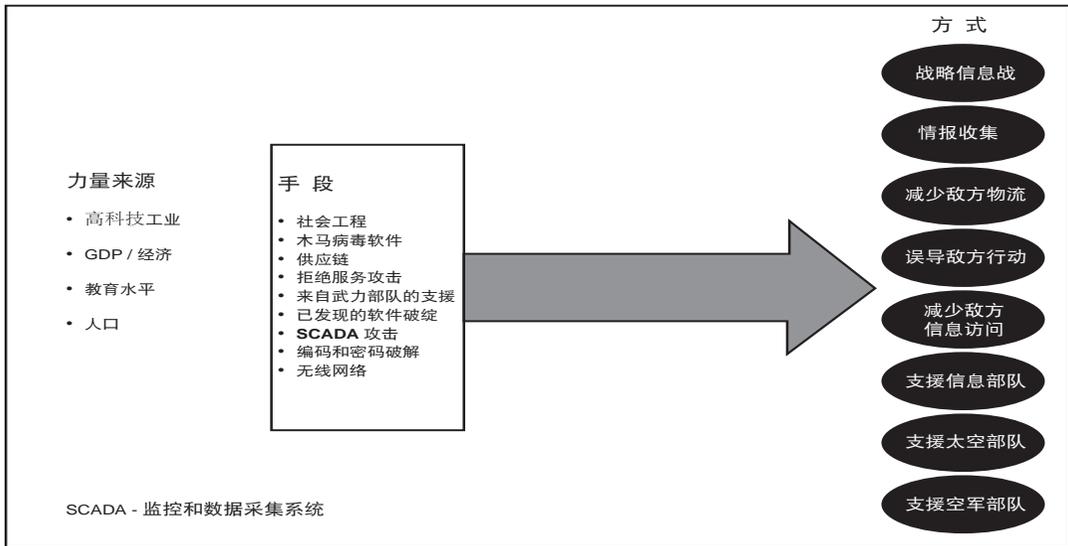


图 4：网空优势的手段和方式

是由战斗机投放联合直接攻击弹药，还是由特工人员投送一包 C4 高爆塑料炸药）摧毁对方物理信息系统。跨域效果可以从物理世界延伸到网空，反之亦然。被进攻方发现的软件破绽是其武库中的“王冠明珠”，因为这些破绽让他能够开发特殊手段进入系统并实施攻击以达目的。但通过逆向关系追踪到破绽，又有助于信息技术界提高对此漏洞的了解和熟悉。一般来说，防御方能很快制作出补丁程序来解决已知的问题，并开始封闭进攻方的机会之窗。不过这个窗口通常不会完全封闭，因为总有一些用户和系统管理人员未能正确地修补其系统，但无论如何，补丁既成，必定使攻击更加困难。

一种特殊类型的网空攻击是把目标对准监控和数据采集系统（SCADA），这些系统控制着发电厂、大坝、水处理设施等各种基础设施。那些喜欢预测网空攻击大灾难的危言耸听者通常引证这些系统向国会要钱。理论上，这种攻击可以关闭几乎任何现代的系统。根据被攻击的系统的不同，有时候，敌人只

需将防御方的某种系统关闭（即使防御方随后立刻重新启动），其之破坏就远远超过一关一开本身。以 Stuxnet 即“震网”蠕虫病毒为例，它能执行针对控制系统的非常精密的攻击，据说造成了组件的物理性破坏，但显示屏却向系统工程师们谎报一切正常。¹⁰ 进一步，代码和密码破解能帮助进入或提取信息，无线网络为进攻方提供另一个潜在入境口岸——甚至能潜入“气隙”隔离系统（即不直接插入更广互联网的系统）。

网空攻击方式

这些手段可以成就多种不同方式来达成战略最终状态。首先，进攻方在战略信息战中可以使用这些方式。在战略信息战中，进攻一方的国家可以使用网空直接攻击重心。根据埃立克·特赖亚斯少校和布莱恩·贝尔上尉(Eric D. Trias and Bryan M. Bell)的文章，“战略袭击的目的是针对敌人的重心系统地运用兵力，用最小的生命和金钱代价产生最大效果”。¹¹ 正如轰炸机轰炸城市惩罚百姓，以

逼服民众迫使其政府改变政策一样，网空攻击也可抑制或摧毁城市的基础设施，以期产生同样的效果。

国家行为体在和平时期进行的大部分网空侵犯似乎重点是情报收集和网络间谍，这在冲突时期也很重要。例子包括闯入敌人系统阅读敌方战争计划或查看其部队或能力的战备状态。

进攻方可能会选择攻击对手的后勤系统。现代军队的后勤支援依靠其信息系统，由于不同地点的多方用户都必须进入这些系统，他们常常访问非保密网络，并容易受到攻击。误导信息，即诱导对方把补给品送到错误地点、改变库存信息、或更改时间表等，都可能对战役产生极大影响——尤其是如果敌人严重依赖在短时间内远距离调动大量部队的话。显然，美国在这个领域特别脆弱。

减少敌人访问信息的机会将削弱其部队的效能。可以采用一种更微妙的方式，这就是误导敌人，改变敌人对自己周围发生之事

的判断而影响其行动。这种技术可能包括假信息，但是敌人可以有多种数据来源，从而阻碍误导取得成功。最容易让敌人上当的误导做法，通常是故意渲染对手本来就趋于相信的东西——当年盟国渲染登陆点在加来而不是在诺曼底，就蒙骗了希特勒。这些攻击可以运用技术上真实的信息（而不是运用假数据）来建立误导性情景。进攻方总是寻求塑造对手周围的决策环境，诱使对手按进攻方的意愿行事。

网空也向所有其它作战领域提供关键性支持。¹² 比如，网空攻击可以愚弄敌人的一体化防空系统，致使它无法发现来袭的空中打击群，也可以瘫痪其太空干扰系统。当然，和空中力量的情况一样，敌人也许不会被动忍受这些行动，而将竭力加以阻拦，如图 5。

网空防御阻拦

防御方可以利用许多措施来保护自己不受网空攻击的伤害。最常用的措施包括安装

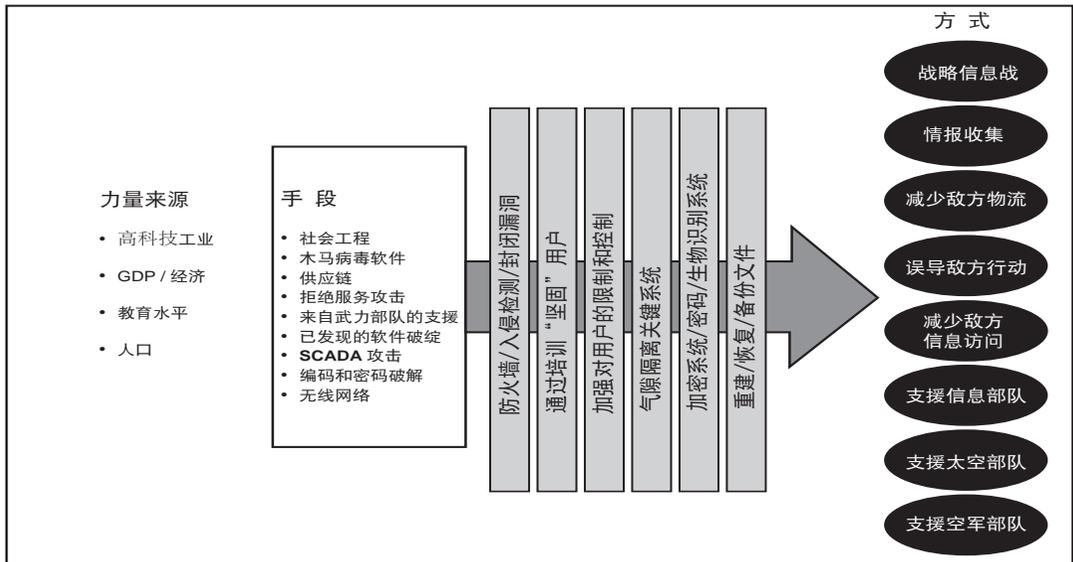


图 5：网空优势的手段和方式及对手的阻拦

防火墙、入侵检测和认证系统来防止未授权访问。封闭已知的漏洞也很关键，因为许多系统没有安装最新补丁。

用户的疏漏是世界各地系统管理员头疼的根源，许多攻击之所以得手，都是那些稍经引诱即易入套的人的恩赐。因为大多数用户对计算机安全意识淡薄，投入财力和时间对用户加强培训可获丰厚回报。

系统管理员也能通过加强限制和控制来降低用户带来的风险，但是降低连通性将付出重大代价。信息系统存在的目的是处理和分享信息，如果管理员小心过度而对外界关闭系统，也许正中进攻方的下怀，因为闭关自守意味着严重降低自己的能力。防御方必须在保持进出和保障安全之间找到适当的平衡，从而避免借己之手而成进攻方之美。

此外，防御方可以气隙隔离（断开）系统，即不让系统直接接入互联网——对于高度敏感和关键系统（比如关系到核武器的系统）来说，这是适当的做法。然而气隙也不能保证关键系统不遭受攻击，因为精明的对手也许会找到其它进入的途径。可能的情况包括物理进入系统、己方启动无线而联网，或者疏忽中把靠气隙隔离的系统接入外界互联网而铸下错误，等等。

己方系统也许可以继续使用互联网的骨干网，同时依靠加密来保证信息不落入非友善之手。使用密码拒绝进攻方进入系统是现在大多数系统的常规作法。进一步，如果实施得当，诸如生物特征识别或令牌识别等共同登录卡，也能拒入侵者于系统之外。

最后一种阻拦进攻的方式是借助备份和加强韧弹生存力。媒体经常提及“梅丽莎”（Melissa）或“监狱”（Slammer）蠕虫病毒，

不过受感染后的大部分信息技术能在一两天之内就完全恢复运行。¹³ 进攻方如果突破所有防御并彻底抹除后勤系统里的数据，可能对防御方造成严重问题。但后者若能在进攻方未察觉或无法进入的移动媒介中存有备份，并能一天之内使系统恢复运行，那么，就能把攻击的后果降到最低程度。图6是建构完成的网空优势模型，其中展示出进攻方为削弱防御方阻拦的效果而可能使用的几种方式：

进攻方对抗防御阻拦

如果敌人精心研究防御方的训练计划，就可能改进其社会工程，把重点放在训练中没有覆盖的那些方式，或按照训练中被认为可接受的例子研制类似的方式。只要有一个用户犯下一个错误，就能开启一扇机会之窗。对手可以使用不基于互联网的攻击来侵入被气隙隔离的系统——也许通过一个被无意漏掉或打开的无线调制解调器，或在防御方供应链里嵌入的恶意代码，或通过间谍活动或特别行动而物理进入系统。另外，通过代码和密码破解可以挫败加密，尤其是如果精明的进攻方发现了获取加密密钥的技术，那么他就不必动用暴力。最后，对手可以同时对付备份系统和主要系统发起攻击，从而破解以简易数据复制作为保护手段的做法。虽然互联网上称病毒能把计算机融化为一滩废物有点危言耸听，但对手的确可能攻击硬件本身，从而使防御方花费更多时间来恢复运作。

上述模型不会保持一成不变；相反，它将随着新开发的技术和程序而变化。就像空中力量模型那样，新技术会产生进攻和防御双方面的新能力。各方都根据对方使出的招数来策划自己的行动，克劳塞维茨的“摔跤比赛”将继续进行下去。

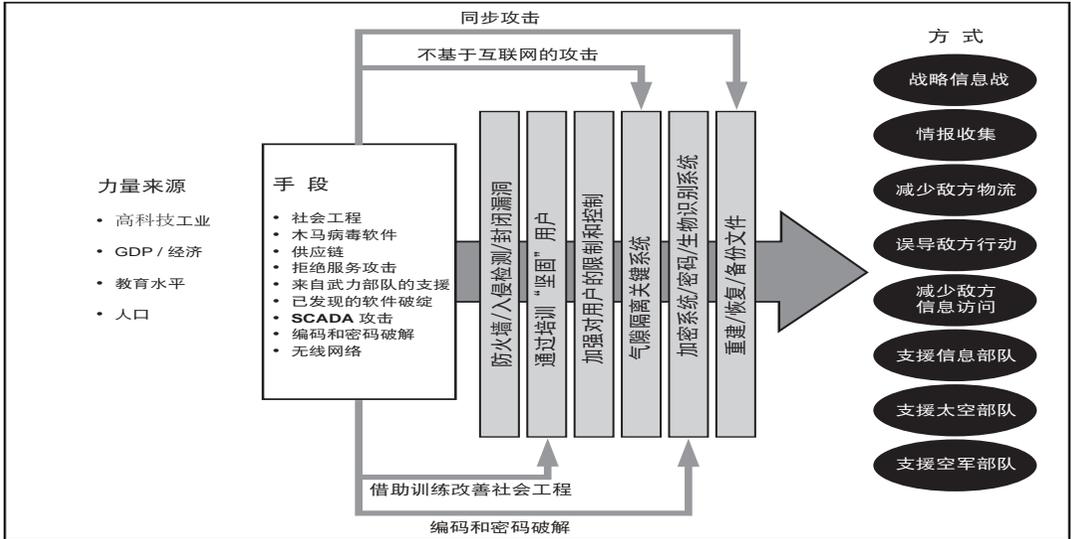


图 6：网空优势模型

网空优势的测量

测试本文建议的模型需要具体的衡量标准，比如由美国联合部队司令部制定的那些标准，如图 7。在该图中，信息由较低层输入较高层，还要注意，每种效用的测量可有多项指标，每种效果又可有多种效用测量方式，每个目标又可有多种效果。进一步，根据形势而定，每个目标也许只有一种效果，等等。

网空优势是局部的和临时的。根据前面提到的空军作战准则文件 AFDD 3-12 的定义：当己方能“在指定时间和指定领域开展行动而不受过度干扰”，他就取得了网空优势。这种优势不是全球性或全面的；它与进攻方企图在冲突中达到的目的有关。在图 6 建议的网空模型中，目标或目的是进攻方寻求的方式。比如，对手想降低敌方的后勤能力，其所预期的效果则是敌方装甲部队由于缺乏补给而瘫痪。进攻方相应的效用测量可能涉及到敌方装甲师补给状况的变化，由该装甲师

拥有的常规补给种类补给品储备水平表示。进攻方可以使用下列指标作为衡量标准：对于该敌军装甲师来说，绿色代表燃料储存等于或少于 24 小时；琥珀色等于 24-72 小时；红色等于 72 小时以上。



图 7：效果要素总结（改编自 Department of Defense, US Joint Force Command, "Tactics, Techniques, and Procedures: Assessment of Joint Operations" [战术 / 战技 / 战规：联合作战评估], 10 March 2008, I-6, fig. I-3)

以上例子中的网络要素可能包括对敌方的电脑化后勤系统进行集中攻击，误导其燃料去向，使燃料送不到进攻方计划与之交战的装甲师而被错送到其他地方。这个过于简化的例子表现出测定网空优势的几个重要问题。首先，进攻方大概不会完全依赖网空攻击来减少敌方的燃料补给，他们还可能使用其它动能打击手段。装甲师燃料耗尽这一事实并不一定意味着是网空行动的结果，进攻方或许也炸断了桥梁、袭击了战地油库、摧毁了防御方的燃料输送车队，等等。由于战斗形势不能重复，因此不可能把战役从头再演一遍，记录下结果，然后从新启动，在不利用网空攻击的情况下再进行一次同样的战役，以便确定是否会出现不同情况。

模型的运用

发生在2012年的针对沙特阿拉伯石油公司Aramco的网空攻击，为我们提供了一个如何把该模型用于现实的例子。有些具体情况仍然模糊，并被各有关政府列为高度机密，但是开放源文献提供了让我们可以合理推演这个事件的足够信息。据《纽约时报》报道，进攻方——他们自称属于一个“正义利剑”的激进团体——企图关闭Aramco的石油和天然气生产。¹⁴然而，美国情报官员断言，伊朗精心策划了这次攻击，是为了报复针对其核计划的“震网”攻击。¹⁵在该网空优势模型里，进攻方的方式涉及到战略信息战和网空攻击的使用，以能直接影响到物理目标。显然，选定的手段包括社会工程和“鱼叉式网络钓鱼”攻击。¹⁶

更具体说，进攻方企图关闭Aramco的石油和天然气生产，并希望产生停产的预期效果。效用测量以生产中的变化来表现，即由Aramco生产的石油和天然气产量表示。尽管

我们不知道进攻方的标准，我们能使用以下假设：低于原生产量的50% = 绿色；50-70% = 琥珀色；75-100% = 红色。在这个案例中，很容易确定进攻方是否取得了网空优势，因为尽管这场攻击影响波及到30,000台计算机，但Aramco的产量根本没有减少。¹⁷通过运用网空优势模型，我们能清楚地看到为什么这次攻击证明不成功。具体说，因为Aramco把办公室电脑与控制石油和天然气生产的电脑隔离开了，所以攻击没能突破气隙隔离层。图8列出Aramco网空攻击事件和阻拦成功的要素。

在这个实例中，成功的防御阻止了进攻方取得网空优势。这并不是说这次攻击一事无成；它确实使Aramco的系统遭受了极大的破坏，也增加了中东的不安定性。然而，进攻方没有达到其完全关闭石油和天然气生产这一既定目标，如此，这场行动没有达到开展网空行动而不受过度干扰的程度。

结语

本文建议的模型可以用来分析网空攻击、网空防御，以及这两者在各种网空攻击行动中的彼此互动。该模型虽然有用，但如果运用不慎，也可能仅仅成为包含战斗毁伤评估和经验总结等元素这种回顾过去的测量法。我们昨日的所作所为固然重要，但主要是作为评估我们明日能为之事的出发点。指挥官想知道的是今天占有多大网络优势，是否足够明日作战之需，如果不够的话如何能获取更多优势。本文的模型能帮助回答这些问题——只要我们慎重地以前瞻方式加以运用。如果气隙隔离层阻拦了昨日的攻击，那么我们怎样才能找到绕过这个障碍的途径？如果今天的攻击成功了，但成功的途径被发觉，防御方已经将它封闭了，我们还能找到

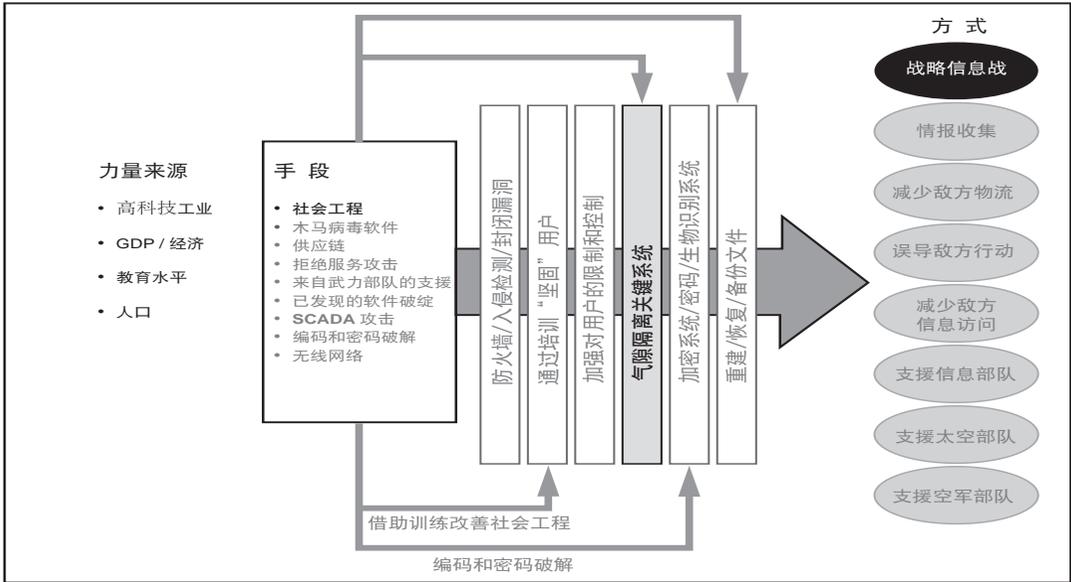


图 8：网空优势模型和 Aramco 网空攻击事件要素

另外的途径来开展明日的攻击吗？我们也必须把多项目的结果累加起来。如果一位指挥官有八项任务要执行，但是期望取得其中两项任务的成功，那么这就不是网空优势，因为敌人能够实施“过度干扰”。该模型提供了一种思考网空领域优势的结构化途径，能帮助网络战士识别机会与风险，提高作战成功的可能性。

战争游戏玩家也可以把该模型用作推演和演习中的模板来模拟环境，对该模型防御端感兴趣的指挥官也可以这样做。尽管本文强调了网空攻击，但防御方可以同样方便地

运用该模型来审视自己的计划，以确定计划的哪些地方可以加强，同时要时刻牢记：敌人将对每个行动都做出反应。

本文模型的真正效用，不在于告诫防御方需要防火墙，也不在于提醒进攻方注意软件破绽。大家已经精通了这些概念。最需要深刻理解的，是网空攻击和防御的各种元素之间的动态互动，是意识到克劳塞维茨的“摔跤比赛”持续到了网空，这才是本模型的最大效用。即使毫无疑问它将需要与时俱进，但毕竟，它为我们了解网空优势的动态变化提供了一个有用的框架。♣

注释：

1. Martin C. Libichi, Cyberdeterrence and Cyberwar [网空威慑与网空战], (Santa Monica, CA : RAND Corporation, 2009),141, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.
2. Air Force Doctrine Document 3-12, Cyberspace Operations [空军作战准则 AFDD 3-12：网空作战], 15 July 2010 (incorporating change 1, 30 November 2011), 2, http://static_e-publishing.af.mil/production/1/af_cv/publication/afdd3-12/afdd3-12.pdf.

3. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms [联合出版物 JP1-02 : 军语词典], 8 November 2010 (as amended through 16 July 2013), 115, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
4. Carl von Clausewitz, On War [战争论], ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75.
5. 同上, 第 7 页。
6. David J. Lonsdale, The Nature of War in the Information Age: Clausewitzian Future [信息时代战争的性质: 克劳塞维茨式的未来], (London: Frank Cass, 2004), 185.
7. 见注释 4, 第 149 页。
8. Gregory J. Rattray, “An Environmental Approach to Understanding Cyberpower” [以环境方式理解网空力量], 收录于 Cyberpower and National Security [网空力量与国家安全], ed. Franklin D. Kramer, Stuart H. Starr, and Larry Wentz (Dulles, VA: Potomac Books, [2009]), 256.
9. Martin C. Libicki, Conquest in Cyberspace: National Security and Information Warfare [征服网空: 国家安全与信息战], (New York: Cambridge University Press, 2007), 5.
10. Paulo Shakarian, “Stuxnet: Cyberwar Revolution in Military Affairs” [震网: 军事领域的网空战革命], Small Wars Journal, 15 April 2011, 2, <http://smallwarsjournal.com/blog/journal/docs-temp/734-shakarian3.pdf>.
11. Maj Eric D. Trias and Capt Bryan M. Bell, “Cyber This, Cyber That . . . So What?” [网空这, 网空那……究竟为何?], Air and Space Power Journal, 24, no. 1 (Spring 2010): 91, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj10/spr10/aspj_en_2010_1.pdf.
12. Shawn Brimley, “Promoting Security in Common Domains” [促进公域的安全], Washington Quarterly, 33, no. 3 (July 2010): 122, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA536657>.
13. 见注释 9, 第 37 页。
14. Reuters, “Aramco Says Cyberattack Was Aimed at Production” [Aramco 称网空攻击是针对生产], New York Times, 9 December 2012, http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0.
15. Nicole Perloth, “In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back” [美国从针对沙特公司的网空攻击中看到伊朗在反击], New York Times, 23 October 2012, <http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all>.
16. Wael Mahdi, “Saudi Arabia Says Aramco Cyberattack Came from Foreign States” [沙特称 Aramco 网空攻击来自国外], Bloomberg, 9 December 2012, <http://www.bloomberg.com/news/2012-12-09/saudi-arabia-says-aramco-cyberattack-came-from-foreign-states.html>.
17. 同上。



威廉姆·D·布赖恩特, 美国空军中校 (Lt Col William D. Bryant, USAF), 毕业于空军军官学院, 美国军事大学文科硕士, 乔治华盛顿大学文科硕士, 空军理工学院太空系统硕士, 高级空天研究院空中力量艺术科学硕士, 现为阿拉巴马州马克斯韦尔空军基地的空军战争学院学员。此前他担任作战支援中队指挥官及作战主任, 以及多个作战和参谋职务。布赖恩特中校是经验丰富的战斗机飞行员, 飞行 F-16 累积超过 1,500 小时。

虚空布兵：正确理解网空战争中的兵力集结和战斗力

Virtually Massive: Understanding Mass and Combat Power in Cyber War

约翰·科布，美国空军上尉（Captain John "Strider" Cobb, USAF）

数量之中自有其质重。

——据称为斯大林语，述及苏联在二战期间的武器生产。

美国空军对“兵力集结”（mass）所给的定义是，“集兵力于最有利的地点和时间，夺取决定性胜利。”¹ 空军作战准则 AFDD 3-12《网空作战》在呼应这一定义时提出，网空部队“必须整合并协同其他部队”。² 此定义从网空战略角度来看意味着什么？一些人建议，兵力集结的概念不再适用于网络空间，因为攻击者可能只是一些散兵游勇，却能从世界任何地方发动毁灭性的攻击。³ 美国空军退役上校格雷戈里·拉特雷（Gregory Rattray）在《网空中的战略战》一书中探讨了诸如网空情报作战、目标判定、工具开发等能提高网空攻击效能的支援功能，其中涉及到和兵力集结相关的另一个层面——打击敌方目标，不仅需要发动攻击的“牙齿”，还需要组建在后面支援的整个团队即“尾巴”，才能确保持续攻击成功（因为他在书中建议，己方的分析员和程序员可能需要在数量上大幅度超过实际发动攻击的人员）。⁴ 此观点显然有其独特之处，也是一个需要解决的重要问题。但我们在理解网空战争中的兵力集结时，不能只局限思考人员的数量。

兵力集结也能从攻击流量来思考，最直白地说，就是有多少字节或数据包投入目标。有时候，也可从同时被释放的病毒的数量来判断，即依据防火墙和防病毒工具对来袭的

恶意软件实施封锁所得到的结果来判断，从而获得对数量的更有意义的界定。也有时候，某种计算机病毒被攻击者或研究人员认定为是同一种类，却可能自我修改代码，表现为数百种不同的病毒，设法通过对方的过滤器。再一种情况是，可以从多少节点受到攻击来理解数量——在最低层次，可以计测多少装置受到攻击；在更高层次，可以计测多少网域或实体地点（如基地）受到攻击。虽然这样的分析过于简单化，但从这些不同角度来理解“数量”，可以更全面地解析网空“火力”。对网空战争中兵力集结的理解还应考虑另一个面向，这就是关注被保护的网络的坚固性或生存能力。一个网络，如果配备很多备用设备、宽带和冗余路径，就更能各种攻击中生存下来（或至少能更迅速恢复）。还有一个常被忽视因而也需关注的情况是，我们配置了多少技术人员和技能来担当被攻击网络的维护和保护。最后一点，大多数国家在和平时期的网空行动要比在战争时期的网络攻击更有节制，因此平时时期中的隐蔽行动所表现的兵力集结，可能不似在公开网空战争中那样的多面性。

网空防御中的签名扫描和探试扫描

很多读者或许不熟悉防火墙和消毒软件如何保护网络，在此简单解释一下。典型的

防火墙扫描从局域网出人的访问流量，而消毒软件扫描计算机的硬盘。当然也有例外，如基于网络的入侵检测系统，或路由器的访问控制列表过滤器，但是保护网络的主要工具是防火墙或传统的消毒软件，其他常用的工具也不外乎使用类似的规则来扫描和过滤。⁵ 扫描病毒有两种主要方法：签名（特征）扫描和探试扫描。网络防御最常用的方法是通过核实签名搜索出恶意软件，通常是将被扫描文件（或网络包）的一部分或全部与已知病毒完整清单进行对照和匹配。对于防御已知病毒的攻击，此举相当有效，但很显然它无法检测出大多数新型病毒攻击，而且通常难以捕捉住那些稍加修改的已知病毒的攻击。⁶

网络防御中发现恶意软件的另一种方法是使用“探试”扫描。这种方式不是去寻找已知是恶意的文字行或文件包，而是寻找可疑的模式或行为。这能更有效（虽然有欠完善）地逮住新的“零日漏洞”攻击，而且更能截获以往攻击病毒的新变种。缺点是，大多数探试式算法语言造成很高的假阳性率，在被截获的访问中，真正的恶意攻击并不多，许多合法的访问和通信却被错误挡住而造成虚警，因此操作过程会非常耗时，会令人沮丧。这些过滤器面临的统计问题，类似于对某些癌症的造影检视。⁷ 毕竟，网络流量中的绝大部分并不含恶意，如果将其中的 95% 标以病毒警示而只承认 1% 为合法，结果只能是将真正的病毒文件淹没在大量假阳性警报中。⁸ 很多商业产品结合使用这两种方法，安全研究人员也在研制探测攻击的一些替代办法。但是总体而言，目前除了最重要的和安全要求特别高的网络以外，大多数网络在很大程度上只依靠基于签名的扫描模式进行检测，因资源的缺乏而难以采纳其他方法。⁹

这样，对很多大型军事或工商业网络而言，新病毒攻击常常在得手之后才被检测到，此时网络已被攻陷。

网空中攻防双方兵力集结的诸种考虑因素和比较

由于网空防御中的这些限制，在目前的网空中，攻击的效果并非总是同其复杂程度成正比。攻击软件必须达到什么样的复杂程度才能成功，取决于被攻击目标的规模大小、复杂性、防御坚固程度和相互联系等因素。攻击者面对的政治限制，例如不得不隐身匿名、隐藏攻击源或伪造假攻击源等，常常提高网空攻击所需的复杂程度，以及攻击者的工作量。对重要军事目标和基础设施目标的攻击，因以上各种因素而效果各异。有些关键目标很难设防保安全，一经攻击就功能俱废；也有些目标，尤其是小型目标，即使不那么重要，却不怕攻击，只有那些非常复杂的攻击才能得手。拒绝服务攻击（DoS）简单易行，复杂性不及间谍企图性攻击。地理分布面广且节点多的网络在监控防御方面更加困难，难以堵住病毒攻击潜入。对于那些从商店直接购置的硬件和软件系统开展攻击，只要经过一般标准训练，使用一般工具，就可能得手。但若想攻击情报部门、核设施或某些基础设施的专门系统，可能需要经过周密的侦察和定制的攻击设计，才能得逞。¹⁰

托马斯·里德（Thomas Rid）曾著一文，其中某些假设虽需商榷，但正确地指出：凡隐形的、有高度针对性的“战略”攻击，如震网病毒，需要动用大量资源来编制复杂程序，而且不易重复使用。^{11、12} 这类攻击可能需要数十名情报分析员、程序员和操作员组成团队来设计、组装和发动。不同团队可能需要其成员接受其中部分或全部的训练，将

其技能加以组合。亦即，若想攻击那些高度戒备的目标，常常需要数十名训练有素的人付出数月努力才能完成。所以，要想迅速破坏或瘫痪大量的坚固和独立的目标，攻击方显然需要投入巨大的人力物力。如不得不匿名和隐藏攻击源，则投资更加高昂。那些参与对独立目标实施攻击的网络战士，就可能无法参与“日常”的网空情报工作，而日常情报工作也不可或缺。

也有很多网络目标的防护并非那么严密，其中一些可能是高价值的目标。震网病毒攻击的目标如核设施，可能网络入口防守严密，一应“闲人莫入”；但其他很多军事和工业系统必须允许大量和频繁通信出入，才能有效运作。例如，电网必须允许各发电站之间时刻保持联系，否则就运转不起来。这些“在线”通信虽然不至于像那些直接送上互联网的非加密通信，但是仍容易被攻击者所利用，可能一次攻击就能控制、削弱、甚至摧毁整个电网系统。当然，我们必须指出，像美国或俄罗斯这样的大国，“电网”系统是由一组区域电网松散连接而成。例如，美国有三个地区电网；¹³ 俄罗斯虽比美国实施更加中央化的控制，实际上有七个地区电网，相互之间的联系很有限。¹⁴ 很多军事网络与之相似，这些网络中必须容纳数量庞大的单位和基地，必须保持互相之间的联系，才能发挥现代军队所依赖的这种力量倍增器的效能。如果让外部的复杂攻击攻破其网络的一个节点，就很难防止其在网络中蔓延。

沿此思路，兵力集结的第二个定义或许能提供更好的理解。有些目标容易受到单一团队发动的攻击，攻击一点而波及整个网络，如果攻击成功，能严重妨碍整个地区。互相关联的公共设施，特别是电网，就是这样的例子，它们通常比其他公共设施网络的规模

更大，也更加相互依赖。另一个例子可能是用于指挥控制、后勤和作战态势感知的军事网络，这些功能必须覆盖战术和作战层面，要求一个由数量众多的关键节点共享的网络。在网空攻击频谱的最简单端，是分布式拒绝服务攻击，其兵力集结体现为对带宽的占有，由此倾覆目标网络。顺此网空攻击频谱向复杂端移动，我们看到，如果某攻击使用有效的自我修改代码，防御方就可能需要在数十至数千个网络外围布防，以拦截不只一个而是数百甚至数千个新病毒签名。保护每一个局部网络的防火墙软件都必须定时更新，将新的病毒签名随时加入其拦截病毒清单。

在有些攻击中，病毒软件使用的“探哨”（exploits）的数量，比病毒如何通过变异渗透过滤器可能更加相关——所谓“探哨”就是某种恶意代码，它利用目标软件的缺陷来控制系统；一旦探获出目标网络的缺陷或漏洞并加以利用，此攻击病毒就可能成功。¹⁵ 大多数军事网络都配备技术人员，他们知道防火墙和消毒软件不能阻止所有攻击，但努力做到在攻击发生之前设法修补已知的缺陷和漏洞，以防被攻击者利用。如果相应的缺陷已有针对性地彻底修补，那么仅使用一个探哨代码的攻击就会失败。迅速实施彻底修补是一项艰巨的挑战。¹⁶ 目前已有工具能在几天时间内就能完成对大型现代网络中众多系统的修补。¹⁷ 如果某一攻击使用多个探哨代码，将增加防御方面面临的挑战。但是，探哨代码（尤其是零日漏洞探哨代码）可能是有重大价值的情报资产，很多政府反对随意透露这些恶意代码。¹⁸ 另一方面，这些探哨代码的数量比人们想象的要更多，例如，在2012年1月到5月间，微软就宣布了视窗7操作系统和常用应用程序（如微软办公套件）

中存在的 31 个严重漏洞，并为此发布补丁程序。¹⁹

此外，有些攻击是以有多少网络作为单次攻击或系列攻击的目标来作为兵力集结的考量因素。笔者在其他文章中曾探讨有些网空攻击能将局部网络与中央控制或反应隔离。²⁰ 在防御这些类型的攻击方面，关注地理位置的分布或受到攻击的局部网络的数量，可能比关注有多少人参与发动攻击或使用了那些攻击类型更有意义。这主要适用于对抗拒绝服务攻击和分布拒绝服务攻击，或适用于高度集中化控制的网络防御。²¹ 如果在每个地点都配备熟练的网空防御人员，他们应能相对轻快地清除简单的攻击（尤其是分布拒绝服务攻击）。但如果采用更加集中化的网空防御方式，可能出现集中于一地的防御人员与其所管理的网络联系被切断，或导致防御人员供不应求，无法同时对所有地点遭受的攻击做出反应。

从防御一方来看，在这些类型的攻击中，人力可以是兵力集结的关键因素。拒绝服务式攻击与有高度针对性的攻击不同，前者在兵力对比上可能高度的不对称。攻防双方固然在开展“军备竞赛”，防御方努力在过滤器、扫描和其他网络工具上赶上黑客的技术，但总体而言，这些拒绝服务攻击可以由一个相当小的团队发起，防御方却可能需要配置大量人员来修补和清除受到攻击的每个局部网络的故障。

对网空作战中战斗力的相对衡量和计算，依据攻击种类和需要保护的网空类型而不同。知识和经验丰富的技术和操作人员始终发挥着重要作用，²² 但军队对人力配置的质量和数量需要做适当平衡，按照预见的攻击类别和工具相应做好搭配。当前军队都面临

着预算限制，而可能发生的网络攻击种类很广泛，因此必须统筹兼顾做好人力搭配和取舍。如果主要威胁来自类似震网病毒的隐身攻击，目的是秘密破坏数据或损坏物理设施，那么网络防御团队必须训练有素，特别在病毒取证分析技术方面，而其人员数量则不需要远远超过攻击方的数量。并且防御方经常能在对方攻击成功（至少是部分成功）侵入后阻止攻击，因为攻击方为避免被察觉，其病毒传播通常较慢，造成的破坏也慢。如果攻击方的主要目的是迅速瘫痪或孤立关键的系统，则防御方需要配备大量人员，所需技能应着重于反击公开的攻击（并且复原被攻击瘫痪的系统）。为了获得对潜在敌人的足够了解从而预测其主要攻击方式，就需要大量培养网空情报人才队伍，有了充分的这类人才，就能成功应对和反击攻击。²³ 偶尔，可能出现对同一个目标同时开展两种不同类型的攻击，但在大多数情况下，对同一个网络和系统的这两种攻击会互相干扰，攻击方可能因此而失去对更高针对性目标精确攻击的控制。可能性更大的，是以公开拒绝服务(DoS)或分布拒绝服务(DDoS)攻击一个地区，而对远离此攻击的另一个系统或网络，则可能采用更精心策划的秘密攻击。当然，在当今任何冲突中，协调和化解网空冲突——无论是来自网空还是来自动能打击——都要求做好重要的作战策划。²⁴

网空兵力集结与传统战争的比较

在思考网空的兵力集结问题时，回顾空中力量作战的历史，可能有助于澄清不同的集结方式——在某些方面，网络攻击方面面临着与美国陆军航空兵及英国皇家空军在第二次世界大战期间轰炸德国工业体系时类似的问题。高度针对性的攻击（如震网病毒）是

以量身定制的、不可复制的独特攻击手段瘫痪几个孤立的高价值目标，通常缓慢而秘密地进行，有点类似二战中美国开展战略轰炸的方式。用这种方式，攻击方确定几个关键的节点，然后集中大量人力、时间和战斗力去摧毁这些节点，²⁵ 确信一旦成功摧毁，敌人便无法继续运作。相较而言，各种形式的拒绝服务攻击，有些类似英国轰炸德国的目标选定方式：英国没有针对具体的（通常有严密防御的）关键系统实施直接攻击，而是试图瘫痪这些关键系统所依赖的当地或区域网络的某些方面。二战中英国皇家空军打击敌方目标的过程中，最初是针对重要工厂，但是未能奏效且蒙受重大损失，经历初期失利之后，皇家空军转而着重轰炸重要的工业城市，把目标锁定在整个工业生态系统，而不是一系列分离的关键节点。美国陆军航空兵部队则将打击目标锁定在那些关键的节点，特别是飞机制造、燃料生产、交通运输、球轴承制造等，虽然在初期也经历了类似英国空军的失利，但通过从 1943 至 1945 年的持续打击，摧毁或瘫痪了其中一些关键节点（例如在施韦因富特的球轴承厂和在普洛耶什蒂的炼油厂），实现了严重打击德国工业系统的意图。²⁶ 美国陆军航空兵和英国皇家空军采用的具体实施方法并非全然不同（美国陆军航空兵 B-17 和 B-24 因为天气原因和德军防御的干扰，常常不能将炸弹投中目标），²⁷ 但是两国部队选定打击目标的方式，同上述讨论的两种网络攻击各有相似之处。当然，军队网络中的个人电脑和交换机等硬件基本上是没有争议的目标，不像打击工业城市的人口一样容易引起争议，但很多拒绝服务攻击不那么精确并更可能蔓延，祸及民用网络并产生意想不到的后果。值得注意的是，无论是高度针对性的定点打击，还是大面积攻击，此两种网空攻击方式都可能非常有效——前

者有震网病毒的成功为证；后者有 2007 年对爱沙尼亚的分布式拒绝服务攻击为证，且此攻击影响深远。²⁸ 另一个例子是据称由俄罗斯 2008 年策划的对格鲁吉亚的拒绝服务攻击，这场攻击破坏了格鲁吉亚对俄罗斯装甲部队进攻做出反应的能力。²⁹

