

# 多域作战——微妙而重要的军事思想转变

## Multidomain Operations: A Subtle but Significant Transition in Military Thought

杰弗里·M·赖利博士,美国空军大学指挥参谋学院教官(Dr. Jeffrey M. Reilly, Air Command and Staff College, Air University)

2011年11月17日,时任美军参谋长联席会议主席马丁·邓普西陆军上将向军事教育协调委员会提出一个预言性的问题:“联合作战之后是什么?”<sup>1</sup>五年后的今天,问题似乎依然无解。其实不然,也许,答案可能要从多域作战的概念中寻找。<sup>2</sup>邓普西将军如此提问,是面对现实有感而发,是认识到以传统做法夺取空、陆、海领域优势,可能不再是有效的作战样式。导致这种演变的主要因素,是先进信息技术的全球扩散。迄今为止,虽然美国在技术上实现了巨变,但是就理解当今时代如何深刻影响未来的军事作战而言,我们仍处在开蒙阶段。强大的、廉价的、唾手可得的商业技术,正洪水般涌向全球,迫使我们开发更加尖端的手段应对军事需要。催生这场军事变革的主要触机,是晶体管的小型化。1965年,戈登·摩尔发现,集成电路上晶体管的数量大约每两年翻一番。<sup>3</sup>晶体管控制着电路中的电流传输,晶体管的微型化技术,达到了能把200亿个晶体管整合在一个指甲盖大小的超薄计算机芯片上。<sup>4</sup>因此计算机处理能力每两年就翻一倍,并且这种进步预计能持续到2020年。<sup>5</sup>按照摩尔定律下的倍增速度,我们的安全环境在快速演变,网络、定向能、纳米、机器人、生物等领域层出不穷地推出新技术,其深远效应,已经远远超出常规的预测能力。先进信息技术也在改变我们对多种领域相互依存的想法。由于国家和非国家行为者努力获取各种先进能力,以抵消美国在空中、陆地、海上、太空和网空各作战领域的优势,美国向海外投送常规力量的能力在迅速削弱。<sup>6</sup>此

外,现在也越来越要求低层官兵培养跨域作战思维,这对未来产生关键的作战速度至为重要,只有取得这种速度,我们才能抓住一闪即逝的局部机会,一举击毁敌方系统。<sup>7</sup>作战环境的诸般变化,加上“新的”财政现状,在迅速改变我们的思考,对威胁,对作战空间,对空中力量概念的理论基础,我们都需要调整思路。

### 多域作战是战争的永久特点

跨域作战的概念并不新鲜。自古以来,跨域作战就是军事思想固有的组成部分。在伯罗奔尼撒战争期间,雅典人征战西西里岛的灾难性失败,就是一个例证。公元前415年,雅典人发动了一场不明智的远征,要征服西西里岛上最强大的国家锡拉库扎。尼西亚斯率领的雅典军队约有6400人和134艘船。战争初期,雅典人取胜,但是在公元前414年包围锡拉库扎期间,斯巴达将军吉利普斯出兵干涉,扭转了局势,使战局对锡拉库扎军队有利。吉利普斯一开始就把重点放在人类能力这个领域,激励锡拉库扎军队的士气,同时游说盟邦支持。然后,他同时在陆地和海上对雅典军队发动攻击。公元前413年,雅典军队被打败。<sup>8</sup>

这次溃败标志着雅典帝国终结的开始,在雅典引起恐慌,使雅典联盟发生重大转折,为斯巴达在公元前404年的最终胜利扫清了道路。不过,从这次历史实例汲取的教训远不止雅典的崩溃。它凸显出了解多领域的重要性,以及转换领域间局部优势的必要性。

吉利普斯和锡拉库扎军队并非在所有交战中都取胜。事实上，雅典人在几个关键战役中打败或击退了吉利普斯和锡拉库扎的军队。然而，吉利普斯把重点放在了一个关键思考——也是我们现今正嵌入“联合作战介入”概念的关键思维——这就是，在任何一个作战领域，军事优势都不可能大范围覆盖，也不可能永久保持，更常见的，是局部的和暂时的优势。<sup>9</sup> 吉利普斯正确理解了多个领域之间的连接和跨域作战，这是锡拉库扎取得最终胜利的内在因素。吉利普斯的这个战例告诉我们，建立相辅相成的多领域优势，就能提供作战成功的所需的行动自由。

