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。

作战研究

对网空战争概念再思考

Refocusing Cyber Warfare Thought

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

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

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

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

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

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

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

能否把网空视为物理领域

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

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

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

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

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

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

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

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

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

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

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

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

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

网空的独有特征

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

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

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

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

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

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

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

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

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

敌人，亦即，稍作深究，便知只是一句空话而已。

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

结语

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

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

注释:

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

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

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

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

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

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

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

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

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

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

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

15. 同上，第 5 页。

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

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

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

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

20. 太空可能作为例外，此领域有其独有特质，本文限于篇幅不予讨论。

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

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

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

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

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

26. 见注释 23 中《网空威慑和网空战争》，第 59 页。

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

28. 见注释 25 中 AFDD 3-01《制空权作战》，第 1 页。

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

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