结果是，瘫痪一个反应堆可能极为困难，需要周密制定一个全新的攻击程序；而破坏军方的一个指挥控制或后勤网络则相对可行，只要使用“现成货架”黑客工具，就能发动相对简易的攻击。网空领域与其它作战领域的一个不同点是，网空中范围更大的且分布更广的目标，常常也是更容易受到攻击和瘫痪的目标。最近对网空战争的讨论，常常把平时的间谍活动误认为战争，一些评论人士倾向于高估探哨代码在战争中的重要性，以及隐形性在战争中的必要性，并以为大型军事或基础设施网络的防御能力同较小的情报系统或核系统通常配设的保护一样坚固。³⁰ 这些误解歪曲了网空战争中兵力集结的性质，可能导致我军在组建网空战争单位或设立网空防御时犯下严重错误。虽然网空间谍活动——包括在和平时期的秘密网空攻击——往往表现为隐形及定点打击，而在公开战争中，网空攻击可能包括上述讨论的所有形式的兵力集结和战斗力；对网空攻击的外交和政治限制也可能不相同，有些冲突可能限制为“仅网空”攻击，也有的冲突可能允许包括网空攻击在内的传统（火力）作战。但是这两种冲突中，都可能包含更多的公开性网空攻击，不再注重隐形匿名，而注重更狠更快，以有限的资源实现广大范围的打击效果。

结语

兵力集结是网空战争中的一个要素，而其含义因攻击性质和打击目标的不同而各

异。其对战术层面的影响可能不太严重（尤其是对非美国军队和 / 或地面部队而言，因为他们对网络的使用相对较少）；但在战役层面，现代军队非常依赖网络开展后勤补给和保持势态感知。这些网络是“重心”所在，如果被破坏，可能对严重依赖这些网络的部队的作战效能造成巨大影响。高度针对性定点攻击可能产生毁灭性的效果，而各种形

式的拒绝服务攻击，只要所选目标正确且实施得当，也能产生瘫痪敌人的效果。对网空战兵力集结和战斗力需做出正确的理解和界定，而此定义又随形势而变化，恰如网空本身。军队若将自身限制于仅发展某一个方面而使其作战准则和组织结构不能全面覆盖敌人发动攻击的各种方式，一旦遭袭，将面临被打败的风险。♣

注释：

1. Air Force Doctrine Document (AFDD) 1, Basic Doctrine [空军作战准则 AFDD 1：基本作战准则], p. 32.
2. AFDD 3-12, Cyberspace Operations [AFDD 3-12：网空作战], p. 16.
3. Martin Libicki, Cyberdeterrence and Cyberwar [网空威慑和网空战争], (Santa Monica, CA:RAND Corp, 2009), p. 59, <http://www.rand.org/pubs/monographs/MG877.html>.
4. Gregory J. Rattray, Strategic Warfare in Cyberspace [网空中的战略战], (Boston: MIT Press, 2001), pp. 100, 464.
5. Edward Skoudis, "Information Security Issues in Cyberspace" [网空中的信息安全问题]. 见 Cyberpower and National Security [网空力量和国家安全论文集], ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, (Dulles, VA: Potomac Books, 2009).
6. "Antivirus Software" [消毒软件], Wikipedia, http://en.wikipedia.org/wiki/Antivirus_software.
7. Maia Szalavitz, "Why People Stick with Cancer Screening, Even When it Causes Harm" [透视检癌有害身体，为何人们乐此不疲?], Healthland, Time.com, <http://healthland.time.com/2012/05/25/why-people-cling-to-cancerscreening-and-other-questionable-medical-interventions-even-when-they-cause-harm/>
8. 见注释 6。
9. 更多介绍，参看 Shon Harris, CISSP All in One Exam Guide [信息系统安全认证考试指导大全], 4th ed. (New York:McGraw Hill, 2008), pp. 250-257.
10. 然而，那些专门的系统可能比与之类似的标准现成商品系统更薄弱，一旦被攻击者了解，便更易受到攻击，尤其是那些在设计时通常不考虑安全因素的基础设施系统。
11. Thomas Rid, "Think Again: Cyberwar" [网空战争三思而行], Foreign Policy, 27 February 2012, <http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=0,2>.
12. 17147818 震网病毒是一个极端复杂的特洛伊木马类病毒，通过 U 盘传播，2010 年侵袭并破坏了伊朗的核设施，几个月后才被发现。参看 "The Stuxnet Outbreak" [震网病毒爆发], The Economist, Sept 30, 2010. <http://www.economist.com/node/>.
13. Richard A. Clarke and Robert K. Knake, Cyberwar: The Next Threat to National Security and What to Do about It [网空战争：国家安全面对的下一个威胁以及如何应对], (New York: HarperCollins, 2010), 167.
14. Rinat Abdurafikov, "Russian Electricity Market: Current State and Perspectives" [俄罗斯电力市场：现状和前景], VTT Technical Research Centre of Finland, 2009, <http://www.vtt.fi/inf/pdf/workingpapers/2009/W121.pdf>.
15. "Exploit" [探哨攻击代码], Wikipedia, [http://en.wikipedia.org/wiki/Exploit_\(computer_security\)](http://en.wikipedia.org/wiki/Exploit_(computer_security)); 另参看注释 9 中 Shon Harris 文，第 62 页。
16. Stephen Northcutt, et al, Inside Network Perimeter Security [揭示网络周边安全], 2nd ed. (Indianapolis: Sams Publishing, 2005), pp. 257-258, 其中讨论了修补大型网络的困难因素。

17. Microsoft Security Update Guide [微软安全更新指南], 2nd ed. Microsoft, 2011 <http://www.microsoft.com/en-us/download/details.aspx?id=559>; 关于补丁系统的简介, 还可参看“WSUS Overview” [自动更新服务概述], Microsoft Technet, <http://technet.microsoft.com/en-us/library/cc539281.aspx>.
18. 见注释 3, 第 57 页。
19. “Patch Tuesday [周二补丁日], (January-May 2012)” Microsoft Technet, <http://technet.microsoft.com/en-us/security/bulletin/ms12-jan>, <http://technet.microsoft.com/en-us/security/bulletin/ms12-mar>, <http://technet.microsoft.com/en-us/security/bulletin/ms12-apr>, <http://technet.microsoft.com/en-us/security/bulletin/ms12-may>.
20. John Cobb, “Centralized Execution, Decentralized Chaos: How the Air Force is Poised to Lose a Cyber War” [集中执行, 分散乱套: 美国空军网战败相已露], Air and Space Power Journal, Summer 2011, http://www.au.af.mil/au/cadre/aspj/airchronicles/apj/2011/2011-2/2011_2_16_cobb.pdf.
21. 拒绝服务攻击 (DoS) 是通过大流量攻击某系统或网络使其超载而瘫痪。分布式拒绝服务攻击 DDoS 是一种特殊类型的 DoS 攻击, 来自世界各地的电脑发送出洪水般的网络流量, 从而瘫痪目标服务器或网络, 导致其死机或停止对合法的流量做出反应。参看注释 9 中 Shon Harris 文, 第 1010-1013 页。
22. 更深入的讨论, 参看 Kamal Jabbour, “Cyber Vision and Cyber Force Development” [网空远景和网空兵力发展], Strategic Studies Quarterly, Spring 2010, www.au.af.mil/au/ssq/2010/spring/jabbour.pdf.
23. 见注释 4, 第 142 页。
24. 有关消除网络攻击的深入讨论, 见空军作战准则 AFDD 3-12, 第 25-26 页。
25. Elinor Mills, “Expert: Stuxnet was Built to Sabotage Nuclear Plant” [专家认为震网病毒意在破坏核工厂], Insecurity Complex, CNET.com, http://news.cnet.com/8301-27080_3-20017201-245.html?tag=mncol;1n.
26. Geoffery Perret, Winged Victory [胜利女神], (New York: Random House, 1993), pp. 240-244.
27. 见注释 11, 第 280 页。
28. 这场分布式拒绝服务攻击据称由俄罗斯操纵 (俄罗斯政府否认有官方参与), 对爱沙尼亚银行和政府造成重大破坏。参看注释 13 Clarke and Knake 文, 第 11-16 页。
29. David Hollis, “Cyberwar Case Study: Georgia 2008” [网战战例研究: 2008 格鲁吉亚之战], Small Wars Journal, January 6, 2011 <http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008>, p. 5.
30. 这些错误的假设出现在多篇文章中, 包括上面的 Rid 文 (例如其文中第 5 页) 和 Libicki 文 (见其文第 56-59 页), 以及对比上述提到的补丁指南文件, 特别是注释 16 中 Northcutt 文中的介绍。事实上, 修补一个大型网络少则数天, 多则数周, 工作量巨大, 而且如果修补过程太快, 补丁本身可能瘫痪关键系统。



作者目前在美国空军大学司令部担任信息工程组负责人。在此之前, 他外驻日本三泽空军基地, 参加第 35 通信中队中的三泽蓝军队, 负责网络作战方面的工作。



走向中美网络关系共同安全平台

Towards a Common Security Platform for Sino-US Cyber Relations

帕纳约提斯·雅纳科乔戈斯博士，美国空军大学空军研究所防务分析员 (Dr. Panayotis A. Yannakogeorgos, Research Professor, USAF)

引言

网络空间及其组成部分互联网，已经成为二十一世纪的火药桶。这个领域，原本代表着全球信息化社会项目的成果，却在过去十年中充斥着竞争利益和意识形态的分歧，各方在其中争夺着数码影响势力范围。今天，网络罪犯、恐怖团伙和其他恶意破坏分子利用国际网络合作的不力和大国之间的紧张关系，在这个领域中为所欲为。各国非但不去寻找加强合作的途径，反而缠斗于意识形态，力图推行自己认定的合作行为规范。

互联网不是奢侈品，它是一个至关重要的工具，在没有限制的情况下，能使信息自由流动于全世界，打开经济发展、知识交流和创新的大门。在互联网骨干的开发和维护上，美国的技术创新领先是毋庸置疑的。然而在网络行为规范上，美国以“盟主”身份主导制定全球网络安全行为规范的努力却一再走入死胡同。借用社会科学的术语来说——正如我们未能就如何保护非排他性全球公共利益达成协议一样——如果无法建立合适的全球规范，就只会增加所有角色的不安全感。于是，一切的努力导致了负和的结果。

网络犯罪和间谍活动将继续呈上升趋势。越来越多的人获得先进的信息和通信技术，进入数字化信息社会，但是，有关各国如何主导和应对针对商业系统和关键基础设施的恶意网络攻击，以及这些行为的后果，

都还有待澄清。消弭分歧固然重要，澄清混淆更为迫切。本文拟就中美网络关系讨论提出一些澄清，目的在于推动两国间实现共同网络安全。笔者虽无法提供最重要的结果即解决方案，惟希望能说清我们面临的问题，认识问题的性质，提出一些供商榷的建议。

简述美中网络合作历史

“奥习”会

美中合作前景从大势而言是积极的，与此大势直接相联，两国的经济和金融关系也日趋紧密。中国持有上万亿美国的美国主权债务，不仅使美国沃尔玛和塔吉特的货架更加充裕，也解决了中国数百万人的就业。¹当我们探讨两国领导人的政治声明时，一定要牢记这个背景，而无需深究所谓的资产负债表。

2013年6月7-8日，奥巴马总统和习近平主席在加州会面，讨论了包括网络冲突在内的各项议题。两位领导人表示愿意加强合作。习近平主席说：“我们需要密切关注这个问题，研究解决这个问题的有效办法。网络安全议题实际上可以是中美相互务实合作的领域。”奥巴马承认：“有关黑客或盗窃等网络安全议题，并非是美中关系中所特有的，这是国际关注的问题。那些非国家的行为者也经常在从事这些非法活动。即便我们在同

* 本文作者出席了2013年长沙国防科技大学第二届网络安全研讨会并做发言，现对其发言稿加以整理和更新，投寄本刊发表。

其他国家磋商建立应遵守的公共规则，我们也必须在私营和公共部门建设防御和保护系统。”²

鉴于美中两国都在研发技术，扩大用户数量并承担大国地位的领导作用，奥习两位领导人将须拉动世界马车，以身作则，开始解决 21 世纪初最大的安全困境。中美在网络合作上存在着巨大的机遇，其进展将在未来数月和数年中展现出来。奥巴马和习近平并同意设立高级别的工作组处理网络问题。双方加强网络合作，应表现在减少针对知识产权的入侵企图。另外，中美计算机应急响应小组加强及时分享信息，加大执法活动力度，也应作为双方提升合作的明显指标。

立足合作精神推进网络合作

奥习会营造出来的美中合作乐观气氛来之不易。曾担任美军参谋长联席会议副主席的美国空军退役上将约瑟夫·罗尔斯顿曾令人信服地指出通过两军交流建立与中国互信的长期效益。同理，在计算机安全和关键基础设施保护领域方面，我们也能同中国建立互信。³ 美国海军退役中将迈克·麦康纳尔提议，美中合作将有助于“清理”恶意网络活动，降低黑客和网络犯罪导致的敌对入侵和破坏。⁴

在美国对台湾售武、联合国制裁伊朗、谷歌被迫撤出中国大陆，以及美国的互联网自由议程等问题导致美中两国出现一系列不断加剧的分歧后，2013 年 4 月，美国国务卿克里赴华访问，企望重新改善双方关系。⁵ 克里的访问没有取得预期的成功，对减少中国网络间谍活动效果不大。布拉德·德隆据此认为：在中美关系中，由于基本的经济因素出现变动，影响力的消长已发生巨大的变化。显然，这种双边关系会经常出现起伏——

最近的“低潮”涉及美方曝光中国持续支持解放军发起大规模工业间谍活动，以及中国在南中国海问题上日益强硬。⁶

此外，一些民间组织以建立互信为己任，例如东西方研究所（East-West Institute）发起了第二轨道外交计划，最近在去年 6 月启动了第五轨道。第五轨道会晤是美国国务卿克里 2013 年 4 月访问北京的结果，克里在北京宣布，要推出一个正式的计划，开始为美中合作建立基础。克里国务卿在声明中说：

由于网络安全影响每个人，我们将立即设立一个工作组。网络安全不仅影响天空中的飞机和轨道上的火车，还关系到大坝泄洪、交通运输网络、发电站、金融、银行和证券交易。使用网络的现代国家在方方面面都受到影响。很明显，我们所有国家都必须保护人民，保护其权益，保护其基础设施。因此，我们将立即行动起来，加速展开网络合作。⁷

如果美国和中国领导人的公开声明是真挚的，那么这是美中在网络空间关系中的一个积极步骤。

超越空谈

不仅政治家释放出善言，我们也看到美中两国执法当局加强了打击网络犯罪的实际合作。中国当局将恶意黑客行为入罪，一旦行为者通过侵入电脑系统和网络的非法行动造成损害的罪名成立，将被判刑入狱。中国的执法部门还与美国同行开展合作。⁸ 在最近的一起案例中，美国联邦调查局和中国公安部合作，相互提供帮助，打击提供儿童色情的中文网站。⁹ 该案延续了双方近年来在刑事案中有限的合作精神。美中经济与安全审议委员会成员拉里·沃茨尔 2010 年在国会的作证也清楚地表明网络合作是可能的，并

列举了具体的执法互相支持的例子：“……在某些打击网络犯罪领域，如打击信用卡偷盗集团以及银行信息盗窃，中国执法部门与美国进行了合作。”¹⁰ 对付网络犯罪的共同历史，可能有助于增加战略信任，为两国之间开展认真讨论(并导致正式的双边会谈)铺设道路，使双方能就打击犯罪、国家安全、网络军事行动等事宜协商制定出坚实行为准则的方式方法。双方之间已经存在一些共识基础，能够支撑美中在网络安全合作上的双边讨论及最终正式会谈。

整体而言，美中两国在网络安全方面的合作需要涵盖军事和非军事网络领域。对军事领域的知情关注和对非军事领域的知情关注，同等重要。在这种合作的基础上，双方可以走向共同网络安全。

谋求共同网络安全

为有助于双方建立信任，让两个大国走向相互保证安全的网络空间关系，本文提出四项建议，相信这四项建议应成为两个大国领导世界建立正式国际条约的长征的第一步。

建议一：规定网络空间恶意行为的通用词汇

参与陆、海、空、天力量辩论的人对武装攻击的含义有一致的理解，就是说，通用词汇及其定义是一切理性辩论的基础。美国及其盟国和世界上其他国家在网络空间投入巨额资金。网络空间不仅是重要的然而漏洞重重的国家基础设施，也是空军和其他军种开展作战和能力建设愈益不可离开的作战领域。本文的目的是鼓励正式的辩论，因此需要我们制定出大家认同的网络空间术语和定义，并最终产生出连贯的国内和国际网空政策、战略和理论。这不只是一个纯粹的学术语义题目。1911年，英国航海理论家朱利

安·科贝特爵士论述了定义的重要性：“如果缺少这样一个工具，没有两个人甚至能顺着同样的思路思考，更难指望他们理出导致分歧的真正所在，找到心平气和的解决办法。”¹¹

关键基础设施

在一些流行的演说、政策辩论和作战准则中，人们常常混淆“网络空间”和“互联网”、“网络攻击”和“网络利用”或“拒绝服务中断”等术语。部分原因是信息和通信技术的融合，经由各种工业控制系统被全球民众使用，支撑着各国的国家关键基础设施的运作，社会依靠这些系统提供二十一世纪生活所依赖的公共事业和其他服务。奥巴马总统最近颁布的一项行政命令朝着区分信息通信技术和工业控制系统迈出了必要的一步，但混淆依然存在。本文将对此做些进一步的澄清。¹²

网络空间包括公开的多功能网络(如互联网)和封闭的固定功能网络(如工业或建筑控制系统)。这两种网络有根本的区别。公开网络的效用取决于网络的用户数量，随着用户数量的增加，网络的效用也随之放大。网络效用最大化的原则是：用户如果信任一个公开网络，相信自己的隐私能受到保护，就倾向于加入。相较而言，封闭的固定功能网络必须确保信息能安全、可靠、经过认证地从传感器传给操作者。工业控制系统的重点放在确保可获得性，即能向重要基础设施和关键资源机器处理过程操作员或操作器提供所需的控制。

工业控制系统因其系统使命特征，在设计上很少考虑安全因素。“震网”攻击和最近其他一些事件表明，它们可能成为军事目标。如果工业控制系统发生故障或遭到破坏，将引发设备受损，资产毁坏，乃至危及生命。

这些系统因设计上的某些欠缺已经导致一些事件发生，造成大规模的损毁。一个例子是2009年萨扬-舒申斯克水电站大坝的爆炸，有分析认为这场造成大规模爆炸和环境损失的灾难是由计算机配置错误引起。如果属实，那么这次事件显示，对计算机实施网络攻击也可能造成如此程度的破坏。¹³ 如果粗心的系统管理员未能适当地实施系统隔离的话，攻击者可以利用互联网发动针对此类系统的网络攻击。现在，随着专门的通信协议、软件、设备配置，以及这些系统操作的标准都在不断改进，也要求攻击者具备更高超的技术才能实施成功的攻击。“极光”（Aurora）漏洞的出现，对电力发电机构成了完全真实的威胁。在美国国土安全部主持的一次演练中，黑客通过远程遥控成功地进入了一台发电机的SCADA控制系统，并能导致物理性摧毁发电机——这次演练支持了把网络犯罪及间谍与网络战争加以区分的必要性。工业控制系统中的很多漏洞是被硬编程到可程序逻辑控制器和远程终端装置及其它系统部件中，因此，修补起来比商业系统更加困难。

定义网络武装攻击和网络武器

现有的国际法框架对如何对待网络战争事件做出了明确的法律和政策规定。《网络战争适用国际法塔林手册》或许是当今对此议题做出最详尽解释的文件，它给出网络攻击的定义是“网络行动，无论进攻或防御，合理预期会造成人员受伤或死亡，或损害或摧毁目标。”¹⁴

如果网络事件中使用了网络武器，就意味着突破了网络武装攻击的门槛，这同使用诸如“火焰”、“宙斯”、“高斯”或其他恶意代码等间谍或一犯罪工具有本质的区别。网络武器可以是指专门攻击工业控制系统的软

件代码，也可以是指嵌入关键系统的硬件缺陷。鉴于工业控制系统的复杂性，要想发现漏洞（所谓零日漏洞），以及找到可攻击目标，获得进入并实施攻击，这一切需要高超技术水平及大量的物力和人力投入。根据国际法，今天只有“震网”事件上升到被视为网络武装攻击的程度，因为它造成了被攻击目标的物理性摧毁。也有人认为，用“沙蒙”（Shamoon）病毒对石油能源设施实施攻击的网络事件是仅次于的第二个事件，这场攻击毁坏了虚拟记录，但后来纪录获得恢复，没有造成大规模财产毁坏或人身伤害。但是，“沙蒙”针对的是网络空间的商业应用，而不是针对可能引发国家安全关切的工业控制系统。