## 未来多项技术威胁构成挑战

在美军着手贯彻邓普西的联合作战总纲概念时，新兴的战略版图上呈现出一系列广泛的新威胁，这些威胁在很大程度上降低了我们过去 20 多年来一直保持的压倒性不对称优势。由于我们的对手无法与美军直接抗衡，便开始利用技术进步，在对抗美军优势中建立他们的不对称优势。<sup>10</sup> 俄罗斯、伊朗、北韩和中国大力发展弹道导弹和超音速巡航导弹，用来挑战美国的常规优势。据信，中国的中程弹道导弹东风-21D，拥有机动重入载具，其特点是根据全球定位系统和有源雷达的末端制导，打击距离中国海岸 1500 至 2000 公里以外的目标。<sup>11</sup>

至少有 9 个国家在进行陆地攻击巡航导弹的研发和生产，其中很多武器今后 10 年将可供出口。<sup>12</sup> 巡航导弹技术的创新构成超音速威胁，能打击 300 公里以外的目标，并能以飞机、潜艇、舰船，甚至卡车等各种系统投送。<sup>13</sup> 此外，现代巡航导弹能被程序设定以最有效的方式接近并攻击目标，让对手从不同方向发射多枚导弹，实施同时打击，命

中对方防空的最薄弱环节而将之瘫痪。<sup>14</sup> 新研制的导弹引入隐形特性，使雷达和红外探测器更不容易察觉，能搭载常规弹头、气体燃料，或甚至低当量核弹头。<sup>15</sup>

除来自先进导弹技术的威胁以外，在 2004 年到 2012 年期间，拥有遥控飞行器国家的数量，从 41 个增加到至少 76 个。<sup>16</sup> 很多国家通过遥控飞行器平台不仅寻求提升其情报获取能力，而且要提升其武装打击能力。

此外，多个国家正在研制高功率微波、定向能和电磁脉冲武器（图 3）。一份 2005 年解密的有关中国电磁脉冲和高功率微波武器生物效应的情报报告表明，中国能在低空引爆一枚低当量战略核弹头，在摧毁电子系统的同时，能最大程度上降低对中国本土产生的影响。<sup>17</sup> 该情报的重要性是，它清楚地显示出使用此武器能同时拒阻多种领域。电磁脉冲能产生超出正常功能的冲击电流和电压，损毁未加固的电路和电子产品。如在美国中部 400 公里高空引爆一个百万吨级的核爆炸，能在几秒钟之内对整个美国大陆产生地面效应，并对太空能力产生重大影响。<sup>18</sup> 例如，美国 1962 年进行的“海星一号”核试验，一枚 140 万吨级武器在地球表面 400 公里的高空引爆。爆炸的电磁效应不仅波及到 898 英里以外的夏威夷，而且还产生了强烈的人工辐射带，开始损坏轨道上运行的气象和通讯卫星。这条人造的辐射带摧毁了 7 颗卫星，并且一直持续到 1970 年代初期。<sup>19</sup> 不要忘记，全球超过 40% 的卫星在低轨道上运行。此外还应知道，敌人能通过多种非核方式投送电磁脉冲效应，产生从系统被暂时干扰，到被彻底摧毁等一系列广泛的后果；投送方式包括弹道导弹、潜艇、飞机、卫星以及人为的系统，诸如爆炸磁通量压缩发生器等等。<sup>20</sup>

