



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, 所以我们首先在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

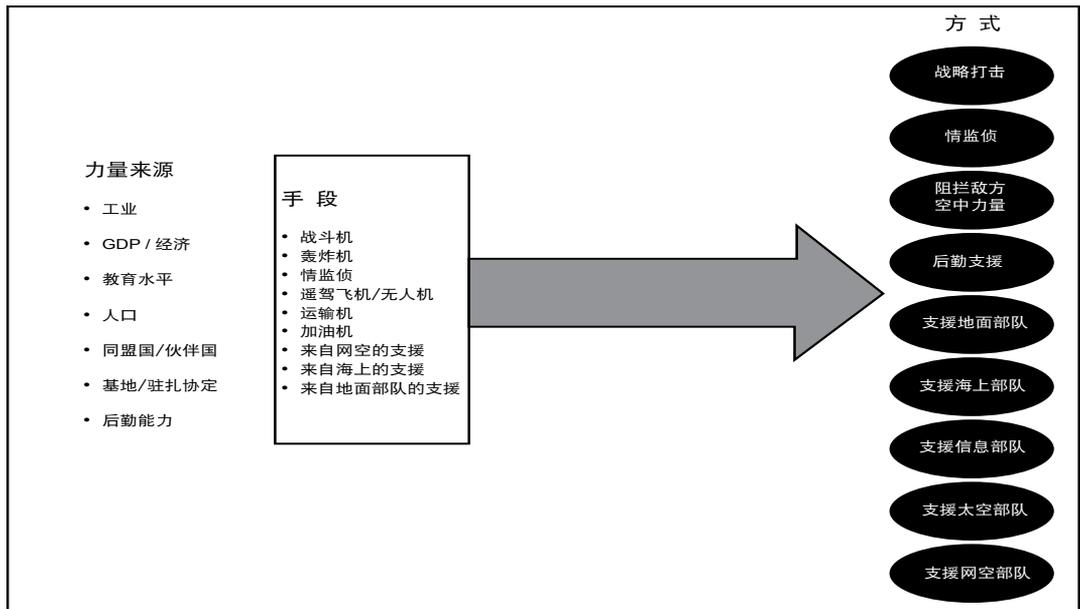


图 1：空中优势的手段和方式

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

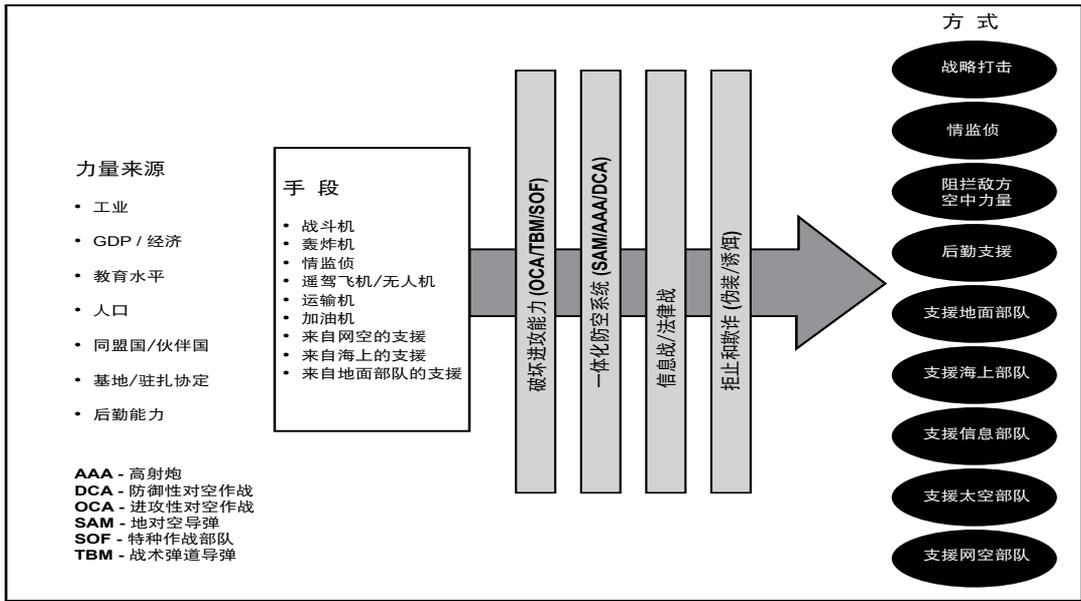


图 2：空中优势的手段和方式及对手的阻拦

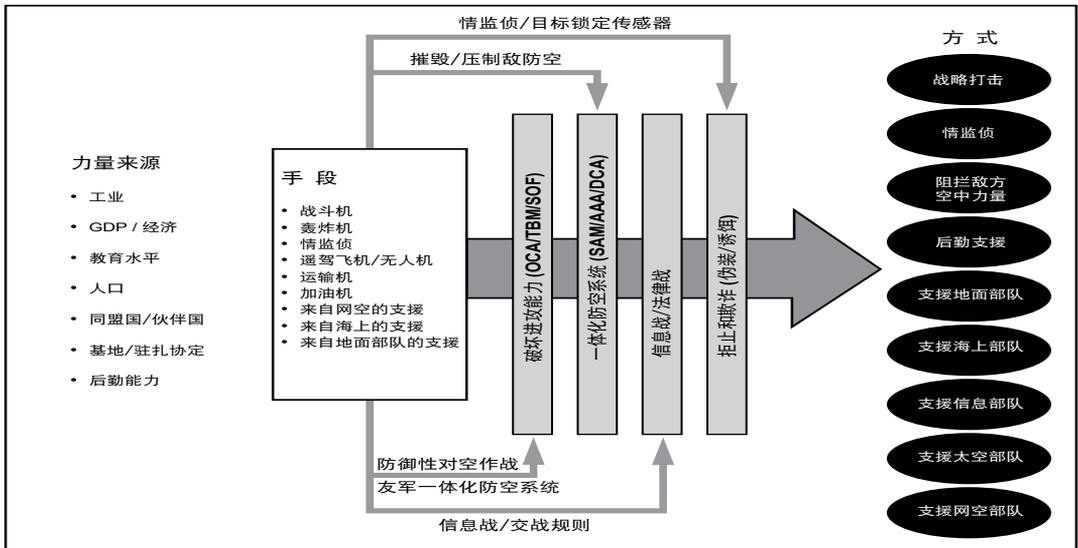