有人会争辩，目的在于获取非法进入某个系统的软件或硬件，只需轻按开关就能导致损毁，网络战争的“不同”正在于此。但这种常常被引用的说法却没有根据。诸如“火焰”、“毒酷”等访问软件也许像一束瞄准激光那样，起到导引武器攻向目标的相同作用。然而，瞄准激光只是武器系统的一部分，导弹的载荷才是武器系统中造成摧毁性效果的实际物体。同理，具体到网络武器，攻击者可能使用先前的进入，导引武器攻击特定目标，但是攻击者还必须研制出另外一套单独的软件，利用漏洞，造成伤亡或毁灭的物理效果。

有人会进一步争辩说，这套软件可以包含在进行网络侦察的工具内，由此产生“按动按钮就能发动网络攻击”的论点。但是，鉴于工业控制系统独有的特征，没有专门针对特定目标的数字和物理环境而制作的网络武器，就不能产生效果。简言之，这需要攻击者勾画出工业控制系统结构图和网络地图，配备程序员团队和密码专家，复制目标的虚拟环境，通过预演测试武器对目标的攻击效

果，然后投入部署和实战。以上的争辩就像是在说，身负击毙本拉登使命的海豹突击队指挥官可以把其对阿伯塔巴德的本拉登住宅的第一次侦察和后来的突击行动合并起来同时进行，指望一气呵成获得成功。事实上，这两种攻击都需要在实施前做大量的准备。

对和平的威胁与侵略行为

低于网络武装攻击门槛的事件，虽然可能带有恶意和具有破坏性，也具有挑衅性，但没有上升到武装攻击的程度。人们常说的分布式拒绝服务（DDOS）属于网络犯罪的范畴，而不是网络战争。中国黑客窃取美国知识产权是网络间谍或盗窃的事例。¹⁵ 虽然网络间谍事件可能对国家安全构成长期的负面后果，但窃取数据本身的行为并非网络武装攻击。

尽管私营界的观点与上面相左，工业间谍不可视为战争行为，不需要政府依据美国法典第 10 卷做出反应，而应以更好的信息安全手段来防范此类犯罪的发生。联邦政府对诸如《计算机欺诈和滥用法》等法律进行修改，将允许私营企业有效保护自己，对数据盗窃行为做出积极的回应——包括销毁被窃数据。

《国防部军语词典》给非致命性武器下的定义是：“专门设计的、主要用于使人员或装备丧失能力，同时尽量减少死亡、人身永久伤害、财产和环境连带损失的武器。”分布式拒绝服务、操纵物流网络中的数据，以及其他软件和硬件事件，都可归于这一类。

由此推论，2012 年末对爱沙尼亚和格鲁吉亚，以及对美国金融行业开展的各种网络攻击，当然达不到网络武装攻击的门槛。这些破坏针对的是互联网的网络层面。但并非所有拒绝服务的事件都是如此。所谓的“简

单网络管理协议过载”（SNMP）就是非网络过载拒绝服务攻击的事例。例如，如果运行陈旧“视窗 2000”的电脑在一个工业控制系统网络上的电脑上为逻辑控制器编制程序，这些电脑就可能成为利用其未修补漏洞的恶意代码的攻击对象，造成“SNMP 过载”。在这个案例中，电脑的内存，而不是网络连接，将会失效。恶意指者可利用这个漏洞，造成系统的停顿，使目标机器上的任何新程序无法启动，于是机器必须关闭，然后重新启动，才能恢复运行。但是许多关键的基础设施必须保持连续运行，否则就会发生事关国家安全的事件。在这种情况下，拒绝服务攻击就不只是针对网络层面的攻击让网站无法访问，而且是针对特定目标电脑的应用层面，有可能导致整个电厂停工。

结论似乎已一目了然——我们必须把关于网络犯罪/网络间谍行为的讨论与关于网络战争行为的讨论截然分开。如果继续交互使用这些术语和概念，目前的讨论就可能从如何保护信息系统，偏移向可能需要做出军事反应的国家安全威胁上去。应对网络犯罪和网络间谍的手段和方式，与打赢网络战争所需的手段和方式，也各不相同。随着美中两国就保护各自重要信息和关键基础设施的网空合作关系逐渐走向成熟，我们必须对各种恶意网络活动做出明确的区分，这一点至关重要。不加区别囊括一切的概括和断言已经不适用。

虽然美国在网络空间一直是技术的开拓者，中国正在证明自己是战略思维的先锋。一名中国军事理论家说：“在未来战场的对峙中，比技术弱勢更可怕的是思维弱勢。”¹⁶ 另一方面，美国一直着重如何使用技术手段解决问题，却不以战略角度来思考如何走出困境，也不知道其技术手段是否有方枘圆凿之

嫌。¹⁷ 于是，中国在网络间谍活动中采取的方式，证明非常有效。

建议二：美国应停止推动互联网自由进程

迄今为止，美国的政策一直侧重于保障互联网的言论自由，以此作为国际接触的主要政策优先。鉴于美国在该问题上的前后不一，以及它在全球网络安全对话中产生的摩擦，继续侧重于国际互联网的自由，只会妨碍美国在国际社会中建立信任。美国领导“互联网自由进程”的努力，致使各方的状况都今不如昔。实际上，创建互联网和监管互联网，是非常不同的两种使命。

固然，言论自由是美国的一项核心价值，但在震撼从欧盟到中国政府的“阿拉伯之春”的背景下，言论自由成了为其背书的辩说理由。世界应该知道，其之需要互联网的言论自由，不在于为了言论自由本身，而在于认识到自由、公开和稳定的互联网能生成强大的经济效益。以促进互联网的繁荣为重，可能比目前强调言论自由更有说服力。立足于这种思路，我们就会更加重视经济效益的得失，而不是在辩论中一味地强调个人的网络自由表达权利。

此外，美国以争取信息自由流通作为一个人权问题而参与公开鼓动和组织“网络活动人士”，导致了国际上的摩擦，对促进国际间网络安全合作适得其反。“互联网自由进程”计划就是这样一个例子。美国国务院公开发“活动人士”软件即翻墙软件，企图帮助这些活动人士避开专制政权设置的网络安全措施。这种技术还能帮助公民活动人士绕过政府的数字哨兵，传播被禁的信息。对俄罗斯、中国，以及其他非民主国家的政府而言，这些活动被认为等同于挑动数字化政权更迭。从他们的角度来说，美国是在帮助和煽动犯

罪活动。这无助于美国在网络安全方面所做的努力。

由于我们把重点落在强调互联网自由的说辞上，就难以在那些肆意滥用信息技术——窃取我们数据，瘫痪我们电脑，甚至引发更恶劣后果——的国家找到愿意与我们合作的伙伴。对很多国家来说，美国国务院推动传播的内容在他们眼中的危害性，决不亚于美国认为的恶意代码或窃取知识产权对美国的危害。

世界各国政府应理解，如果互联网能够发挥其今天的作用，自由流通的信息对其国家的繁荣将产生直接积极的影响。这项美国的发明已经与世界共享，今天互联网作为包容性信息社会的基础，能促进全球社会和经济的发展。如果互联网能允许信息在主权国家所设的合理安全限制内自由流通，这些效益才能得以持续。

建议三：中国国营公司应增加透明度来减少美国的疑虑

在计算机科学和工程方面，中国取得长足的发展。正如美中经济与安全审议委员会的报告说：“如果目前的趋势持续，根据消费、生产和创新，中国（以及其代理利益）将有效地成为包括通信在内的很多行业的主要市场动力。¹⁸ 美国的决策者担心，依赖中国作为电脑芯片和其他信息和通信技术硬件的制造方，会让病毒和后门程序埋伏在美国部门——包括美国军方——使用的设备中。中国制造的电脑硬件价格极为便宜，在亚洲和发展中国家非常畅销。¹⁹ 此外，中国企业，如华为公司，在发展下一代移动 4G LTE 网络标准方面处于领先优势地位。²⁰ 长沙是世界最快超级计算机“天河-2”的所在地，也是中国设计的开放源代码软件“中标麒麟

麟”Linux操作系统的研发基地。²¹虽然设在美国的企业传统上建立了互联网技术的标准，但来自中国的企业，如中兴通信公司，正在国际电讯联盟领头起草的、将影响全球下一代网络的重要国际标准中，发挥越来越重要的作用。

中国当然有权在全球市场上竞争其信息技术领域的份额。但是那些不幸的事件降低了外界的信任，例如发生在2010年4月8日的流量路由误导影响了美国政府和美军的网络，当时“中国电信公司服务器错误地开始在广告上标榜自己是互联网大流量的最佳路径。过去也因简单的配置错误发生过类似的路由变更事件，但这一次无疑是蓄意行为所致。”²²这类事件发生后，却缺乏公开的惩罚，让美国的一些人对中国公司介入美国和盟国境内的通信行业表示担忧。中国的这些通信公司因此被认为不负责任，缺乏透明性，对技术事件不承担责任，因而被拒于美国国内市场大门之外。因此，对中国来说，在这个领域增加一些透明度，将有助于中国通信公司发展壮大，也减少美国公司的担忧。

建议四：明确界定和理解国家间谍的含义

阻碍美中网络安全合作的一个最关键的领域，可能是两国对间谍活动的不同解读。有人认为，美国最近对中国五名军人的起诉，以及美国私营网络安全公司CrowdStrike（众击）对中国间谍活动的更多曝光，将严重打击美中两国在网空领域的合作努力。²³就在此前一个星期，中国人民解放军总参谋长房峰辉将军应美军参联会主席邓普西将军邀请访问了五角大楼。在访问中，中方表示：“目前，中美双方正在依据两国领导人取得的重要共识积极构建新型大国关系模式，两国关系一步一步走到今天来之不易。双方的军事

关系发展表现出积极势头，这对中美两国人民都有益，有助于保证地区和全世界的和平、稳定和繁荣。”²⁴一周之后，美国司法部却根据美国国内法，以中国盗窃美国公司知识产权为由宣布起诉中国军官。美国司法部长霍尔德在新闻发布会上表示：“当一个外部国家动用军事或情报资源和工具来以美国企业主管或公司为目标，图谋窃取商业机密或敏感业务信息，提供给我本国的国有企业以获益，我们必须说：‘够了。’要让他们知道，美国政府将不容忍任何国家以非法手段破坏美国公司，侵蚀自由市场的公平竞争原则。这项诉讼应被视为一声棒喝，宣告美国开始对日益猖獗的网络窃密采取行动。对他们的犯罪指控代表着美国跨出具有划时代意义的第一步，今后将加大努力解决这种威胁。”²⁵虽然这项指控的对象是中国政府和中国人民解放军，起诉书的内容列举了有关犯罪手段和范围的大量细节，可以被解释为美国对外国政府的网空领域行为划出红线。

在美国发出对中国政府支持工业间谍活动的指责之后，中国组织互联网媒体研究中心立刻反击，发表《美国全球监听行动纪录》，但其中对国家间谍行为问题有明显误读。文件中重复列举美国前情报合同官员斯诺登已经曝光的美国机密项目内容。从分析角度看，这份文件没有认真解读美国起诉中国军官的原则立场，这就是，为了国家安全目的开展网络间谍活动和一国政府为帮助本国企业在国际竞争而进行网络窃密的行为有本质区别。当然，文件中确认了美国对这两种活动的区分，也提出了数码时代侵犯个人隐私的合理忧虑。²⁶

起诉事件发生之后，有人可能觉得美中网络安全合作从此走入死胡同。这种观点其实是短视的。大国之间面对战略性挑战，需

要时间、冷静和理性应对。美中网络对话目前（截至本文完稿时）停摆，但未来一定会恢复，两国间的合作努力从过去到现在一直就是这样，在网空领域及其它场合有许多迹象可为印证。首先，今年6月5-6日，中国外交部在北京主办“信息与网络安全问题国际研讨会”，美国派代表团与会。在另一个非网空领域，中国受邀参加了世界最大规模的环太平洋国际海上演习。早先，在中国和俄罗斯等国向联合国大会共同提交“信息安全国际行为准则”后，美国没有给予支持，当时因为国际上对网络空间行为规范并没有取得共识。这本身就表明美中两个大国需要通过对话和交往加深理解，才能领导世界建设起一个有利商业发展与繁荣而非充斥着冲突与猜疑的网络环境。美国反对这份联合国大会议案的主要理由是，这份议案将允许政府对互联网实施更严格控制。眼下，中国激烈反对美国对中国盗窃知识产权的起诉，美国也不支持中俄的议案。但是，美国和中国之

间在网络安全问题上将继续进行政府间对话，双方需要对共同关注的问题协商出共同的立场。只要这些问题存在，双方就必须珍惜过去十多年来建成的合作基础，坚持对话，找到解决方案。

结语

网络冲突，从非法进入到破坏到武装攻击，构成一种新的力量形式。防止网络战争符合所有人的共同利益，它应比任何纯粹的国家福祉利益和国家安全更重要。真正的网络安全不仅应存在于中美两国的合作中，而且应存在于世界各国的集体努力中。中美关系的合作发展是积极的一步。这将要求双方——今天的形势也迫切需要双方——切实放弃过去寻求网络安全的做法。很清楚，从真正意义上来讲，过去的国家安全模式与我们希望实现的网络空间安全目标并不契合——毕竟，网络空间包含着很多的相互依存关系。♣

注释：

1. Stephen Cohen and J. Bradford DeLong, *The End of Influence: What Happens When Other Countries Have the Money* [影响力的终结：其他国家的富有对美国的影响], (New York: Basic Books, 2010); 另参看 Niall Ferguson, "Complexity and Collapse: Empires on the Edge of Chaos" [从复杂到崩溃：面临混乱悬崖的帝国], *Foreign Affairs*, March 2010.
2. 有关两位领导人的引述见 Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting [奥巴马总统和中国国家主席习近平双边会谈后发表的评论], <http://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china->
3. Joseph W. Ralston, "Why the Pentagon Needs Friends in Beijing" [为什么五角大楼在北京需要朋友], *Wall Street Journal*, 5 March 2010.
4. James Fallows, "Cyber Warriors" [网络武士], *Atlantic*, March 2010, 58-63; 另参看 "Mike McConnell on How to Win the Cyber-War We're Losing" [麦康奈尔评说如何打赢我们正在输的网络战争], *Washington Post*, 28 February 2010, B01.
5. Hillary Rodham Clinton, "Internet Freedom" [互联网自由], (Prepared Remarks, Newseum, Washington, DC, 21 January 2010); 另参看 John Pomfret, "China Suspends U.S. Military Exchanges in Wake of Taiwan Arms Deal" [美对台军售后，中国中断与美军事交流], *Washington Post* (29 January 2010), http://articles.washingtonpost.com/2010-01-29/world/36893526_1_china-s-defense-ministry-chinese-energy-companies-china-over-internet-censorship.
6. Richard Rosecrance and Gu Guoliang, *Power and Restraint: A Shared Vision for the U.S.-China Relationship* [权力与自律：对美中关系的共同设想], (New York: Public Affairs, 2009).
7. John Kerry, Solo Press Availability in Beijing, China [约翰·克里在中国北京举行的单独记者会], <http://www.state.gov/secretary/remarks/2013/04/207469.htm>

8. James Areddy, "People's Republic of Hacking" [黑客“人民”共和国], Wall Street Journal, 20 February 2010, p. A1. 文中提到一名被判入狱三年的中国黑客。
9. 请见相关网站：<http://www.justice.gov/usao/nys/pressreleases/May13/WangYongPleaPR/Wang,%20Yong%20Indictment.pdf>.
10. Larry M. Wortzel, "China's Approach to Cyber Operations: Implications for the United States" [中国的网络作战方法：这对美国意味着什么], Testimony to the Committee on Foreign Affairs, U.S. House of Representatives, 10 March 2010.
11. Julian S. Corbett, Some Principles of Maritime Strategy, [海上战略若干原则], (Annapolis, MD: Naval Institute Press, 1988; first published in 1911), p. 7.
12. Executive Order -- Improving Critical Infrastructure Cybersecurity [行政命令 — 改善关键基础设施网络安全], <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.
13. "Insulating oil spreads along Siberian River after Hydro Disaster" [水电站灾难后阻隔石油沿西伯利亚河扩散], RIA Novosti. 18 August 2009. <http://en.rian.ru/russia/20090818/155846126.html>.
14. The Tallinn Manual on the International Law Applicable to Cyber Warfare [网络战争适用国际法塔林手册], <http://www.ccdcoe.org/249.html>.
15. Mandiant Report [曼迪昂特报告], <http://intelreport.mandiant.com/>
16. Timothy Thomas, The Dragons Quantum Leap [龙的量子腾跃], (Fort Leavenworth, KS: Foreign Military Studies Office, 2009), 238.
17. 美国历史上的例子很多。第二次世界大战依靠的是技术优势,并非策略技高一筹。战争初期,美德两军力量相当时,德国人通常会获胜。最近的例子是美国入侵伊拉克。美国以错误的战略走入战争,地面的局势一直到战略赶上技术发展、“增兵”计划实施后才扭转。同上,第13-33页。
18. The National Security Implication of Investments and Products from the People's Republic of China in the Telecommunications Sector, U.S.-China Economic and Security Review Commission Staff Report [中华人民共和国对我国通信行业的投资和产品带来的国家安全考量], January 2011, 7, http://www.uscc.gov/RFP/2011/FINALREPORT_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf.
19. LCDR A. Anand, "Threats to India's Information Environment" in Information Technology: The Future Warfare Weapon [印度信息技术环境面临的威胁：未来的网络武器], (New Delhi: Ocean Books Pvt. Ltd., 2000), 56-62.
20. "Huawei Conducts World's First Commercial Network LTE Category 4 Trial [华为进行世界第一个商业网络LTE四级测试], Cellular News, 9 May 2012, <http://www.cellular-news.com/story/54329.php>.
21. China to create home-grown operating system [中国将研发本土操作系统], <http://www.bbc.co.uk/news/technology-21895723>
22. 请见相关网站：http://www.computerworld.com/s/article/9197019/Update_Report_sounds_alarm_on_China_s_rerouting_of_U.S._Internet_traffic.
23. 请见相关网站：<http://www.justice.gov/opa/pr/2014/May/14-ag-528.html>；以及 <http://www.wtae.com/blob/view/-/26051954/data/1/-/mbff4iz/-/Indictment--PDF.pdf>
24. 请见相关网站：<http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5432>
25. 请见相关网站：<http://www.justice.gov/iso/opa/ag/speeches/2014/ag-speech-140519.html>
26. China Internet Media Research Center, "America's Global Surveillance Record" [美国全球监听行动纪录], http://www.chinadaily.com.cn/America's_Global_Surveillance_Recordworld/2014-05/26/content_17539247_5.htm (26 May 2014).