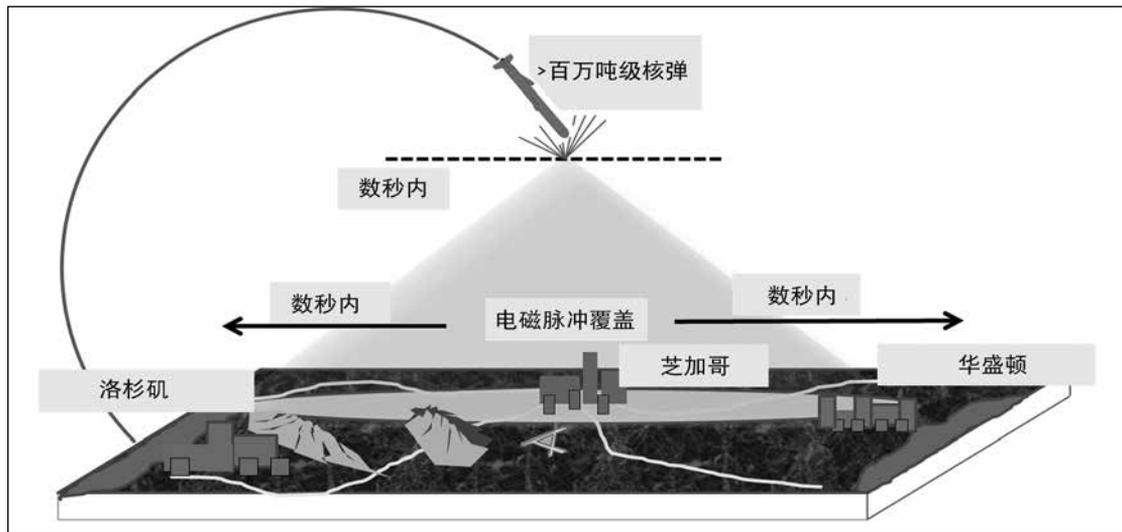


图 1：电磁脉冲效应（Headquarters Department of the US Army, Nuclear Environment Survivability [ 核环境生存几率 ], [US Army White Sands Missile Range, NM: US Army Test and Evaluation Command, 15 April 1994], appendix D.)

技术进步也在改进敌人的自我防卫能力。一体化防空系统利用被动传感器技术，如红外搜索与跟踪，越来越对抗压制性电子干扰。具有先进跟踪和远程能力的地对空导弹，加速了这些技术的突飞猛进。潜在的敌人还在投资于造价低廉的低功耗干扰器，阻挠我方为实施有效打击所必须的定位、导航和报时系统。<sup>21</sup>

## 对手的思维和战略在改变

虽然潜在敌人的军事现代化令人不安，这只是未来威胁态势中的一部分。未来的敌人把技术进步与作战概念和战略相结合，目的是要拒止美军在多种领域中的不对称行动。中国在大张旗鼓地走这条道路，把所谓的“杀手锏”技术与超限战及信息战等战略概念相结合。杀手锏指的是一套军事能力，能让技术劣势一方打败技术优势一方。这些能力包括先进的一体化防空体系、弹道导弹和巡航导弹、先进的攻击机、攻击潜艇，以

及制太空能力。<sup>22</sup> 中国的一些作者力主，为了实现国家的政治目的，在必要时可以超越传统的作战界限。他们提议使用杀手锏打击占优势敌人的关键节点，瘫痪其军队，导致其崩溃。<sup>23</sup> 乔良和王湘穗在他们所著的《超限战》中提出杀手锏的概念基础，以及超限战的概念，其见解格外发人深省，节选如下：

假定在两个已经充分信息化的发达国家之间发生了战争，按照传统战法，进攻的一方，一般都会采取大纵深、宽正面、高强度、立体化的模式对敌展开战役突击。而用组合法，则可能完全是另外一番景象，另外一种结局：如，在敌国完全没有察觉的情况下，进攻一方秘密调集大量资金，对其金融市场发动偷袭，引发金融危机后，预先埋在对方计算机系统里的电脑病毒与黑客分队，再同时对敌进行网络攻击，使其民用电力网、交通调度网、金融交易网、通讯电话网、大众传媒网全面瘫痪，导致其陷入社会恐慌、街头骚乱、政府危机。最后，大

军压境，逐步升级地运用军事手段，直到迫使敌签订城下之盟。<sup>24</sup>

2013 年，美国麦迪安网络安全公司披露了中国人民解放军上海 61398 部队的行踪，凸显出中国在全球进行网络利用和网络攻击的能力和意愿。<sup>25</sup> 中国广为人知的网络能力，远远超越搜集和利用情报数据。网络利用和网络攻击的区别，只不过是一键之差。中国人民解放军在积极建立使用计算机网络作战的战略指导方针、工具，以及训练人员，以支援传统作战科目。<sup>26</sup> 网络空间为中国和其他国家和非国家行为者提供机会，让他们有可能预先在对手国家的后勤、指挥、控制、通讯、计算机、情报、监视和侦察，以及商业支援网络中植入恶意代码，从而阻延对手对动能打击做出反应。<sup>27</sup>

尽管中国在网空领域获得重大的进步，网空并非中国信息战略的重点。中国人民解放军对目前和未来冲突的评估表明，战争将在所有作战领域同时展开，但其对电磁频谱的重视，使解放军能采取远更全面的战争样式。<sup>28</sup> 2002 年，解放军戴清民少将称，电子战的特征是取胜的无形力量，他指出，电子战中的输方，将沦为瞎子和聋子，他们的武器丧失能力，失去在战斗、战役、甚至整个战略局势中的主动。<sup>29</sup> 中国的文章强调，在一个战役初级阶段，夺取制电磁权是确保战场成功最重要的任务之一。中国的战略展现为一体化网络电子战，该战略结合电子战，计算机网络作战，以及动能打击，来破坏支援对手作战和力量投送能力的战场信息系统。这种战争还强调，电磁频谱是生死攸关的第四维空间，与传统的陆军，海军和空军部队一样重要。<sup>30</sup>