图 3：空中优势模型

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。防御方一旦发现有敌人窃取信息，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

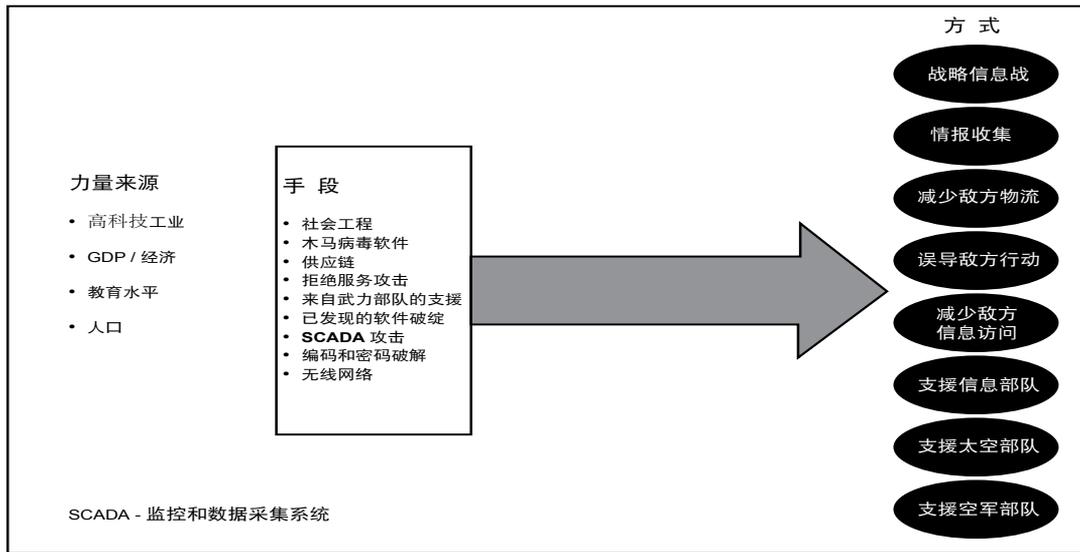


图 4：网空优势的手段和方式

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。这种技术可能包括虚假信息，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