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员, 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。

陆军科曼奇人直升机项目对空军勒颈之结的启示

The Comanche and the Albatross: About Our Neck Was Hung

迈克尔·皮鲁查，美国空军上校（Col Michael W. Pietrucha, USAF）

就是 F-35，我们别无它选。

——美国空军参谋长马克·韦尔什将军

美国空军计划装备 F-35A，最终取代越战后战斗机群中的大部分飞机。按照原先设想，这款隐形飞机不仅采用当前最新技术，造价亦不会高于其将取代的飞机。空军希望采购 1,763 架 F-35A，替换 2001 年在服役中的所有的 F-16、A-10 和 F-117。F-117 曾在海湾战争中大显身手，空军受此鼓舞，在海湾战争后制定的新飞机采购计划注重飞机躲避雷达的低显性。F-35 联合攻击战斗机的设计目标是向美国空军、海军和海军陆战队以及若干盟国提供数种新款作战飞机，它将给美国空中力量带来划时代的变革。

然而，这项采购计划诸事不遂，五角大楼的采购计划主管称这个项目为“胡管乱理”，而且进度延误，预算超支。¹ F-35 没有像原先预想的那样成为成本适中、性能可靠、可在 2015 年大量服役的战斗机，其交货期一拖再拖，其成本不断攀升。² 其间，这项进度拖延、性能未达标、成本骤增的采购计划又迎头撞入了 2011 年预算控制法案营造的严峻预算紧缩环境。³ 但更需关注的是，该计划源自过去以北约为中心的几十年冷战经历，而且空军当时没有考虑到太平洋战区的需要，也没有想到敌方拥有像中国那样的防空能力。有鉴于此，尽管在过去的十几年中已经对该计划投入了大量的人力和财力，预算现实应该促使我们重新审视空军对 F-35 计划的参与以及其战斗机群的未来。

TACAIR = 战术空中作战

为时未晚，我们还有选择余地——如果我们愿意考虑重新选择。美国陆军对“科曼奇人”（Comanche）直升机研制项目的处理是其航空史上一个具有魄力的决策，使得陆军航空兵实现了现代化和装备汰换。这个例子也为空军发展指出了一种可能方向，它应该启发空军认识到几点，一是空军对保障国家安全至关重要，二是任何一种飞机在保障国家安全中都从未证明非我不可，再一点是空军应该防止为了追求单一的作战平台而危害国家空中力量的整体作战能力。本文提出另一种未来兵力结构，目标在于建设起一支机动灵活、战备全面、功能多样的空中作战部队，恢复在 1990 年代基本上被空军抛弃的“高低搭配”混合编制。⁴ 本文把这种未来部队称为“替代部队”，它比按目前发展计划所将建成的部队具有更宽广的作战能力，且成本更可承受。

“科曼奇人”项目

在关于 F-35 联合攻击战斗机计划的讨论中，核心问题是，一般认为这个采购项目无法取消——因为该计划结构庞大，涉及美国国内和国外许多部门，任何想取消该计划的企图都将以失败告终。尽管许多人不愿意终止该计划，如果真想终止的话，也并非不可能。显然，陆军对“科曼奇人”项目的处理有启示作用。

2004年，RAH-66“科曼奇人”直升机的研发已进入第22个年头，多年来它一直是一项重大的国防采购计划，当时已制造了两架样机，计划进展顺利。但是陆军毅然刹车，原因是对该款直升机的用途存有疑问，同时预期到其成本难以承受，并且已有一种可信的替代方案。陆军代理部长雷斯·布朗利（Les Brownlee）和陆军参谋长彼得·斯库梅克将军（Gen Peter Schoomaker）共同宣布了计划终止，并解释道：

我们仔细审查了航空部队的资金使用计划，认为这些资金可提供的某些作战能力不再适应已经变化的作战环境。因此，斯库梅克将军和我建议终止“科曼奇人”直升机项目，重新分配这些资金，用于重组和增强陆军航空兵。我们的建议已获得总统和国防部长的批准，因此，我们在今天早上开始向国会的相关议员做简短汇报。⁵

终止“科曼奇人”项目的关键措施是，经由参谋长联席会议和国会同意，将原先拨给该计划的资金全部用于提高陆军航空兵的作战能力。今天，陆军旋转型机队的平均机龄低于2004年的机龄，AH-64E直升机即将开始量产，八年前根本没有出现的无人机也已在陆军投入使用，而且旋转型运输机队已经大体上实现了装备汰换，连陆军国民警卫队也用上新装备。2004年，陆军断然下马了“科曼奇人”项目，在同期的两场战争中，陆军航空兵皆表现不凡；倘若在2004年继续推进“科曼奇人”项目，陆军未必能达到这样的表现水平。⁶陆军砍掉“科曼奇人”的处理方式甚为得体，没有造成任何政治风波或财务问题。原先的资金分配给陆军其他航空计划，基本上调拨给原本应收到“科曼奇人”项目拨款的相同地区的相同承包商。

不错，“科曼奇人”和F-35计划之间的相似点到此为止。F-35计划的规模要大得多，目前已在生产飞机，而且涉及到已向该计划不同程度投资的许多国际合作伙伴。但是，终止F-35计划，以便能够重新设计战术空中作战（TACAIR）机群体系的理由不变：占用这些资金的某些作战能力不再适应已经变化的作战环境，沿着目前的道路继续走下去，对美国和合作伙伴国家都没有好处。

我们面临的挑战

即使资金没有限制，终止F-35计划的理由仍然存在。具体而言，F-35的性能没有达到当初的要求，其有效载荷偏低，航程偏短，而且中国通过间谍活动也许早在飞机投用之前已经对其性能了如指掌。⁷我们对于作战环境的假设是在十几年以前做出的，已经不符合目前的威胁现实（威胁更严重）和潜在敌方现实（敌人更多元化）。该款飞机的使命是突破最先进的防空系统，对劲敌的重要目标投放精准制导弹药，但是对这项使命，说得最客气些，是令人怀疑；尤其是，如果敌方位于印度洋和亚太地区，我们在那里的基地受限，航程太长，并且潜在敌方拥有后勤优势。尽管政府声称支持F-35计划，空军必须记住，它对国家的贡献主要是空中力量，而不是任何特定类型的飞机。在资源紧缩的环境下，我们在排列重要性时，必须把对F-35的执意追求放在满足联合TACAIR的要求之后。

若干相关的挑战都与空中作战部队的未来结构有关。这些问题不仅是训练资源不足，而是产生于已持续二十年的部队缩编。首先，财务撙节导致的部队结构缩减趋势仍然存在，迫使我们在今后几年仍要跨越一些关键的障碍：

1. 自 EF-111A 和 F-4G 退役以来的将近二十年间，空军压制敌防空系统的能力有所减退。空军汰旧而未换新，更严重的是，没有更新机组人员（海军则不一样，他们不断增添 EA-18G Growler [咆哮者] 飞机）。空军的 F-22、F-35 和 B-2 飞机原本可提升其作战效能，却缺乏支援能力，不得不依赖海军的支援。

2. 空军没有成本适中、可灵活部署的、适合非正规战争的轻型攻击 / 武装侦察飞机。更糟糕的是，除了 A-10 之外，空军的高速喷气式战斗机 / 攻击机均无法使用跑道偏短或道面粗糙的机场。这个弱点给空军的全球到达愿景制造了难题，因为即使有加油机的支援，空军仍无法在全球许多地方提供持久的 TACAIR 掩护。倘若没有舰载机队提供短期掩护，空军基本上没有其他方案可向远在海外各处作战的部队提供空中作战部队支援。如果苏联人当初没有在伊拉克和阿富汗建造大型机场，我们可能早在十年前就会碰到这个问题。

3. 建立基地的机会不多，世界各地绝大多数机场没有能力支援现有的或未来的战斗机。空军难以从简陋的基地、依赖薄弱的后勤供应线和当地支援来运作小型部队，我们没有做这样的准备也没有配置这样的装备。如果我们能够重视那些只需要简单支援的飞机，成立更多装备这些飞机的中队，把他们部署到世界各地许多机场，就能生成敌人难以抵抗的高效作战能力，尤其是在南美、非洲和太平洋地区。在亚太地区，如果我们的飞机能使用 6,000 英尺跑道起降，则可使潜在的基地数目增加两倍以上，并使无法建造长跑道的岛屿基地有机会发挥作用。

4. 缺少充分数量的飞机用于提升实战经验和资质的跟班飞行实习，已经导致空军的战斗机飞行员不敷使用，使求大于供，且这种状况预计将远远延续到 2024 年之后。甚至这个日期预测也只是一纸妄测，不是认真研究供求关系平衡的计划分析结果。如果不快速补充硬件装备和扩充飞行员训练管道，我们将没有足够的战斗机 / 攻击机飞行员配备到这些中队中，将无法执行所有的相关任务，包括进行测试、训练飞行员、参加专业军事院校学习和补充技术等级岗位。⁸

5. 空军实际上没有能力向买不起 F-16 的伙伴国家空军部队提供作战飞机——这个问题在组建或重建这些国家的空军部队时造成了特别的困难，尤其是在亚洲和非洲。为阿富汗空军采购轻型空中支援飞机时遇到了很大的障碍，而缺乏战术手册，缺乏成熟的战术 / 战技 / 战规，以及缺乏有经验的机组人员来训练阿富汗飞行员，则使得情况更加复杂。

6. 过去十年，空军花费了大量的时间和精力，努力提高自身的近空支援能力和北约合作伙伴的这种能力。由于对地攻击机的数量减少而飞行成本上升，空军已经没有足够的架次可用于支援联合终端攻击控制员的近空支援训练。

7. 至于国土防卫，海关和边界巡逻队 / 海岸警卫队的直升机和高速喷气机之间有一段武器系统的缺口，我们却没有一个合适的武装平台能填补它，因而当我们需要截击慢速飞行的飞机时，总是面对作战能力与目标不匹配的问题。

8. 使用高成本、老机龄的 F-15 和 F-16 执行领空主权警戒任务，一直是高能低用式的巨大浪费，完全可以由现代化的低成本飞机去执行。空军国民警卫队面临的这种挑战

特别明显，因为旧型号战斗机和 A-10 飞机纷纷退役，致使它持续丧失前线作战能力。

执意追求 F-35，使得上述各问题越来越严重，不仅是因为该款飞机不能填补所有的空档，而且因为涉及的资金数额庞大，空军根本不能获得解决问题所需的资源。问题的症结，在于我们死抱着二十年以来的愿景不肯放开，坚持发展完全由先进的低显性战斗机组成的“全部第五代”机群。⁹ 这个思路把全部筹码押在了臆想中与某个同等对手对决的未来冲突，固执地假设只要这支战斗机部队设计成能打赢强度最大的冲突，就能自动适应其他任何突发事件。但要想实现这个愿景，将需付出很高的机会成本，将在兵力规划和开展作战两方面都引发大量的风险。

评估改变采购方向的可行性

空军坚持宣示的战略，是采购全部 1,763 架 F-35 飞机，这个采购目标对现有的 TACAIR 机群带来了重大伤害。不仅新近升级的 A-10 行将退役，空军并在实施前所未有的全军兵力结构缩编，缩减各种型号战斗机和攻击机的实力。2013 年，17 个战斗机中队因飞行时数不足而停飞，与此同时，空军却试图加快 F-35 的生产速度。¹⁰ 尽管 F-35 的成本不断上升，但空军仍竭力试图大量采购，此举已对旧型号飞机和 F-22 飞机的飞行时数及升级造成不利影响。目前，战斗机飞行员的飞行时数大致上是海湾战争时期的一半，低于中国和若干欧洲盟国飞行员的飞行时数，情况不容乐观。¹¹

“精简战斗机”做法也严重影响到空军国民警卫队和空军后备役人员储备，其中有些战斗机和攻击机单位只能改行，从飞行 A-10 和 F-16 转为执行空运任务或操纵遥控飞机，

其他一些单位则完全停止了飞行任务。¹² 这个做法尽管有短期节省资金的效果，但是改变了空军后备部队作为战略后备队的作用，也丧失了“返聘”那些离开常规空军部队的现役飞行员和维护人员的机会。空军后备部队应该调整，使其重新拥有各种航空作战能力，重新配备执行领空主权警戒任务所需的装备，充分发挥其驻守地点靠近陆军和海军陆战队基地及训练区域的优势。调整装备后的空军后备部队可包括各型作战飞机，从升级的第四代战斗机直至 OA-X 和 FT-X 等轻型飞机。¹³

即使减少 F-35 采购数量，仍然会有问题，因为自 2001 年以来，单机成本已经上涨一倍，支援一支任何规模的 F-35 机队都需要庞大的经费。¹⁴ 该款飞机的测试计划至今完成了大约三分之一，空军对其实际成本和作战能力仍然不太了解。在本文撰写之时，该款飞机刚在测试场试用其第一批武器。在许多方面，很难对 F-35 提出反对意见，因为它的潜力基本上仍是未知数，关于它的讨论往往是围绕着它“能够”做什么，事实上，目前还没有可用于实际确定其性能的作战测试数据。在这种情况下，尽管缺乏测试或验证，人们将该款飞机“应该”能够或“也许”可以做什么视为既定事实。

空军执意追求“第五代”战斗机，视其为一项必不可少的作战要求。这种观点的一个关键缺陷是，它在两个方面基本上是“立足于信念”。首先，不管 F-35 计划的发展史如何，这种观点认定我们期望的作战能力将会兑现。其次，空军继续相信飞机以其雷达低显性能有效对抗未来的防空威胁。需要提醒的是，对这种隐形能力的假设不一定能站得住脚。在 1991 年的海湾战争中，F-117 飞机确实能够有效对抗伊拉克的凯利（Kari）

防空系统，但是，未来战争的敌方已经有二十年的准备时间来对付美国隐形战斗机；何况 F-35 的红外、目视和放射源显迹性都大大高于 F-117，因而其以隐形能力对抗敌方防空系统的胜算并不大。¹⁵ 海湾战争仅仅八年之后的 1999 年，一种早在 1959 年投入实战的地空导弹系统就找到了 F-117 的软肋。有鉴于此，我们不应该假设，自海湾战争以来的几十年间，俄罗斯和中国的雷达研发团队一直无所作为。

F-35 计划的支持方，在辩论中总是强调一种高端威胁环境，但是此环境远非是全球性的。实际上，只有俄罗斯和中国能够建立这样的反进入 / 区域拒止 (A2/AD) 环境，这种环境便成为我们大规模投资于隐形飞机的合法理由。空军领导人正确地考虑了未来敌方可能拥有的其他作战能力，但在现实中，世界上只有一支部队飞行着真正的隐形战斗机——那就是美国空军。¹⁶ 自 1980 年代后期以来，美国空军是唯一拥有隐形战斗机的部队。即使再过十年，仅凭我们现有的 F-22 机群，也几乎肯定超过所有其他型号的外国第五代战斗机的总和。

自越南战争以来，美国空军没有在空中空战中损失过一架飞机。在过去二十年间，各国的地面防空能力有巨大发展，但是尽管潜在敌方可以获得某些高精尖系统，真正能够购买和操作这些系统的国家毕竟有限。除了中国和俄罗斯，不存在来自先进综合防空系统的大型威胁。此外，如果有人试图证明我们有必要发展短程战斗机而举中国为例，显然不恰当，因为这种战斗机的有效载荷有限，而且必须从处于中国强大导弹攻击射程内的岛屿基地起飞。

在这些事实面前，风险计算中把隐身性置于性能、航程和载弹能力之上的做法必然令人质疑——F-35 有可能是在整体表现上显著不如上代机型的第一款现代化战斗机。不错，F-35 的许多作战能力是保密的，不能完全披露，公众也无法对这些能力展开辩论。但是，如果我们把雷达低显性列为首要考虑因素，而牺牲战斗机必须具备的许多其他特性，那么追求隐身的同时也是受制于隐身。如此安排轻重缓急，确有可能损害战备状态、部队规模、弹仓深度（弹药供应量）以及组建和维持一个机队所必需的其他兵力结构因素；机队用途受限变窄，就难以应对世界各地 TACAIR 中的大部分挑战，何况这款飞机能否突破西太平洋地区的反进入 / 区域拒止环境还无定论。

一项立足于能突破先进防空系统的假定能力的战略，只有在它不阻碍其他能力建设的情况下，才是可行的。如果部队设计仅注重某个专项精锐作战能力，只追求在有利条件下战胜某些敌方，而且只推崇该项战略，那么我们将显著降低自身作战能力的灵活性，不啻是放弃眼前必要的空中力量使用选项，而去追求那种要在十几年以后才可能兑现的单一作战能力。执意追求高成本和现代化的高精尖空军部队，已经对我们的兵力规模、结构和飞行时数产生负面影响，并且导致我们不再拥有许多领域的专业经验。空军过去追求 F-22，现在追求 F-35，放弃了专用的电子战战斗机，冷落了支援这些飞机的训练计划以及熟悉电子战的机组人员，使得电子战飞机成为海军和海军陆战队的专用武器。鉴于 A-10 即将退役，看来近空支援能力难逃和电子战能力一样的命运。

替代方案

要批评一个开发项目，很容易；事实上，所有的先进战斗机项目都在开发阶段遭受过猛烈的批评。但如果没有真正的替代方案，批评再猛，也无济于事。不愿意探究替代方案跟不存在替代方案不是同一回事。本文提出替代部队的建议，旨在尝试说明替代方案不仅存在，而且可以为美国及其国家利益提供更强大的国防力量。

在规划替代部队的结构时，关键在于合理地比较数量有限用途窄而精的 TACAIR 部队与规模更大用途更广且能应对上述各种常规挑战的部队，在两者之间做好平衡。鉴于我们已经拥有的 F-35 在数量已经超过过去曾经拥有的 F-117，本文建议的替代方案并未完全抛弃 F-35 部队，而是呼吁空军在 2014 财年之后终止对 F-35 计划的参与。本建议希望达到以下几个目的：

- 维持有限数量的 F-35A（已经采购的那些飞机），替代因 F-117 退役而损失的作战能力；
- 建立一支现代化的 TACAIR 机队，此机队采用高低搭配，包括经过现代化升级的旧型战斗机、轻型攻击机，以及多用途喷气教练机 / 攻击机；
- 挽回 F-35 计划的某些“成本损失”，使用先进的系统对旧型战斗机进行现代化改造，即把第五代系统安装到第四代飞机上；
- 恢复空军的压制敌防空系统 / 电子战战斗机和机组人员；
- 扩充空军的全球到达能力，包括提供可部署的 TACAIR 资产，这些飞机可利用较短的粗糙道面跑道起降，而且只需要很少的后勤支援；

- 增加跟班飞行实习位置和机会，使空军扩充战斗机 / 攻击机飞行员人数，达到作战要求；
- 投资研发成本适中、可供出口的“轻型作战飞机”，该类飞机衍生自空军教育训练司令部的 T-X 计划；
- 允许空军国民警卫队保持其战役后备队的地位，并继续充当有经验的战斗机 / 攻击机飞行员的“减压阀”，同时更新改造其空中作战部队；
- 建设一支符合国家需求的 TACAIR 部队，即使面临燃油成本上涨和预算缩减，仍能保持必要的空中力量作战能力。

根据这种部队设计，我们可有效地利用原先打算用于 F-35 的各种传感器和系统，把它们安装到新建的和改装的 F-16 及 F-15E 中。目前已经大致上在实施这个过程，但经费没有完全到位。对未来的部队结构做这样的调整，可终止 F-35 计划，代之以先进的第四代战斗机，把隐形特性推迟装备到未来某代飞机。这个设计方案涉及把大量资金用于第四代飞机的改良，保留 A-10，并且增加数百架 OA-X、FT-X 和 AT-X 飞机。

在谈论这种部队设计时，有必要对全球环境做某些假设：

1. 最有实力的潜在敌方仍是中国，伊朗和北朝鲜也拥有各自独特的挑战力量。
2. 海外永久基地没有发生大的变化。
3. 至少到 2024 年，空军的经费一直按自动削减法案降低。
4. 中国维持目前水平的军费开支，并且继续发展作战航空部队和战区弹道导弹。

中国、伊朗及北朝鲜的统治体制基本上没有变化。

5. 美国中央司令部和 / 或美国非洲司令部责任区域内仍需要继续部署战斗机。
6. 现有的 B-2 和 B-52 部队没有变化。
7. 燃油成本继续上涨。¹⁷

这种部队设计还反映了这样的现实：自越战以来，美国卷入的非正规冲突多于正规冲突——但是如果部队设计中放弃对同等对手的威慑效应，会产生不必要的风险。本文的替代设计方案在包含 F-16 和 F-15 的高低搭配模式的基础上再做扩展，形成高 / 中 / 低搭配，构建出所需的 TACAIR 能力。¹⁸

兵力结构设计

现有的 F-22 机队是 TACAIR 高 / 中 / 低搭配模式中的高端部分。一个超大型 F-35 联队将填补 F-117 退役后遗留的隐形战斗机空档，该 F-35 联队参照驻守内华达州托诺帕测试场的第 37 战术战斗机联队形式组建。但高端飞机中的主要构成，将是升级后的 F-15C、F-15E 和 F-16C/D/F。第四代机队的许多升级装备将来自 F-35 计划，其中包括已可投入实战的 F-35/F-22 的先进子系统，将被改装到旧型战斗机上。实际上，F-15E 和 F-15C 已经在进行某种程度的升级改装。传感器和电子战装备的升级应尽可能在空军内部全面推广，包括本文其他部分未予论述的 B-52 等。空军应该购买数目有限的新飞机，以 60 架 F-15G 和 72 架 70 批次的双座 F-16F 作为基线配置。购买的这些新飞机只是起到部分补充作用。装备 70 批次 F-16F 的飞行中队将是 40 批次飞行中队的就地升级，F-15G 则替代久已退役的 F-4G/EF-111A 以及随之消失的重要飞行