中国军队的现代化和战略，预示出未来更广泛趋势的走向，意味着较小的区域强国，甚至非国家行为者，在谋求发展或获取可以改变传统军事作战概念的不对称能力。<sup>31</sup> 对美国而言，这种现象的影响重大且严重，足以促使我们重新思考如何培养未来的空军领导人具备正确制定、协调并实施空中行动的能力。而其中最强有力的触动，是促使这些领导人转变对作战空间概念的看法，以及这种转变对国土防卫、太空和电磁频谱的思考的影响。

## 作战空间概念在变化

技术的发展，不动声色地把全球推入一个新境界，在这个新的境界中，所有作战空间的固有概念因为所有领域变为相互依存而发生根本改变，领域间的互相依存性又来自各种因素，从先进技术的效用到财政分配的约束，不一而足。这些因素的结合而产生了互相影响的环境，于是某个领域的失败，会对另外一个或更多领域产生连环影响。后现代技术在迅速把互相依存的所有领域融合为一个连续的整体，如以下图 2 所简略展示。在这个构造中，电磁频谱为太空充注能量，使太空领域能够对天空、陆地和海洋领域提供关键保障支援，进而加强对人类功能领域的影响或控制能力。假设某个敌手通过网络或其他途径攻击或操纵电磁频谱范围内的无线电频率的使用，他就可能拒止我们接入关键卫星，使我们无法依靠卫星获取情报、通讯、早期预警和导航；这种结果将严重影响联合部队空中统帅指挥官的计划、决策和执行周期，并可能致使天空、陆地和海上作战行动无法达成目标。未来的空军官兵必须充分认识到这种作战环境的一体化，确保在

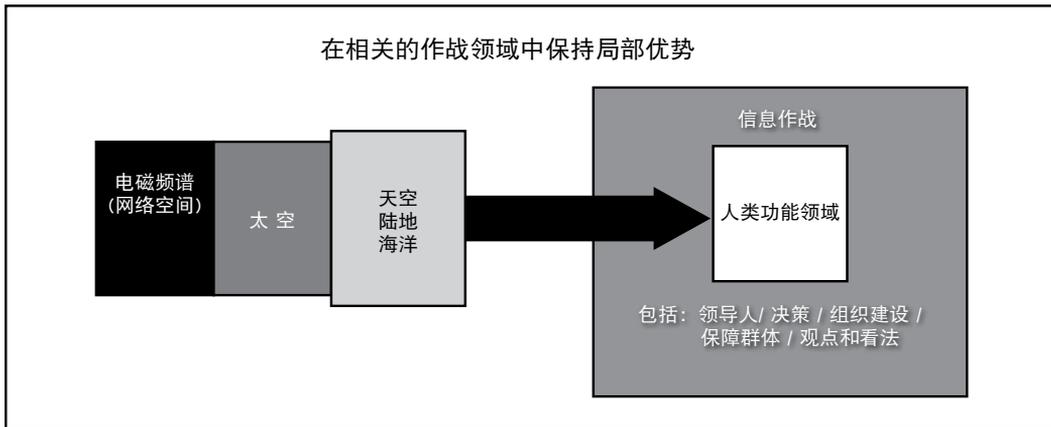


图 2：互相依存的领域融合为一个连续的整体

相关的作战领域中保持足够的和有机结合的局部优势，创造作战制胜所需的条件。

还有必要指出，作战空间的转变，其重要性要远超过在一个特定联合作战区域里所面对的激烈电子对抗带来的挑战。自冷战结束以来，美国首次面临本土受到灾难性攻击的威胁，灾难规模势将超过 2001 年发生的 9/11 恐怖攻击。大西洋和太平洋的传统屏障已不再是拒敌于千里之外的有效方式。经由无线电频率信号，以光速运行的简单程序，能在瞬间把计算机数据包传输到美国本土的系统。此外，这些数据包可能在发动任何攻击前，早早地预置并且潜伏在我们的系统中，而不被及时发现。网络化系统，装置和平台的不断发展，造成太多的弱点而为未来的国家和非国家对手提供可乘之机，其危及美国国家安全的程度远超过军事目标。网络空间将输电网、运输网、通讯和金融系统等方方面面连接起来，这种一体化性质，为敌人提供了诱人的目标，让敌人有机会对美国本土造成大范围实体破坏和经济干扰。