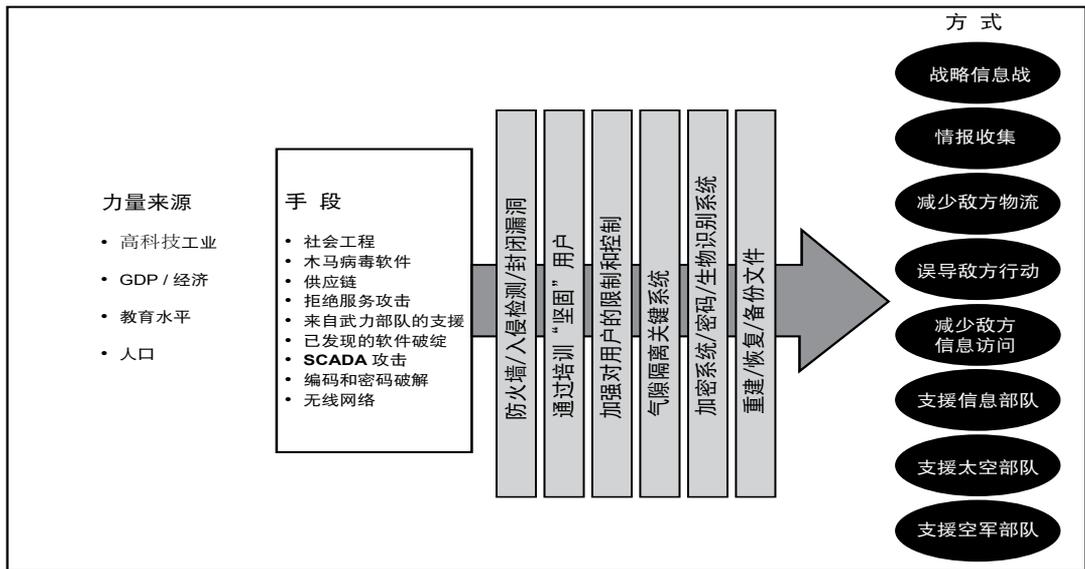


图 5：网空优势的手段和方式及对手的阻拦

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，对手可以同时对各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。

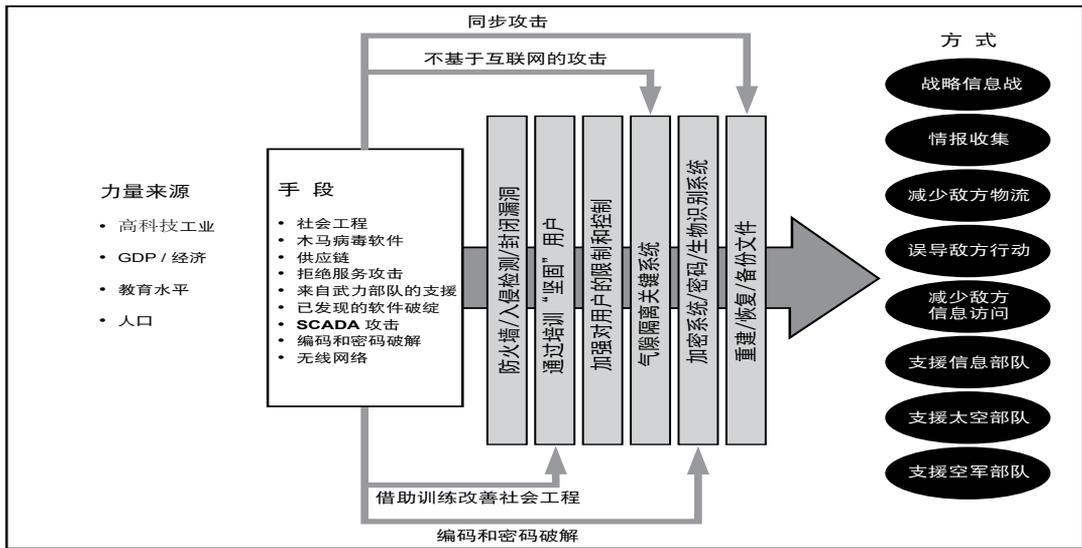


图 6：网空优势模型

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

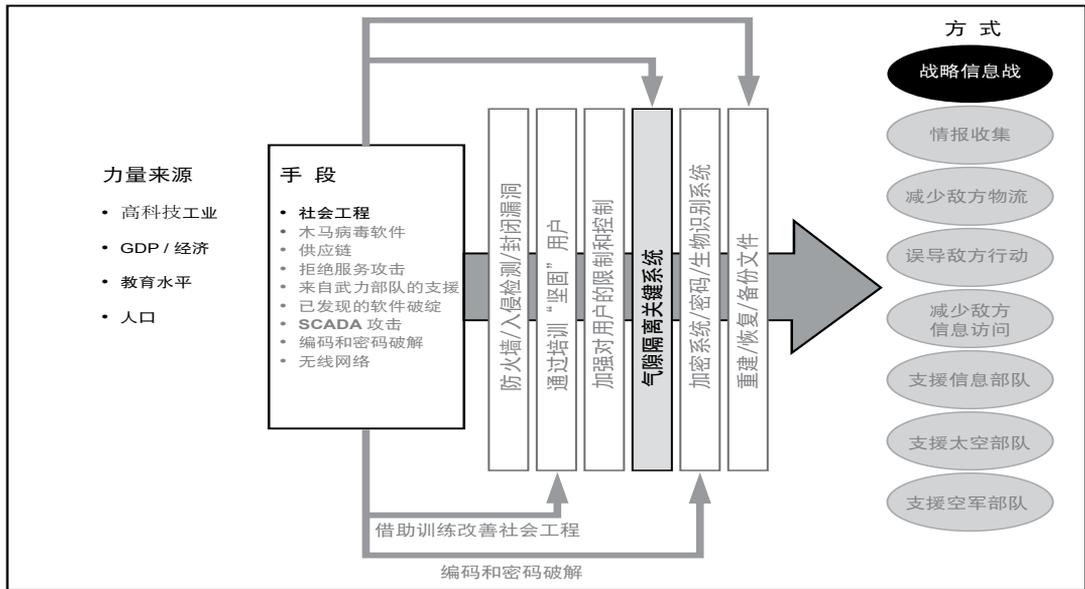


图 8：网空优势模型和 Aramco 网空攻击事件要素

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。