经验。¹⁹ 在经济上可行时，现有的第四代飞机若仍有较长的使用寿命，应升级到一个共同标准。

TACAIR 高 / 中 / 低搭配模式的中档部分将包括 A-10 和各型 T-X 飞机 (FT-X 和 AT-X)。A-10 有它自己的疲劳问题，新增 OA-X 飞机 (见下文) 可允许空军减少 A-10 数量，递减到能确实可信地支援朝鲜半岛作战行动为宜。空军应该购买 F-X 飞机的三个变型，作为 T-38 的替代机。基本型 T-X 实质上是 T-38 的现代化版本，现货随取，它将构成数目最大的机群 (400 架)。AT-X 将是 T-X 的全天候、多用途作战机型，拥有空对地作战能力，包括火炮、火箭和精准制导弹药。FT-X 将是一款全功能轻型战斗机，配备现代化机载截击雷达和空对空导弹，可与 F-16C 媲美。FT-X 非常适合空军国民警卫队执行领空主权警戒任务，亦可用作假想敌攻击机。因此，它可以替代已到达使用寿命期限的空军国民警卫队 F-16 飞机。AT-X 和 FT-X 还可作为低成本、双用途战斗机 / 教练机用于出口 (类似于 F-5A/E)。TACAIR 有人驾驶高 / 中 / 低搭配模式的低端部分是 OA-X 飞机，它是空中作战司令部设想的一种现代化涡轮螺旋桨轻型攻击机，用于补充现有的 TACAIR 飞机，但直接升级的 A-10 飞机则属例外。OA-X 将承担非正规战争和反恐部署任务，并按需提供领空主权警戒支持。²⁰

下文概述在没有 F-35 的情况下未来空中作战部队的组成。去年 4 月，美国空军总部 / A8 (战略计划与项目部) 的有关人员采用利弊权衡分析工具，针对空军的空中优势和全球持续打击武器系统所需的预期经费，以 2023 年为截至点，做了一系列成本预测。²¹ 这个基于现实的评估使用锁定在 2011 年预算控制法案预期支出水平的预算基线，计算出

实际国防预算增长率仅为微不足道的 0.3%。从 2014 财年到 2023 财年，所有用于 F-35 的采购经费都重新调拨给空中优势和全球持续打击武器系统，其中不包括 MQ-9、B-52 和 B-2 飞机。²² F-35 的研究、开发、测试和评估经费不变动，但用于系统转换和已采购飞机的维护，当然这么做根本谈不上成本效益。以下表 1 反映装备汰换后可用的现役战斗机 / 攻击机（加上 B-1）总数。最后两列数字表示与 2013 财年规划兵力展望（1,763 架 F-35）

相比较的飞机和驾驶舱座位增量。在有些方面，这个比较是不公平的。例如，2013 财年规划兵力展望测算已经比甚至在自动削减措施实行之前的预期预算限额超出几百亿美元（尤其是五年后的预测），而本文所述替代部队的费用并没有超出自动削减限度，并且没有所谓的预计效率改善或从其他武器系统移用等小花招。

根据上述预测，战斗机 / 攻击机部队在 2023 年的总共可用飞机可达 2,100 架，比未

表 1：战斗机 / 攻击机编制替代方案，2023 年可用飞机总数

| 使命平台设计系列 | 来源 | 空军常规部队 | 空军后备部队 | 总计 | 飞机增量 | 驾驶舱座位增量 |
|--------------------|-----------------|--------|--------|-------|------|---------|
| F-22 | 现有 | 167 | 20 | 187 | 0 | 0 |
| F-35 | 现有 | 56 | 0 | 56 | 0 | 0 |
| F-15C/D | 升级 ^a | 113 | 116 | 233 | -16 | -16 |
| F-15E | 升级 ^b | 218 | 0 | 218 | 0 | 0 |
| F-15G ^c | 新建 ^d | 60 | 0 | 60 | +60 | +120 |
| F-16C/D | 升级 ^e | 377 | 361 | 738 | -282 | -282 |
| F-16F | 新建 ^f | 54 | 18 | 72 | +72 | +144 |
| AT-X | 新建 | 38 | 18 | 56 | +56 | +112 |
| A-10C | 现有 | 60 | 90 | 150 | -133 | -133 |
| FT-X | 新建 | 36 | 58 | 94 | +94 | +188 |
| OA-X | 新建 | 132 | 108 | 240 | +240 | +480 |
| 战斗机 / 攻击机总计 | | 1,311 | 789 | 2,100 | +91 | +613 |

a F-15C/D 升级包括红外搜索与追踪、主动电子扫描阵列雷达 (APG-63v3)，以及鹰式被动 / 主动告警生存系统 (EPAWSS) 升级至电子战系统。

b F-15E 升级包括 APG-82 雷达和鹰式被动 / 主动告警生存系统 (EPAWSS)。

c F-15G (波音称为 EF-15E) 把电子战系统从 EA-18G 移到 F-15E+。

d 新建飞机的价格根据现有实例制定，包括采购费用和运行及维护费用。F-15G 的单价是 1.10 亿美元，F-16F 的单价是 7,000 万美元。AT-X 的价格参照英国皇家空军 Hawk T2 飞机，换算成美元的单价是 3,300 万美元；FT-X 的单价是 3,500 万美元。OA-X 参照轻型攻击机 / 武装侦察机定价，上调 20%，单价是 1,200 万美元。

e F-16C/D 升级主要是 40/42/50/52 批次飞机，升级内容包括战斗航电系统程序扩展组件雷达 / 电子战系统升级，以及使用寿命延长。

f F-16F 是 70 批次 F-16 机型，参照以色列国防军的双座中程 F-16I Sufa 飞机。

表 2：轰炸机编制替代方案，2023 年可用飞机总数

| 使命平台设计系列 | 来源 | 空军常规部队 | 空军后备部队 | 总计 | 飞机增量 | 驾驶舱座位增量 |
|----------|----|--------|--------|----|------|---------|
| B-1B | 现有 | 20 | 0 | 20 | -18 | -72 |

受限的规划兵力展望测算多 91 架，与此同时，驾驶舱座位也有增加，因为每架新飞机都是双座飞机。²³ 表 1 没有列出全部支出款项；B-1B 飞机数量有所减少（见表 2）。

到 2023 年，整个替代计划将淘汰 18 架 B-1B 飞机、仍未更换机翼组件的 A-10 飞机，以及型号最陈旧的 F-16 飞机，代之以 540 架全新的 F-15G、F-16F、OA-X、AT-X 和 FT-X 飞机。空军长期闲置的电子战战斗机将重新入列，从而减少对短程 EA-18G 的依赖。资源再分配计划包括把整个全球持续打击 / 空中优势自动削减经费和弹药经费用于 80% 的必需作战储备以及旧型飞机的现代化和升级。训练和测试场经费不挪作他用。在目标年份，轻型作战飞机（OA-X、FT-X 和 AT-X）的生产线保持开通，以便今后在支出紧缩的“船头浪”过去之后继续采购，并且有助于研发远程攻击轰炸机和第六代 F-X 飞机。总之，替代方案不仅存在，而且能够使空军恢复长期闲置的作战能力和扩大部队规模。

战略风险管理

这支替代部队是否可行，与兵力结构的讨论密不可分，而兵力结构关系到能否实现二十一世纪空中力量的预期发展。我们可以合理地假设，涉及联合部队的任何冲突也将涉及空中力量的运用；因此，我们应该仔细思考空中力量会给作战行动带来什么影响。

我们已经习惯的思维方式，是对潜在的冲突加以分类，从“最有可能发生”直到“最

有威胁性”，然后认定最有威胁性的冲突是最重要的。在伊拉克和阿富汗战争中，空军遵循了这种思维方式，结果却令人遗憾，空军让旧型号喷气战斗机担任主战飞机，这些飞机在此两场战争中只使用了很小部分的作战能力。空军偏爱的兵力结构注重最有威胁性的冲突，而这经常是指与实力等同或相当的敌方国家的正规武装部队进行大规模作战行动。

第五代战斗机被标榜为应对最强威胁的克星，仿佛我们必须使用这种飞机才能与实力相当的国家打仗。这种态度是典型的思维惯性使然，认为优势技术将给美国带来胜利，而如果我们缺乏技术最先进的飞机，就无法打赢。这种依赖装备和忽视战略的想法，没有考虑到包含各种空中力量作战能力的作战方式具有多种可能性，而是偏重某个非常具体的专项精锐作战能力。事实证明，这种想法是错误的。在越南战争中，我们明显拥有技术优势；在朝鲜战争中，双方大致旗鼓相当；而在二次大战中，我们可以说在技术上落后于德国空军。但是，这几场冲突的结果和飞机技术的优劣并无必然联系。

从 2001 年以来流行的想法和做法是，除了最有威胁性的冲突之外，其他任何可能的冲突都属于“次等冲突”，都可以由精锐隐身战机部队有效摆平。在他们看来，F-35 既然能够应对所谓的高端威胁，自然对其他任何形式的冲突更不在话下，因此特别被视为具有多种适用性。然而，现实情况并不支持这个结论。以阿富汗战争为例，我们当时根本

不能像使用 F-16 和 F-15E 那样部署或使用 F-35——我们负担不起这款飞机的运行维护成本及燃油消耗，更何况会造成飞机寿命递减。²⁴ 即使在伊拉克和阿富汗战争中使用第四代飞机，其成本也显著高于用现代化轻型攻击机实施相似的战略，因而“次等冲突”思维和做法给装备、后勤和人员都造成严重的负面影响。²⁵

实际上，根据有案可查的西方军事史，非正规冲突是最有可能发生的战争形式。²⁶ 从伊拉克撤军和最终从阿富汗撤军都不能预示美国从此将不再参与非正规战争。目前，美国仍然涉足马里、菲律宾、阿富汗、巴基斯坦、也门、约旦、乌干达和非洲之角的事务；利比亚冲突的记忆逐渐淡薄，而叙利亚仍有可能成为冲突的热点。此外，各类冲突的分界线可能非常模糊——如果美国与中国为了台湾而发生冲突，只要是限制在常规冲突范围，也许算不上是对美国威胁性最大的冲突；另一方面，如果若干非正规挑战交集起来，却很有可能导致最具威胁性的局面，尤其是涉及某个拥核国家崩溃，或丧失关键资源、领土或某些全球共有资源使用权的时候。

使“次等冲突”思维方式更站不住脚的，是那种认为针对威胁性较低而范围较广的挑战所组建的部队其作战能力必定较弱的观点。非黑即白（隐形 / 非隐形）的二元分类法总是把续航力、军械多元化、载弹量、机动性、燃油经济性、航程和粗糙道面机场起降能力等作战能力因素视为无关紧要。冲突发生的环境是任何战争的决定因素之一，无疑会影响可运用的空中力量作战能力的选择。如果所有的环境、战略和敌人等都属于“次等冲突”类，都可用“隐形飞机”这一副药方来解决，那么我们建造庞大的 F-35 机队尚有其道理——假如能买得起这些飞机。但是，

如果事实并非如此，那么我们就是在忽视因无法应对迅速扩散的“最可能发生的冲突”而导致的后果，或者说把非正规战争视为“次等冲突”的明显后果，而固执地用 TACAIR 高速喷气机应对非正规挑战，全然不顾十几年来的事实对这种方式的效果的验证。

让部队全部配备第五代飞机的做法，还忽视一支灵活机动的部队所具备的多用途适用性和威慑价值。机动灵活的部队能够执行多方面的任务，尤其是在危机突发、形势充满不确定因素的情况下。只要风险在可承受范围，把作战航空兵部署到前线总是有价值的。对此类风险的判断同飞机的隐形特性没有关系，我们需要考虑的是，如何才能把空中力量快速部署到严峻环境中，如何在人力有限的情况下，在没有备好的基地和固定的基地设施的情况下开展作战行动。如果我们想把 OA-X 或 AT-X 飞机部署到乌克兰，这个决定马上就能做出，即使我们知道这些飞机面临地面火力威胁；相比之下，想用 F-35 飞机进行同样部署，其决策要艰难得多。假定驻欧美国空军目前拥有轻型作战飞机（OA-X、AT-X 和 FT-X），这些飞机仅靠少量后勤支援就能够从乌克兰简陋的机场起降，那么，面对俄国的非正规威胁，驻欧盟军最高司令官无疑可以睡得更香一点——凭这些飞机就足以保卫克里米亚。

分别以“最有威胁性”和“最有可能发生”为据而展开的无谓争论，其所围绕的是利弊交换的假命题。仅只针对最大威胁而设计的部队结构具有根本缺陷，因为它立足于一个错误的假设，认为解决反进入 / 区域拒止挑战只需要动用第五代战斗机，更具体地说，是一种在没有电子战 / 压制敌防空系统能力支援下的、需要长跑道的短航程战斗机。一支部队，如果抛弃了应对最有可能发生的冲

突所需的作战能力，将难以满足国防需要，因为这样的部队结构设计还基于另一个错误的假设，认为按最有可能发生的冲突而建设起来的部队不可能对同等对手产生威慑效应，因而没有什么价值。²⁷这两种假设都忽视了战争艺术的基本道理。如果我们拥有更多的可选方案，能够从更多的地方实施兵力部署，我们就有更多的机会获得对敌作战优势。如果我们蓄意减少可选方案，就会让敌方有机可乘，他们将专门针对作战能力狭窄的美国空军，组建和训练自己的部队。

最终结果

本文从大范畴出发建议的替代部队设计，将使战斗机/攻击机中队数量增加，使可用于跟班飞行实习的飞机数量大幅度提高，同时可减少规划兵力展望所测算的运行维护费用。²⁸这个替代方案指出，战备状态产生问题的主要原因之一是高速喷气机队承担的轮值负担过重，并据此设计出另一种部队结构，从而把大部分轮值负担转移到成本最低、运行维护费用最低、燃油消耗也最低的飞机上。按照这种方案，很多飞机将能够从简易跑道升空作战，有助于实施全球到达的使命。替代部队设计保留了压制先进防空系统的能力，但是恢复采用越战和“沙漠风暴”行动中行之有效的办法——由老练的机组人员驾驶专用飞机执行专门任务，支援攻击机。目前，空军完全依赖海军提供干扰支援，已有16年之久。替代部队方案将一反现行的做法，将反雷达/干扰机功能整合到F-15G中。替代部队方案将保留已经采购的F-35飞机，同时，美国将信守对伙伴国家做出的承诺，继续向它们提供先进作战功能。

这种替代方案还生成各种附带效益，包括把研发低显性战斗机的昂贵成本负担推给

中国，他们无法有效地使用这些飞机作远程力量投射，只能局限在中国大陆周边。按照本建议方案，尽管过去十年减少的战斗机数目没有补回来，但是机队的平均机龄略有缩短。替代部队将包含F-16F飞机，即增添一种中程F-16变型机，更适合在太平洋战区作战。增加成本低于重型战斗机的几种作战飞机，使我们的空军能与新兴伙伴国家空军开展更有效的交往，扩大我们的影响和开创负担分担的机会。重要的是，到2023年完成大部分采购任务后，我们将可腾出几十亿美元，在2023年之后用于研发和采购远程攻击轰炸机和/或下一代战斗机(F-X)——这是目前的规划兵力展望测算绝对无法实现的奖励效益。

爬出战备问题坑

通过终止F-35计划获得的资金，不能全部用于飞机采购和升级，尤其是在本文所述TACAIR可用飞机总数实际上有所增加的情况下。有些飞机计划，例如F-X和OA-X计划，最终会“赚钱”，因为运行维护成本低，既可满足当前需求，又可用节省的运行维护费用补偿采购费用。把燃油成本上涨计入维持费用，比较困难，也没有尝试这么做，但是替代部队设计架构对这笔费用的容忍程度比规划兵力展望测算为高，因为其燃油消耗较低。

TACAIR的有效性取决于是否特别注意若干其他领域——例如，战备状态。²⁹鉴于我们已使用战备资金支付硬件装备采购账单，我们现在必须使用TACAIR系统专用资金来弥补战备资金的短缺部分。终止F-35计划的一个目的是，避免我们目前的低战备状态延伸为永久性状态。第二个需要特别注意的领域是弹仓深度。尽管我们暂时放弃了让飞机进入最危险的敌方防空圈的(假定胜任)能力，

我们不应该完全放弃对敌方防御目标构成威胁的能力。这就要求我们增加防区外打击武器的投资，包括 AGM-158 联合空对地防区外导弹和反辐射导弹。它还意味着我们需要增加改良型空对空导弹数量，并且研发适合放置在 F-35 武器舱内的高性能和高战斗力武器。最后，恢复长期闲置的反地面发射武器，在太平洋区域至关重要。第三个需要特别注意的领域是系统的运用，尤其是传感器和通讯系统的运用。这原本是研发 F-35 的成果，现在如果我们终止此研发计划，可继续利用其研发成果，即把原本用于 F-35 的先进雷达、电子战装置和数据链路技术用于其他战斗机和常规轰炸机中。

结语

现在该是理性讨论 F-35 计划的时候了。这样的对话必须抛弃关于虚设的对抗空域范围的空谈，认真考虑整个空中作战部队的状

况及其在全球各地的运用。我们早已明白不能指望 F-35 计划会在宽广的作战范畴内提供显著超越原有计划的作战能力。F-35 计划的设计宗旨是应对实际上并未发生的欧洲冲突和低于目前状态的更高端威胁环境，它并不比其前辈飞机有多大改进，却要求从不断紧缩的经费中占用巨额资源。

我们应该以陆军处理“科曼奇人”直升机计划的方式为榜样，考虑取消 F-35 计划，停止执意追求短程隐形飞机专项作战能力，改为创建一支注重强大的广泛作战能力的现代化空中作战部队。面临连续十年的预算削减和二十几年的持续作战，我们必须以稳妥的方式恢复我们的作战能力。这样做将有助于解决各种附带问题，包括部队战备状态、全球到达能力和可用的战斗机/攻击机机组人员数量。F-35 计划的可行替代方案是存在的，关键在于我们是否有勇气正视它们。♣

注释：

1. Dave Majumdar, "Kendall: Early F-35 Production 'Acquisition Malpractice'" [肯德尔：早期 F-35 生产是‘胡管乱理’], DefenseNews, 6 February 2012, <http://www.defensenews.com/article/20120206/DEFREG02/302060003/>.
2. Government Accountability Office, Joint Strike Fighter: DOD Actions Needed to Further Enhance Restructuring and Address Affordability Risks [联合攻击战斗机：国防部需要采取行动以进一步重组该计划和解决成本可负担性风险], GAO-12-437 (Washington, DC: Government Accountability Office, June 2012), <http://www.gao.gov/assets/600/591608.pdf>.
3. General Accounting Office, Defense Aircraft Investments: Major Program Commitments Based on Optimistic Budget Projections [国防部的飞机投资：基于乐观预算预期制定的大型计划承诺], GAO/T-NSIAD-97-103 (Washington, DC: General Accounting Office, 5 March 1997), <http://www.gao.gov/assets/110/106735.pdf>.
4. 高低搭配的指导思想是采购适当数量的 F-15 和 F-16。F-15 是高端飞机，采购数量有限，F-16 则是低端飞机，可大量采购。这样做的目的是在越战后预算受限的情况下维持一支具有广泛作战能力的空军部队。
5. Acting Secretary of the Army Les Brownlee, "Briefing on the Restructure and Revitalization of Army Aviation" [关于重组和增强陆军航空兵的简报], Department of Defense, 23 February 2004, <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2122>.
6. Julien Demotes-Mainard, "RAH-66 Comanche—the Self-Inflicted Termination: Exploring the Dynamics of Change in Weapons Procurement" [RAH-66 科曼奇人直升机项目——自伤式下马：探索武器采购中的变化动向], Defense Acquisition Research Journal 19, no. 2 (April 2012): 183-208, http://www.dau.mil/pubscats/PubsCats/AR%20Journal/arj62/Demotes-Mainard_ARJ62.pdf.