2006 年以来，未经授权进入美国政府电脑的恶意软件事件增长了 650%。<sup>32</sup> 此外，国

土安全部报告，在 2012 年，美国关键基础设施遭到的网络攻击达 198 起，比 2011 年增加 52%。<sup>33</sup> 发表于 5 年前的国家科学院报告，在 2012 年 11 月解密并公布，该报告发现，恐怖主义分子对大型变压器造成的物理损坏，能中断向美国大范围地区的供电，需耗时数月才能维修完毕。<sup>34</sup> 此外，这种攻击能在几乎没有任何被发现或拦截的风险下得以实施。作为参考，北美历史上最大规模的停电发生在 2003 年 8 月 14 日，当时俄亥俄州北部的四条高压电缆下垂触到一些大树，引起短路。电脑系统的差错使这次事故更加复杂化。<sup>35</sup> 这次事故造成美国和加拿大 5 千万人断电，耗费 60 亿美元才得以修复，并可能导致 11 人死亡。此例可见，不难想象，一个决意与美国为敌的敌人能同时攻击关键基础设施的组合，如电网、管道、通讯、运输和金融网络。灾难性的破坏将无法估算。乔尔·布莱纳（Joel Brenner）在其《美国的脆弱性》一书中估计，修复向大城市供电的大功率发电机组需耗时两年。<sup>36</sup>

作战空间中另一个重要变化是太空的变化。从 1991 年以来，美国越来越依赖天基能力支援军事行动。太空资产担当全球范围的

通讯,提供精确打击所需的定位、制导和报时,并且提升情报侦察能力。此外,在太空飞行基本上不受领空限制,可以任意飞越,这对开展导弹发射侦察、导弹跟踪以及早期预警至为关键。对手很清楚,太空对美军而言起着强大的力量倍增器作用,同时也意识到,这种对太空的依赖也是其弱点所在。

卫星系统由三个基本部分组成:卫星本身、指挥和控制卫星的地面站,以及各个部分之间的通信链接。这三个部分都有程度不同的弱点。卫星本身需要沿着可预测的轨道运行,几乎无法隐藏,能为地球大范围的观察者所见,若想变轨,需要经过极大努力。敌人则有各种攻击选择,包括动能打击地面站,干扰或欺骗通信链接,以及使用定向能武器使卫星眩盲或部分失明。未来的打击方式可能更具革命性,例如,有理论称,未来的敌人可能使用“寄生微卫星”,紧紧贴住目标卫星,致其瘫痪,变其轨道,或者劫持其所搜集的信息。<sup>37</sup>

太空军事化和武器化的迅速升级,是当今的主要担忧。2007年1月11日,中国首次成功进行了直升式反卫星武器试验,发射了装备动能拦截器的弹道导弹,摧毁了大约在低轨道530英里高度上运行的“风云1C”气象卫星。<sup>38</sup>随后,中国又在2010年和2013年进行反卫星试验。2013年5月13日,中国发射导弹进入太空,到达的高度超过6000英里,或可超过2万英里。<sup>39</sup>这个高度范围能让中国攻击在中轨道和高轨道运行的美国全球定位系统、军事和情报卫星。但是,反卫星导弹绝非是对美国太空军事应用的唯一威胁。天基能力必须依赖电磁频谱进行有效的作战,因为电磁频谱是收发太空信息和信号的唯一途径。<sup>40</sup>此外,天基系统使用频谱内的频带是固定的,在发射后无法改变。

电磁频谱是基于物理原理的无形机动空间,对控制所有军事行动的作战环境必不可少。<sup>41</sup>该频谱包含电磁辐射赖以传播的各种波长和频率,其使用者有无线电、微波、可见光、紫外线、X光和伽玛射线等,对各个领域产生支配影响。电磁频谱对通讯、指挥控制、蓝军跟踪、精确打击,以及每天使用的和通常视为理所当然的各种其他联合功能,极为重要。此外,国防部投入数十亿美元研发、维护和部署各种依赖电磁频谱的作战能力。<sup>42</sup>仅在2007至2016年,预计研发和采购固定翼机载电子攻击系统本身的投资就超过176亿美元。<sup>43</sup>

像太空一样,电磁频谱也极为复杂。这个作战空间的主要制约之一是,军用和民用频谱的90%都挤占在这个频谱的1%范围内。各系统间的电磁干扰、电磁脉冲、军用和民用之间的竞争,以及自然现象,如闪电、太阳耀斑和降水等,都使电磁频谱的有效性变得更加复杂。还需要指出,我们的敌人也了解电磁频谱,他们会咄咄逼人地与我们争夺对频带的使用。美军对电磁频谱的分配,需要进行协调、优先排序,以及冲突排解。受援的联合部队指挥官有权向用户分配频率,而且当频率被分配到特定地理地区内的系统后,就不再供其他地方使用。这种情况需要指挥官和其参谋班子了解如何在作战层面评估一旦失去对电磁频谱的依赖,将造成什么影响,并思考如何使用其他替代能力。