7. David Alexander, "Theft of F-35 Design Data Is Helping U.S. Adversaries—Pentagon" [五角大楼称敌人偷窃 F-35 设计数据获益匪浅]. Reuters, 19 June 2013, <http://www.reuters.com/article/2013/06/19/usa-fighter-hacking-idUSL2N0EV0T320130619>.
8. "Aircrew Summit 2012, 21 June General Officer Steering Group VTC Brief" [2012 年 6 月 21 日空军官员峰会将官指导组视频会议简报], v7 (Washington, DC: Headquarters US Air Force / A30, 21 June 2012).
9. "第五代飞机"的含义不是很确切,一般指主要设计特性包含雷达低显性的现代化战斗机。通常,第五代飞机包括 F-22、F-35、俄国 PAK-FA 样机和中国 J-20。而 F-15、F-16 和 F-18 则是第四代飞机。
10. Brian Everstine and Marcus Weisgerber, "Reduced Flying Hours Forces USAF to Ground 17 Combat Air Squadrons" [缩减飞行时数迫使美国空军停飞 17 个空中作战中队]. DefenseNews, 8 April 2013, <http://www.defensenews.com/article/20130408/DEFREG02/304080011/Reduced-Flying-Hours-Forces-USAF-Ground-17-Combat-Air-Squadrons>.
11. Julian E. Barnes, "Warning Sounded on Cuts to Pilot Training: Air Force Responds to Cost Concerns by Reducing Flight Hours to 120 Hours or Less, Fewer Than Those of Allies—and China" [降低飞行员训练要求拉响警报:空军为应对成本问题而把飞行时数缩减到 120 小时或以下,低于盟国飞行员——以及中国飞行员的飞行时数]. Wall Street Journal, 19 December 2013, <http://online.wsj.com/news/articles/SB10001424052702304773104579268651994849572>.
12. 过去十年的一系列战斗机兵力压缩行动被统称为“精简战斗机”或“空中作战部队精简”。十年中至少有两次大规模的兵力压缩行动,计划把战斗机兵力总数缩减到 2,000 架以下。
13. OA-X 是空中作战司令部提议的一种涡轮螺旋桨轻型攻击机,类似 Embraer A-29 Super Tucano 或 Beechcraft AT-6B。FT-X (有时称为 AT-X) 是空军教育训练司令部提议的 T-X 训练机(取代 T-38)的一种作战机型。
14. Government Accountability Office, F-35 Joint Strike Fighter: Current Outlook Is Improved, but Long-Term Affordability Is a Major Concern [F-35 联合攻击战斗机:目前前景有所改善,但长期可负担性仍是需要关注的主要问题]. (Washington, DC: Government Accountability Office, March 2013), 5, table 1, <http://www.gao.gov/assets/660/652948.pdf>.
15. 凯利(Kari,由法文 Irak 逆序拼写而成)是法国制造的综合防空系统,伊拉克在“沙漠风暴”行动之前购置。该系统在海湾战争之后只是部分重建。F-117A 没有配备雷达、数据链路、加力燃烧室或电子战装置;实际上,它在飞越敌方边界之后甚至没有使用无线电。
16. Gen Mike Hostage, speech at Air Force Association [对空军协会的演讲], 17 September 2013), <http://www.af.mil/Portals/1/documents/af%20events/17SeptAFAGen%20HostageCOMACCSpeech.pdf>.
17. 全球环境假设依据目前的趋势。像任何其他假设一样,无法预测的骤变(例如伊朗爆发新的革命或北朝鲜政权崩溃)将会显著改变这些假设的重要性排序。美国内部的事态发展趋势也许比较容易预测——国会竭力反对缩减 B-1 机群是众所周知的事实,2011 年预算控制法案是不容改变的法律,以及尽管全球石油增产,燃油成本仍然持续上涨二十年(也许可以说四十年)。
18. 本文所述的“高端”、“中端”和“低端”飞机,指其成本和适用的冲突强度。“高端”飞机的成本高,因为它们配备在对抗空域执行任务所需的先进传感器、武器和通讯设备;“低端”飞机的成本较低,它们适用于不需要在敌对空域作战的任务。
19. F-15G 是 F-15E+ 的改装型,它的电子战系统取自 EA-18G “咆哮者”,就像 F-111 取用 EA-6B 系统之后成为 EF-111A “渡鸦”。
20. MQ-9 无人机没有变动,因为它的资金来自情报监视计划,没有直接与 TACAIR 计划争夺资金。
21. 建议方案没有使用包括 MQ-9 的情报监视计划资金,也没有使用包括 B-52 和 B-2 的全球打击计划资金。
22. 利弊权衡分析工具不仅考虑采购成本还考虑维持成本。
23. 出于明显的理由,双座战斗机中队的成本高于单座战斗机中队。但是,在我们没有足够的双座训练驾驶舱飞机可供使用的情况下,双座战斗机中队可以使跟班飞行实习机会的数量增加一倍,但成本不会随之增加一倍。
24. 目前, F-35 的运行维护成本大约是每小时飞行 32,000 美元, F-16 是 19,000 美元, A-10 是 18,000 美元, F-15E 是 28,000 美元(空军 2013 财年总体成本数据库资料)。相比之下,空军国民警卫队实施了两年 AT-6B 试运行计划,每小时飞行成本不到 1,500 美元。
25. 关于轻型攻击机对空军在“伊拉克自由”行动和“持久自由”行动期间的作战行动之潜在影响的详细论述,请参看 Michael Pietrucha and J. David Torres-Laboy, "Making the Case for OA-X" [我们需要 OA-X 飞机的理由], Air Land

Sea Bulletin 2010-1 (January 2010): 15-18; 以及 Michael Pietrucha, “Logistical Fratricide” [后勤互毁], Armed Forces Journal 149, no. 6 (January/February 2012): 14-37.

26. 尽管“游击战”一词产生于西班牙对抗法国皇帝拿破仑的半岛战争，非正规战争的实例在历史上不胜枚举。例如，罗马人参与的非正规冲突数目远远超过诸如三次布匿战争之类的正规大型战役，因而他们拥有因地和因时制宜的军事结构，能够根据敌方的性质进行调整。
27. 若要对一个大型海洋国家产生胁迫效应，不一定需要有第五代飞机组成的突防空军部队。第二次世界大战初期和中期对付日本的方法就是一个有效战略实例，说明可以利用空中力量远距离实施胁迫，不需要大规模突防其防空网。
28. 跟班飞行实习位 (absorbable cockpit) 是为战斗机 / 攻击机组人员提供的实战飞行实习岗位，是测量空军培养和历练机组人员提升其资质和经验的一项能力指标。
29. 本文的重点在于 TACAIR，因而对轰炸机着墨不多；但是读者应注意，战备状态、系统升级和弹仓深度等问题也涉及轰炸机。



迈克尔·皮鲁查，美国空军上校 (Col Michael W. Pietrucha, USAF)，宾夕法尼亚州立大学文学士，美国军事大学文科硕士。现为夏威夷希卡姆基地太平洋空军总部 A8/9 后备役单兵动员增补现役人员。他于 1988 年由空军预备役军官训练团毕业获授军官衔，先后派驻德国斯潘达勒姆空军基地、内华达州内利斯空军基地（两次）、英国雷肯希思皇家空军基地、弗吉尼亚州兰利空军基地以及五角大楼服务。他曾担任 F4G“野鼬鼠”及 F15E 的电子战作战教官，历经十次作战出征，积累了 156 次战斗的经验，此外曾在伊拉克和阿富汗随美国陆军步兵战地工程兵及宪兵部队参与两次地面作战部署。

国防部的人员可靠性计划：皇帝的新衣

The Department of Defense's Personnel Reliability Program: The Emperor Has No Clothes!

约翰·保尔·米克尔，美国空军中校（Lt Col Jon Paul Mickle, USAF）

国防部通过人员可靠性计划甄别和监控具有核武器接触权限的个人。该计划的最基本部分是，对每一个履行与核武器相关职责的人，若其责任能力或可靠性因为任何可能剥夺资格的违规活动或问题——无论发生在值班或非值班时段——而受到质疑，皆须上报。引发质疑的最常见的例子包括犯罪事件、精神或身体健康问题，以及不负责任的财务行为。这些违规活动或问题被察觉后，可能导致相关人士被暂时或永久禁止接触核武器。

人员可靠性计划是对 1962 年以前发生的一系列核事故 / 事件的反应，那些事故和事件导致美国公众开始怀疑武装部队对核装备的管理能力。于是当时的战略空军司令部司令柯蒂斯·李梅空军上将创建了该计划，以期传递一个公关信息，告诉公众只有最优秀的人员才能接触核武器。将军希望让公众了解，只有在相关人员通过人事 / 医疗记录甄别和安全保密级别审查之后，国防部才会允许他们接触核武器；这些人员还必须接受人员可靠性计划的持续监控。但是，由于甄别流程缺乏客观性和零前科要求，有些在入伍前有犯罪和 / 或吸毒前科的人员进入了该计划。之所以会发生这种情况，是因为个别单位指挥官在实施该计划时根据自己的经验和偏见评判受审查人员的历史。尽管指挥官们签发的证书大多符合钟形曲线的意图，但是左右两侧仍存在异常情况——有些合格的人员未能通过该计划的审查，而另一些不符合条件的人员却进入了该计划。这种情况削弱了李梅将军发出的国防部“只”允许最优秀

人员接触其威力最强大武器的公关信息的可信度。其实从一开始，就不是那么回事。

空军全球打击司令部使用一套标准化情况简报幻灯片，作为强制性教育材料，用于接受可靠性计划初步认证的所有人员。但是，这些信息没有列出历史证据或经验教训，未能显示人员可靠性如何可以防止 1962 年以前发生的或该计划开始实施以来发生的某个事故 / 事件。最高层管理人员未能用量化方式显示该计划对核武器安全保障的影响。

效果

国防部在所有下属单位实施、推行和宣传可靠性计划 45 年之后，即 2007 年 8 月，空军丢失了六枚核弹头，违背了所有的核武器操作规程、安全保障措施和管理要求。这次事件导致一个中队、两个大队和一个联队的指挥官，还有四名军士长被解职。另有 25 名官兵受到惩罚。显然，可靠性计划未能预测到这次严重事件的发生或 33 名肩负重要核责任的官兵的渎职。哪怕可靠性计划只要稍微有一点作用，它怎么可能会没有预见到这么多人的失常行为？答案是，可靠性计划根本不能做出这些预测——这是各军种的统计数据已经证明的事实。

军法总长对全球打击司令部及其前身空中作战司令部和空军太空司令部的刑事犯罪与除役统计数据显示，每 1,000 人的刑事犯罪人数和惩罚性退役人数与空军其他各单位的数据差不多。这些司令部历史上任何一年的情况都是如此。如果仅是最优秀的人员接

触核武器，那么拥有核武器的这些司令部应该在基本纪律和遵守军法及民法方面反映出优于其他单位的表现。但是，军法总长的统计数据显示并非如此。大多数空军官兵好比是临床医学试验的“对照组”，其成员的安全保密级别较低（或根本没有），而且不接受严格的监控，但是他们的表现并不比少数官兵组成的“试验组”差，后者的安全保密级别较高，而且接受可靠性计划的监控。

代价

可靠性计划给核武器联队带来沉重的负担。具体而言，每所医院必须平均配备一至三名医生，外加二至四名行政人员，管理一个专职的可靠性计划诊所。此外，通常还需要有三至五名其他医生及三至四名牙医执行与可靠性计划相关的额外任务。而且，每个核武器中队要有二至三名人员专职管理日常的计划通知事项。每个核武器联队有一个可靠性计划办公室，配备二至三名人员，负责监督可靠性计划在整个联队的实施。全球打击司令部有三至四名检查员，他们巡视各个核武器基地，检查可靠性计划在联队的实施情况。根据保守的估计，每个联队每年单是人力费用就要消耗 200 万美元，还不包括从核心任务岗位抽调官兵去“尽量挤出人力”填补大多数中队计划岗位而需要的费用，而且这么做实际上使得相应数目的前线官兵的工作量增加了一倍。

每年，要对可靠性计划的每个成员进行记录审计，导致每年平均有三个月的时间，医院和基地可靠性计划军官需要审阅历史文件，查看是否有证据显示出现了错误。基本上，这些人员在 90 天内的生产率是零，唯一的工作就是确定他们是否漏报了某人可能违规违标的信息，而这些信息对于计划中绝大多数无差错人员的实际可靠性并无任何影响。大

约每隔 12-18 个月，一级司令部或国防部会对 10% 的纪录进行复查，于是再次出现零生产率阶段，再次重复历史结论，对漏报剥夺资格信息的复查同样对计划参与者的服役表现并无影响。这一次，单是人力费用的保守估计就是每个联队一年 250,000 美元。

建议

可靠性计划并非一无是处。它要求有适当管辖权的医务部门和作战单位指挥官共同讨论计划人员的健康状况是否适合服役——对于可靠性计划之外的人员则不要求有这个程序。如果服役官兵有精神健康问题，指挥官可以通过“观察—指导—决定—行动”流程提供帮助，防止部下发生自杀等灾难性事件。指挥官须对其部下的所有行动（值勤和非值勤时的所有行动）负责，因此必须关心部下的生活。可靠性计划指挥官享有了解部下健康状况的特权，其实所有的指挥官都应该享有这种特权，以能更有效地履行职责。

至于可靠性计划的其余部分，即甄别、文件记录、检查和日常管理要求等，国防部应该全部终止，参与计划管理的人员应该返回到各自的核心职责岗位上去。此外，应该考虑让各方面符合条件的人员到核武器单位服役。这些人员再转往别的岗位后，有助于在整个空军逐渐推广遵守技术命令和指示的核武器管理标准。

结语

在目前财力和人力都窘迫的情况下，各军种不应继续沿用 50 年来并不成功和无济于事的人员可靠性计划。在全面赞美战略空军司令部和李梅将军的时代，挑战传统的核武器管理概念也许显得是亵渎神明——但是人员可靠性计划并没有真正地给皇帝披上任何衣服！♣



正义事业锻造的友谊万古长青

——纪念美国军事观察组访问延安七十周年

Evergreen Friendship Forged in a Righteous Cause --- 70 Years in Retrospect of the Yan'an Tour by the US Army Observation Group

鲍世修，中国人民解放军退役大校，高级研究员（SrCol, People's Liberation Army of China, retired, senior researcher）

第二次世界大战后期，1944年7月22日，美国总统罗斯福派遣军事观察组（United States Army Observation Group）来到延安。观察组一行的使命，是了解日军在华北和东北的基本情况、作战特点和我军的政治、军事情况，研究将来在中国作战的各种可能，同时利用我边区有利的地理位置为美海军提供作战用气象等情报。观察组此行还有一个隐含目的，这就是为与中国共产党合作及未来地缘政治战略布局探路。¹ 观察组分两批到达，共18人，先后在延安地区留住两年多，最后一名成员于1947

年3月11日乘美国C-47运输机撤出。在此期间，中国抗日的正义力量在盟国的支持下，彻底战胜了日本法西斯侵略势力，军事观察组在延安地区与中国共产党高层领导人、根据地军队及民众的互动和互相了解，也锤炼了中美两国军人之间、人民之间的深厚情谊，并在中美两国人民交往史上绘就了相互依赖、友好合作的重要篇章。

一、国内外战场的有利形势

美国军事观察组访问延安之所以得以成行，当时国内外的战场形势起了重要作用。



图1：美国军事观察组成员穿着东道主赠送的中山装合影留念

就国际范围来说，1944年的欧洲战场形势一片大好，苏联军队对德军的攻势十分强劲，步步逼近侵略国本土。与此同时，美、英等国联军又在法国诺曼底登陆，开辟出第二战场。德、意法西斯侵略势力的彻底溃败已成定局。

在亚洲太平洋战场，情况稍有不同。日本侵略军尽管面临盟国联军的巨大攻势压力，但仍保存有一定的作战力量。美国对日宣战之后，美国政府视中国为太平洋战场对日作战的主要盟国，加大了对华援助的力度。但是，国民党军队在正面抗日战场上的整体表现，令美国政府很是失望。与此同时，中国共产党领导的军队在中国敌后战场上坚定对日作战，不断重创日军，共产党在整个中华抗战中的地位引起了盟国领导人的格外关注。在这种情况下，为了不失时机地彻底摧毁日军的最后顽抗，减少自身军队的损失，缩短整个战争的进程，罗斯福领导下的美国政府从其当前和未来战略布局出发，开始慎重考虑与纪

律严明坚定抗战的共产党领导下的武装力量合作，共同对抗日本侵略者。而时任中缅印战区外交官的约翰·戴维斯（John Paton Davies, Jr.）及时向罗斯福政府提交了一份秘密备忘录，遂促使美国政府下决心向延安派遣一个军事观察组。戴维斯的这份备忘录就说服美国政府和中国共产党合作列举了6点理由，如下：

这一切，已然清楚。在共产党管辖的中国地区：(1) 这里是在日本最大军事集群地和第二大工业圈以内及附近开展对日军事行动的立足之地；(2) 和其他任何地方相比，这里可以向我们提供有关日敌的最大量情报；(3) 这里有一个最团结、最严明、最勇敢的抗日政权；(4) 这个政权是对蒋介石政府的独一无二的最大挑战；(5) 苏联如果进攻日本将从这里进入；(6) 这里将是新中国和苏联政权接近的奠基之地。²



图2：罗斯福总统于1945年4月12日逝世，美国军事观察组在延安下半旗致哀。

就中国国内的形势来说，国民党为了不让中国共产党在抗击日寇侵略斗争中进一步扩大影响，一直限制舆论媒体对之进行报道，更不用说让外国军事人员访问延安。但1944年的夏天，情况却有些不大一样。中国战场的形势迫使蒋介石不得不对其限制稍微放松。

1944年1月，日军拟定“一号作战纲要”，发起侵华以来较大规模的一次战略进攻。而对日军有计划的掠夺攻势，国民党军队却未做认真抵抗的准备。河南战役打响后，许昌和临汝相继陷落。5月25日，洛阳被占。6月18日，日军攻占长沙。至此，美国对中国国民党政府军队的实际作战能力已丧失信心。7月7日，罗斯福甚至致电蒋介石，提出由美国将军史迪威指挥在华美军及中国军队，包括中共军队。蒋介石当然不会同意，推说此事要有一个准备时期，并提出：与美方“军事之彻底合作，必须以政治合作为基础。”这个政治合作，明眼人都知道，是指蒋介石说了多年却从未拿出诚意的对中共之合作。

然而此时，蒋介石在军事、政治、外交上都陷于被动局面，加上6月18日来华造访的美国副总统华莱士又当面向蒋介石提出要求，蒋介石不得不勉强同意了美国军事观察组访问延安的安排。后来，毛泽东在欢迎使团到来的宴会上风趣地对美国客人说：“你看你们是多么重要！为了让你们到来，连美国副总统也不得不亲自到重庆去见蒋介石做说服工作。”³

二、开展国际统一战线的需要

那么，中国共产党方面对美国军事观察组的来访又是怎么样看待和对待的呢？要回答这一问题，首先要了解一下毛泽东对中国

抗战在第二次世界大战中的地位和作用的看法。

1939年1月，毛泽东在《论持久战》英文本序言中指出：“伟大的中国抗战，不但是中国的事，东方的事，也是世界的事。”⁴在毛泽东看来，中国的抗日战争，不是单单为了保卫一个民族的生存，而且是为了维护东方的安宁和世界的和平而进行的战争。它是全世界人民反法西斯战争一个不可或缺的重要组成部分；那么，要消灭共同的敌人，就必须联合一切为正义而战的国际朋友。其实，毛泽东的这一重要军事策略思想，早在1936年同埃德加·斯诺谈话时，就作过清楚表述。他说：“日本侵略不仅威胁中国，而且也威胁世界和平，尤其是太平洋的和平。日本军国主义不仅是中国的敌人，同时也是要求和平的各国人民的敌人，特别是和太平洋有利害关系的各国、即美、英、法、苏等国的人民的敌人。日本的大陆政策和海洋政策不仅指向中国，而且也指向这些国家。这样，日本的侵略就不仅是中国的问题，而且是太平洋地区所有国家的问题，中国苏维埃和中国人民因此要同各国、各国人民、各党派和各群众组织团结起来，组成反对帝国主义的战线。”⁵

毛泽东相信，外援，包括美国的对华援助，对中国抗战的胜利至关重要，他清楚地指出：中国的抗战离不开外援。在1939年1月，他就明确表示：“在伟大抗战中，基本地依靠自力胜敌，中国的力量也正在发动，不但将成为战胜的力量，且将压倒敌人驱除之，这是没有疑义的。但同时，需要外援的配合，我们的敌人是世界性的敌人，我们的抗战是世界性的抗战，孤立战争的观点历史已指明其不正确了。”⁶

毛泽东的所有这些言论集中说明了一个观点，即中国的抗战同世界范围的反法西斯战争紧密相连，必须联合一切可争取到的进步力量共同对付强敌。正是在这一正确思想的指导下，1944年夏，延安迎来了美国军事观察组。毛泽东对美国政府的这一重大外交举措非常重视，认为争取同美国政府合作，对夺取抗日战争胜利有很大的意义。6月29日，他主持中央六届七中全会主席团会议，专门讨论观察组来延安问题，并作出决定：向美方表明，我们现在需要合作作战；抗战胜利后需要和平建国，民主统一。