国际环境进一步模糊了电磁频谱在支援军事行动中的有效使用。电磁频谱超越所有物理领域,没有任何具体或国际承认的疆界,能产生一系列广泛而意想不到的附带效果,从通讯中断的烦恼,到民用铁路运输系统致命的相撞。因此,批准使用电磁系统用于军事行动,要求与跨国联盟和东道国之间密切

合作与协调。这也要求在作战行动策划中发挥创新，才能做好带宽分配，确保数据交换，满足灵活的安全要求和组织程序，一切为着支持作战行动取得成功。

## 作战环境的变化如何影响空中力量的运用

作战环境正在发生巨大的变化，由此将从多方面影响空中力量的运用，包括空中优势、战略攻击、制陆作战、制海作战，以及支援特战部队。但最重要的影响是在两个方面，一个方面是作战的规划-决策-实施周期，另一个方面是在特定领域的优势。未来，这些周期将会压缩，接受后方支援的回取能力将受限，前线指挥官必须依靠任务型命令更多地发挥主观能动性，因为敌我双方将激烈争夺电磁频谱，地面和天基通讯将受损或被阻断。因此，空中力量运用中所奉行的“集中指挥分散执行”根本原则，将被迫转变成适应作战变化的分布式控制方式，需要预先规划好带宽分配，以及设想在各频带门户间机动切换。

作战环境迅速逼近的变化也将影响领域优势的概念。先进技术继续在扩散，实现领

域优势会更加困难。事实上，这种优势极可能是局部的和暂时的。此外，必须指出，作战的成功可能不再依赖追求传统的领域优势，而可能在于对某单一领域的精确把持和出入，由此保障在其他各作战领域的行动。空军必须学会更好地适应在所有这些领域的各种形式的机动，空军官兵只有在理解和把握多域作战机动之后，才能真正激发对空天力量的创新运用。

## 结语

邓普西将军在提出“联合作战之后是什么？”的发问时，他强调的是，到未来的某个时间点，联合作战的重点将不足以应对正在出现的新作战环境挑战。在过去 20 年，空中力量赋予联合部队压倒性的空中优势。但是，技术上的重大进步，以及财政紧缩的现实，推动着作战环境的动态变革，推动我们进入渐进适应的时代。我们必须精心形塑这种演变，确保作战领域间的相互紧密依存，避免疏忽导致蚁穴之溃。迫切性更甚以往，空军必须深刻领会超越天空、太空和网空的多领域同时作战，形成思维共识，飞向未来。★

## 注释：

1. 军事教育协调委员会是向联合参谋部主任就联合作战教育问题提供咨询的机构。该委员会的主委是 J-7 级副职即联合参谋部军事教育副主任，联合及军种大学和学院的校长、指挥官 / 司令官，以及经联合职业军事教育机构认可的其他院校的负责人。
2. 目前作战准则中尚未对“领域”给出定义。本文将该术语定义为关键的作战影响范围，对该范围的控制为行动自由奠定基础。跨域作战涉及利用跨多领域的不对称优势，以实现作战任务所要求的行动自由。
3. Gordon E. Moore, “Cramming More Components onto Integrated Circuits” [ 将更多元件填入集成电路 ], *Electronics* 38, no. 8 (19 April 1965): 114-17.
4. John Markoff, “IBM Discloses Working Version of a Much Higher Capacity Chip” [ IBM 发布实验室阶段的高性能芯片 ], *New York Times*, 9 July 2015, [http://www.nytimes.com/2015/07/09/technology/ibm-announces-computer-chips-more-powerful-than-any-in-existence.html?\\_r=0,9](http://www.nytimes.com/2015/07/09/technology/ibm-announces-computer-chips-more-powerful-than-any-in-existence.html?_r=0,9).
5. 同上。
6. Mark Gunzinger with Chris Dougherty, *Changing the Game: The Promise of Directed-Energy Weapons* [ 改变游戏规则：定向能武器的承诺 ], (Washington, DC: Center for Strategic and Budgetary Assessments, 2012), ix.