为了做好对美国军事观察组的接待工作，周恩来还专门为此草拟了《关于外交工作的指示》，以中共中央的名义于1944年8月18日下发各有关部门贯彻执行。《指示》要求大家把对外国记者和美国人员的接待，作为开展国际统一战线的工作切实做好，作为将要走上领导全国各族人民治理国家岗位的中国共产党的最早外交工作认真做好。

美国军事观察组来到延安后，中共中央的高层领导人毛泽东、朱德、周恩来、彭德怀、叶剑英等人先后多次会见了他们，向他们介绍了我敌后抗日根据地政治、经济、军事各方面的情况。8月23日，毛泽东还亲自同“迪克西使团”（Dixie Mission——美国军事观察组的美方称谓）两位政治官员之一、时任美国驻华大使馆二等秘书的约翰·谢伟思（John S. Service）进行了一次内容丰富的长时间谈话。在这之后，直到1945年8月16日使团被正式撤回先后整整一年的时间，中美双方人员有了更多的广泛接触，彼此增进了了解，建立了难以忘怀的战时情谊。

按照规定，观察组须定时地向美国政府发去他们关于中国敌后边区各方面的所见所

闻。正是由于观察组许多成员的如实报道，中国共产党领导的各抗日根据地的政治、经济、社会情况，中国人民抗日武装力量的军政素质、战斗能力和抗敌业绩等，才得以按其本来面貌，而不是经过国民党某些部门过滤、甚至歪曲后成为戴维斯备忘录中所称的“二手”信息，呈现到美国国家最高决策人的面前。⁷这对加深罗斯福总统对中国共产党在领导中国军民抗击日寇入侵的战场上举足轻重地位的认识，无疑是十分有益的。

三、战时情谊弥足珍惜

美国军事观察组人员在履行“迪克西使团”使命的过程中，深入我各抗日根据地实地考察，同我广大抗日军民大量直接接触，对中国共产党领导人民开展的实实在在的抗日战争和敌后边区建设，渐渐有了清楚的背景认识。对抗日斗争的残酷性和艰苦性，他们也感同身受，甚至为此付出了生命的代价。1945年4月21日，观察组的惠特尔赛中尉（1st Lieutenant Henry S. Whittlesey）在太行山的榆社县堡下村遭日寇杀害，从此便长眠在这远离家乡的土地上。战争时期，共同的奋斗目标和血与火的洗礼，锤炼了两国军人和两国人民之间的真挚感情和纯真友谊。而在那之后，随着时间的推移，大家对战时共同生活的美好回忆以及对那段生活所具认识价值的深入思考，便成了进一步发展和加深两国人民间真诚友谊的真正动力。半个多世纪来，我们的美国朋友在这方面做了大量卓有成效的工作。

观察组成员约翰·高林（Captain John G. Colling）青年时代在中国生活过，接触过中国文化，又精通汉语，并对抗日战争背景有一定了解。在执行“迪克西使团”任务期间，他深入到中国敌后抗日根据地了解中国军民

边浴血抗战边建设家园的真实情景，并从中看到了中国人民争取抗日战争胜利和人民解放事业胜利的伟大力量，从而形成了一个重要信念：同中国共产党人领导的军民合作抗日，是美国在亚太战场赢得胜利的唯一正确选择。

他的回忆录《延安精神——战时中美友好篇章》一书，通过记述他本人和他同事们参加军事观察组的亲身经历，展现了中美交往史上许多十分珍贵的场面，集中体现了中国人民的抗战决心和革命圣地延安的精神风貌。由于这本书以确凿的事实检讨了美国对华政策的失误，所以为书做序的美国知名记者兼作家哈里森·索尔兹伯里（Harrison Evans Salisbury）指出：“约翰·高林拯救了美国对华政策中一卷失去的篇章。这卷篇章本来可以改写当代的历史，使美国在亚洲避免两次失败的战争——朝鲜战争和越南战争。”因而，“这本书值得美国政策制订者和美国公民仔细阅读。”⁸广大读者从索尔兹伯里这些话中不难看出约翰·高林这本著作所包含的重要历史文献价值和促进中美两国人民友好关系持续发展的现实意义。

约翰·谢伟思是“迪克西使团”中又一位毕生致力于美中友好事业的知名人士。他曾向自己政府提出过联合中国共产党共同抗日的政策主张，并预言共产党领导的革命将在中国全国取得胜利。尽管上世纪五十年代美国麦卡锡主义盛行时，他备受歧视，横遭迫害，但他对中国人民的友好情谊却从未减退。雨过天晴后，他先后6次偕夫人一起访华。1984年，为了重温战争年代在延安听过的关于长征的故事，谢伟思还陪同索尔兹伯里千里迢迢重走了一次长征路。

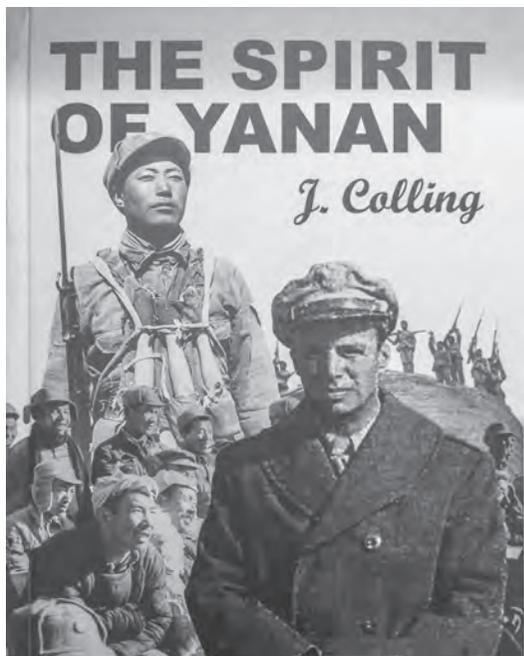


图3：约翰·高林回忆录《延安精神——战时中美友好篇章》

当然，中国抗日战争时期，支持中国共产党领导的中国军民抗敌御侮正义事业的美国好心人，远不止军事观察组范围之内的各位朋友。这里特别需要提到的一位，是埃文斯·福·卡尔逊（Evans Fordyce Carlson）。在抗日战争中，他冒着炮火，深入到我华北敌后根据地，在枪林弹雨中同中国共产党领导的八路军同甘共苦。⁹卡尔逊后来写了《中国的双星》（The Twin Stars of China）等著作，表达了对中国共产党和八路军的敬重之情。美国对日本宣战后，他遵照罗斯福总统的指示，组织了著名的卡尔逊突击队，参照八路军的作战经验，袭击日军占领的多个岛屿，获得了鼓舞人心的胜利，为太平洋上的抗日作战和世界反法西斯战争建立了卓越的功勋。日本投降后，卡尔逊组织了美国争取远东民主政策委员会，在争取美国实行进步的对华外交政策方面做出了贡献。

除了上面提到的高林、谢伟思和卡尔逊三位先生之外，迪克西使团的其他许多人士都怀着对中国人民正义事业的同情。对他们，以及广大美国友人在中国抗战期间和之后提供的真诚帮助和支持，中国民众将永远铭记心间，将把这作为进一步推动中美两国人民友好关系持续健康发展的不竭动力。

研究历史，是为铭记，为鉴今，为知远——何况这段历史并不遥远。从美国政府派出迪

克西使团到现在，中美关系经历了多少风风雨雨，现在随着中国的崛起和强大，正面临着史无前例的最困难的考验。如何消弭误解，看清世界发展的逻辑走向，正需要像高林、谢伟思、卡尔逊等人的大量有识之士，在中美两国政府和人民之间增进了解，发展友谊，锻造互信，避免冲突。只有朝这个方向努力，而不是背道而驰，中美两国并肩作战流血牺牲得来的和平，才能长久延续下去。祝正义事业锻造的友谊万古长青！♣

注释：

1. 参看 John Paton Davies' memo to president Roosevelt [戴维斯提交给罗斯福总统的备忘录], http://en.wikipedia.org/wiki/Dixie_Mission.
2. 原件下载自 <http://en.wikipedia.org/wiki/File:JPDmemo.jpg>, 原文是：“This much, however, seems clear. In Communist China, there is: (1) a base of military operations in and near Japan's largest military concentration and second largest industrial base, (2) perhaps the most abundant supply of intelligence on the Japanese enemy available to us anywhere, (3) the most cohesive, disciplined and aggressively anti-Japanese regime in China, (4) the greatest single challenge in China to the Chiang Kai-shek government, (5) the area which Russia will enter if it attacks Japan, and (6) the foundation for a rapprochement between a new China and the Soviet Union.”
3. 约翰·高林，延安精神——战时中美友好篇章，华艺出版社，1992年版，第21页。英文版见 John Colling, "The Spirit of Yanan---A wartime Chapter of Sino-American Friendship" [延安精神——战时中美友好篇章], (Beijing: Foreign Language Press, 1991), Chap. 1, 16.
4. 《毛泽东军事文集》第2卷，军事科学出版社、中央文献出版社，1993年版，第448页。
5. 《毛泽东一九三六年同斯诺的谈话》，人民出版社，1979年版，第125页。
6. 《毛泽东军事文集》第2卷，军事科学出版社、中央文献出版社，1993年版，第449页。
7. 见注释1。
8. 见注释3。哈里森·索尔兹伯里为高林此书作序的英文原文如下：“John Colling has rescued a lost chapter in American policy in China, one which might have changed contemporary history and spared the country two lost wars in Asia --- the Korean and Vietnam.” (Beijing: Foreign Language Press, 1991), xxiii.
9. 中国八一电影制片厂近年拍摄了“共和国将领”历史系列影片，其中，《孔庆德生死护送卡尔逊》提供了一些相关情节。



鲍世修，中国人民解放军退役大校（1950年11月入伍，1990年9月退役），军事思想专业高级研究员，资深军事翻译家，曾任军事科学院马克思主义军事理论毛泽东军事思想研究所所长。熟悉英、俄、德语，长期从事马克思主义军事理论经典作家和资产阶级军事理论经典作家著作的译校和研究工作，写有这方面的专著和大量学术论文，培养了军事思想专业的研究生，是国家级有突出贡献的专家，在军内外马克思主义军事理论、国际战略和国家安全理论等研究领域和翻译界享有较高知名度。

美国陆军航空队 1946-1947 年在中国

The USAAF in China, 1946-47

戈登·皮克勒中校 (Lt Col Gordon K. Pickler)

尼克松总统的 1972 年中国之旅，以及美国国内媒体大规模的报道，戏剧性地重新点燃了美国人对中国事务的兴趣。记者、学者、退休外交官以及对中国有所接触的其他人士，趁着民众兴趣高涨之际，发表了大量文章和专著。许多撰写者探讨美国政府在 1940 年代对中国事务的深度介入，一时间，各种信息纷呈而来，有各式调研报告，有关于中国人生活的生动描述，有回忆录，还有对于美国在那个时期对中国共产党人政策的重新检讨和逸闻趣事。¹ 这些文字引起了公众的高度关注，也导致了一些争论。例如，权威的《外交》杂志在当时某期中刊登了芭芭拉·塔奇曼 (Barbara W. Tuchman) 撰写的一篇文章优雅的有趣文章。²

塔奇曼太太的文章取用了新近解密资料，意在揣测如果当初毛泽东和周恩来到访华盛顿，世局又将如何发展。这个假设的起因是，

1945 年派驻延安的一名美国军事代表发来一份电报，转述毛泽东和周恩来表示有兴趣拜访罗斯福总统，以便与美国政府发展工作关系。只是，塔奇曼太太没有继续假设接下来可能如何如何，却将笔锋机巧地一转，用大量篇幅责难蒋介石大元帅和 1944-45 年期间在中国的罗斯福总统私人特使帕特里克·赫尔利 (Patrick J. Hurley)。塔奇曼太太的主要佐证资料似乎来自美国政府派驻延安的军事观察组负责人大卫·巴雷特上校 (Colonel David D. Barrett) 和国务院职业外交官约翰·谢伟思 (John S. Service) 提供的信息，而此二人提供的信息都不能被视为公正无偏，因为他们的职业生涯被赫尔利的报复心态所挫伤。塔奇曼太太的主要论点是，赫尔利即使不是阻止毛泽东和周恩来直接与华盛顿对话的唯一主要障碍，起码也是其中之一。因此，美国失去了与中共领导人维持有效接触和建立友善关系的机会。



图 1: 南京国共谈判在 1947 年 3 月破裂之后，中共一行人乘车抵南京大校场机场，准备搭乘美军 C-47 撤回延安。

塔奇曼太太似乎认为，由于未能向中共领导人传达美国的善意，与他们维持有意义接触的所有真诚努力也就此结束。不过，她忽略了杜鲁门总统特使马歇尔将军（General George C. Marshall）的努力。马歇尔将军花了一年多的时间在中国国民党人和共产党人之间进行调停，试图让双方达成持久的停战——甚至是建立联合政府（国共双方已在1946年7月下旬爆发内战）。到1946年底，马歇尔愤而退出调停，但是他的离开并不表示美国完全终止了与中国共产党人的接触或对他们的友好姿态。

除了塔奇曼太太在文章中提到的几件事以及马歇尔的调停努力外，美国人和中国共产党人之间另外还打过几次交道。当时，中共如果想要同美国官员会谈，沟通渠道是敞开的，可以做出相应的安排；实际上，双方确实也接触了几次。共产党人和美国飞行员之间的交往就是一个例子，这也许是双方最后一次的友好接触。

1947年3月，美国陆军航空队派出飞机和机组人员帮助中国共产党的官员、工作人员和他们的家属从南京和国民党占领的其他城市撤离到位于陕西省的共产党根据地首府延安。³ 那次空运发生在国共两党主要在南京举行的谈判无果而终之后。共产党方面没有自己的交通工具，估计必须长途跋涉600英里，穿过国民党统治区，才能到达他们在北方的根据地。由于距离遥远，并且有“土匪”或特务伏击的危险，共产党方面要求我们提供交通工具，把他们从南京市内居住的大院接送到南京机场，然后搭乘美国飞机。陆军航空队提供了所需的交通工具，帮助他们安全通过数百英里国民党统治区，救出了共产党重要人物中的许多人，其中最引人注目的，应是后来担任中华人民共和国总理的周恩来。

执行撤离任务的飞机和机组人员隶属于驻华美军顾问团的航空队。那支部队当时称为航空分队，组建于1946年初，总部位于南京，编制包括大约250名官兵，由约翰·麦



图2：撤离行动完成后，周恩来在延安与美军机组人员同饮咖啡。这可能是中共和美国空军之间最后一次友好交往，此后将近四分之一世纪，双方互不来往。

康内尔准将 (Brigadier General John P. McConnell) 指挥 (他后来成为美国空军参谋长)。撤离任务的代号是“鲶鱼行动”(Operation Catfish), 由航空分队的机组人员和设施在 1947 年 3 月初执行。

“鲶鱼行动”于 3 月 9 日早晨启动。共产党人及其家属携带行李, 乘坐美国卡车到达南京大校场机场。级别较低的工作人员搭乘 C-47 运输机, 周恩来和代表团的一些重要成员乘坐比较舒适的 C-54 飞机到延安。此前, 麦康内尔将军曾经驾驶一架 C-54 飞机把毛泽东送到延安, 他告诉手下的机组人员, 共产党人已经在一条黄河支流旁边的一个山谷里建造了一个机场, 而穷乡僻壤的延安城就在山上, 居高临下地俯瞰着机场。跑道顶端有一堵墙, 飞机如果发生紧急情况, 不可能成功地掉头。⁴ 机场没有导航设备, 因此美国人在上一次飞到延安时使用了一架特别装备的 C-47 飞机, 上面安装了全套无线电设备, 包括归航台、空对地通讯装置和仪表进场系统。此次从南京飞延安, 美国飞行员到达后当天即返回, 没有发生任何意外, 一切圆满完成。共产党人似乎非常感激, 在美国飞机返航南京之前, 特地用咖啡和三明治招待了机组人员。

出乎美国飞行员意外的是, 就在飞机从延安升空不久, 还在盘旋爬高时, 飞行员看



图 3：南京至延安撤离行动完成后, 美军机组一些人员在一架 C-54 飞机旁摄影留念。

到地面人员用炸药炸毁了几段跑道, 使得飞机无法再返回做紧急着陆。事后回想, 这个做法以富有戏剧性的方式表明共产党人要结束所有接触和未来对话。一周之内, 他们的士兵在残留的跑道上横向挖了几条深沟——或许是为了节省炸药——使机场完全无法使用。

美国飞行员在 1947 年的友善姿态也许是中国共产党人和美国空军之间的最后一次友好交往, 此后将近四分之一世纪, 双方互不往来。尽管时过境迁, 中国大陆那位精力充沛的总理在其有生之年也许仍然记得那次友善举动, 甚至可能想到那一天, 是美国空军救了他一命。♣

注释:

1. 其中两本书, John Paton Davies, Jr., *Dragon by the Tail* [抓住龙尾], (New York: W. W. Norton & Co., 1970); 以及 Seymour Topping, *Journey Between Two Chinas* [跨越两个中国之旅], (New York: Harper and Row, 1972).
2. "If Mao Had Come to Washington: An Essay in Alternatives" [如果毛泽东前来华盛顿: 揣议世局之变], *Foreign Affairs*, Vol. 51 (October 1972), pp. 44-64.
3. "History of Air Division, Army Advisory Group, March 1947" [军事顾问团航空分队的历史, 1947 年 3 月], 861.01, Albert F. Simpson Historical Research Center, Maxwell AFB, Alabama.
4. 前任美国空军参谋长麦康内尔将军访谈记录, 华盛顿, 1971 年 2 月 9 日。



本期词汇

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

- **absorbable cockpit** = 跟班飞行实习位（用于提升实战经验和资质的跟班飞行训练机会）
- **Airman and Family Readiness Center** = 空军军人家庭支持中心
- **capability-based deterrence** = 基于（核技术储备）能力的威慑
- **capstone concept** = 顶层概念，总纲概念
- **countervailing reconstitution** = 复原重构，对抵重构
- **cyber arms control** = 网空军备控制
- **digital attacks** = 数字化打击，网空打击
- **groupthink** = 群同思维，群体思维
- **intransit visibility** = 在途可视跟踪，在途物资透明化
- **LEP (warhead life extension programs)** = 弹头延寿计划
- **Missileers** = 导弹兵
- **MWS (major weapons system)** = 主要武器系统
- **nuclear complex** = 核武器集成能力，核武器集成体系
- **OEF and OIF** = “持久自由”行动和“伊拉克自由”行动的英文缩写
- **plutonium pit lifetime** = 钚裂变核寿期（美国估算通常为45-60年）
- **proactive defense** = 先机防御
- **punitive discharge** = 惩罚性退役
- **responsive nuclear infrastructure** = 快速响应核基础设施
- **responsiveness** = 快速响应
- **RRW (reliable replacement warhead) program** = 可靠替代弹头（RRW）计划
- **second-strike retaliating warheads** = 二次报复打击弹头
- **spillover effects** = 溢出效应
- **strategic latency** = 战略储存（将可用于军事战略目的的技术和/或设施储存或封闭，可随时开封投入应用）
- **strike package commander** = 打击组合机群指挥官
- **surface-to-air missile** = 面对空导弹（地对空和舰对空武器的合称）
- **surviving and retaliating warheads** = 生存报复弹头（能安全度过一次打击后用于二次报复性打击的战略弹头）
- **trigger event** = 引信事件
- **U.S.C. (United States Code)** = 美国法典（结构顺序为：卷 [Title]、章 [Chapter]、部 [Part]、节 [Section]、段 [Paragraph]、条 [Clause]）
- **W88 pit production program** = W88（核弹头）裂变核生产计划（Pit表示fissile core or fissile nucleus，多指钚核）
- **weaponless deterrence** = 无武器威慑（依靠可快速研发和生产核武器的隐伏能力而非现成核武库所构成的威慑），也称为“虚拟核武库”，是核裁军运动中的主导理论之一
- **weighted airman promotion system** = 空军加权晋升制
- **Wingman Day** = “僚机”日（美国空军的一种安全教育活动，空军指示各部门每年安排一天时间开展安全及安保教育，要求树立“人人都是僚机”意识，即人人有责保护自身和别人安全）