7. Department of Defense, Joint Operational Access Concept, version 1.0 [ 联合作战介入概念, 1.0 版 ], (Washington, DC: Department of Defense, 2012), 16.
8. Thucydides, History of the Peloponnesian War [ 伯罗奔尼撒战争史 ], trans. Rex Warner (New York: Penguin Books, 1954).
9. 同注 7, 第 15 页。
10. Office of the US Air Force Chief Scientist, Technology Horizons: A Vision for Air Force Science and Technology, 2010-2030 [ 技术地平线: 空军 2010-2030 年科学技术愿景 ], (Maxwell AFB, AL: Air University Press, Air Force Research Institute, 2011), 19.
11. Amy Chang, Indigenous Weapons Development in China's Military Modernization [ 中国军队现代化中的本土武器发展 ], US-China Economic and Security Review Commission Staff Research Report, (Washington, DC: US-China Economic and Security Review Commission, 5 April 2012), 21.
12. National Air and Space Intelligence Center, Ballistic and Cruise Missile Threat [ 弹道导弹和巡航导弹的威胁 ], NASIC-1031-0985-09 (Wright Patterson AFB, OH: National Air and Space Intelligence Center, April 2009), 3.
13. Victor N. Corpus, "America's Acupuncture Points, Part 2: The Assassin's Mace" [ 美国的死穴, 第二部: 杀手锏 ], Asia Times, 20 October 2006, <http://www.atimes.com/atimes/China/HJ20Ad01.html>.
14. 同注 12, 第 27 页。
15. US General Accounting Office, Nonproliferation: Improvements to Better Control Technology Exports for Cruise Missiles and Unmanned Aerial Vehicles [ 不扩散: 通过改进更好地控制巡航导弹和无人空中飞行器的技术出口 ], GAO-04-175 (Washington, DC: US General Accounting Office, January 2004), 6.
16. US Government Accountability Office, Nonproliferation: Agencies Could Improve Information Sharing and End-Use Monitoring on Unmanned Aerial Vehicle Exports [ 不扩散: 各机构能改善对无人空中飞行器出口的信息分享和最终用户监控 ], GAO-12-536 (Washington, DC: US Government Accountability Office, July 2012), 9.
17. National Ground Intelligence Center, China Research on Bio-Effects of Electromagnetic Pulse and High-Power Microwave Radiation [ 中国对电磁脉冲和高功率微波辐射生物效应的研究, 非保密版 ], (Charlottesville, VA: National Ground Intelligence Center, 17 August 2005). Unclassified.
18. Headquarters Department of the US Army, Nuclear Environment Survivability [ 核环境生存几率 ], (US Army White Sands Missile Range, NM: US Army Test and Evaluation Command, 15 April 1994), appendix D.
19. Chuck Hansen, U.S. Nuclear Weapons: The Secret History [ 美国核武器秘史 ], (Arlington, TX: Aerofax, 1988), 78-79 and 81.
20. Jim Wilson, "E-Bombs and Terrorists" [ 电磁脉冲炸弹与恐怖分子 ], Popular Mechanics 178, no. 9 (September 2001): 51; 另参看 Frederic P. Miller, Agnes F. Vandome, and John McBrewster, Explosively Pumped Flux Compression Generator [ 爆炸磁通量压缩发生器 ], (Mauritius: Alphascript Publishing, 24 November 2009).
21. 同注 7, 第 13 页。
22. Andrew F. Krepinevich, 7 Deadly Scenarios: A Military Futurist Explores War in the 21st Century [ 七个致命场景: 一位军事未来主义者对 21 世纪战争的探讨 ], (New York: Bantam Dell, 2009), 187.
23. John E. Bruzdinski, "Demystifying Sha Shou Jian: China's 'Assassin's Mace' Concept" [ 揭秘杀手锏: 中国的“杀手锏”概念 ], 收录于 Civil-Military Change in China: Elites, Institutes, and Ideas after the 16th Party Congress [ 中国的军民变化: 中共 16 大后的精英、机构和观念 ], ed. Andrew Scobell and Larry Wortzel (Carlisle Barracks, PA: Strategic Studies Institute, US Army War College, December 2005), 345.
24. Qiao Liang and Wang Xiangsui, Unrestricted Warfare [ 超限战 ], (Beijing: PLA Literature and Arts Publishing House, February 1999), 145-46.
25. Mandiant, APT1: Exposing One of China's Cyber Espionage Units [ APT1: 揭露中共网络间谍部队 ], [Milpitas, CA: Mandiant, n.d.], [http://intelreport.mandiant.com/Mandiant\\_APT1\\_Report.pdf](http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf).
26. Deepak Sharma, "China's Cyber Warfare Capability and India's Concerns" [ 中国网络战能力和印度的担忧 ], Journal of Defence Studies 5, no. 2 (April 2011): 66.
27. Office of the Secretary of Defense, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2013 [ 2013 年度中国军事与安全态势发展报告 ], (Washington, DC: Office of the Secretary of Defense, 2013), 36.

28. Deepak Sharma, “Integrated Network Electronic Warfare: China’s New Concept of Information Warfare” [一体化网络电子战：中国信息战的新概念], *Journal of Defence Studies* 4, no 2 (April 2010): 37-38.
29. 同注 23 中 Bruzdinski 文, 第 346 页。
30. 同注 27, 第 37 页。
31. 同注 6, 第 5 页。
32. United States Government Accountability Office, *Information Security: Weaknesses Continue amid New Federal Efforts to Implement Requirements* [信息安全：联邦履行法律的最新努力仍存在弱点], GAO-12-137 (Washington, DC: United States Government Accountability Office, October 2011), 4.
33. Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* [美国的脆弱性：洞察数字间谍、犯罪和战争的新威胁矩阵], (New York: Penguin Press, 2011), 4.
34. House of Representatives, *Electric Grid Vulnerability: Industry Responses Reveal Security Gaps* [输电网的脆弱性：行业反应揭示安全隐患], report written by the staff of Congressman Edward J. Markey (D-MA) and Henry A. Waxman (D-CA) (Washington, DC: House of Representatives, 21 May 2013), 12, [https://portal.mmowgli.nps.edu/c/document\\_library/get\\_file?uuid=b2f47e65-330e-4d89-adee-e2ed58908927&groupId=10156](https://portal.mmowgli.nps.edu/c/document_library/get_file?uuid=b2f47e65-330e-4d89-adee-e2ed58908927&groupId=10156).
35. US-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations* [美加 2003 年 8 月 14 日大停电的最终报告：原因和建议], (Washington, DC, and Ottawa: US-Canada Power System Outage Task Force, April 2004), 17-18; 另参看 JR Minkel, “The 2003 Northeast Blackout—Five Years Later” [2003 年东北大停电 — 5 年之后], *Scientific American*, 13 August 2008, <http://www.scientificamerican.com/article/2003-blackout-five-years-later/>.
36. 同注 33, 第 110 页。
37. David Wright, Laura Grego, and Lisbeth Gronlund, *The Physics of Space Security: A Reference Manual* [太空安全物理学参考手册], (Cambridge, MA: American Academy of Arts and Sciences, 2005), 109.
38. Shirley Kan, *China’s Anti-satellite Weapon Test* [中国的反卫星武器试验], CRS Report for Congress (Washington, DC: Congressional Research Service, 23 April 2007), 1.
39. Craig Murray, *China Missile Launch May Have Tested Part of a New Anti-satellite Capability* [中国可能已通过导弹发射测试部分新的反卫星能力], Staff Research Backgrounder (Washington, DC: US-China Economic and Security Review Commission, 22 May 2013), 2.
40. Joint Publication 3-14, *Space Operations* [联合出版物 JP 3-14：太空作战], 29 May 2013, 1-9, [http://www.dtic.mil/doctrine/new\\_pubs/jp3\\_14.pdf](http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf).
41. Joint Publication 6-01, *Joint Electromagnetic Spectrum Management Operations* [JP 6-01, 联合电磁频谱作战管理], 20 March 2012, 1-1, [http://www.dtic.mil/doctrine/new\\_pubs/jp6\\_01.pdf](http://www.dtic.mil/doctrine/new_pubs/jp6_01.pdf).
42. United States Government Accountability Office, *Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight* [电子战：国防部需加强管理和监管], GAO-12-479 (Washington, DC: United States Government Accountability Office, July 2012), 1.
43. United States Government Accountability Office, *Airborne Electronic Attack: Achieving Mission Objectives Depends on Overcoming Acquisition Challenges* [机载电子攻击：实现任务目标取决于克服采购挑战], GAO-12-175 (Washington, DC: United States Government Accountability Office, March 2012).



杰弗里·M·赖利博士 (Dr. Jeffrey M. Reilly), 休斯敦大学文科硕士, 阿拉巴马大学博士, 担任陆军步兵现役军官 26 年, 历经多个指挥与参谋职位后退役。他的规划与作战经验包括担任战区层级联盟联合作战军官, 规划部主任, 以及“两大战区战争”规划团队成员。他曾担任北约学院综合作战规划课程兼职教员, 美国空军武器教官课程定期讲师, 及参谋长联席会议主席军事教育协调委员会工作组成员。赖利博士也曾向各国防务学院发表多次讲演, 包括汉堡的德国武装部队总参学院, 亚的斯亚贝巴的埃塞俄比亚国防参谋学院, 及华沙的波兰国防大学。此外, 他于 2010 年、2011 年和 2012 年在阿富汗进行了设计研究。他是《作战设计：为决策行动而作的去粗取精》(空军大学出版社, 2012 年)一书的作者。赖利博士现任空军指挥参谋学院联合教育主任, 及该院多域作战战略家学科主任。