军事科学院优秀博士文库
Selected Doctoral Dissertation of Military Science Academy

A STUDY OF U.S. THOUGHT ON CYBER WARFARE

美国网络空间战思想研究

吕晶华 著

军事科学出版社

军事科学院优秀博士文库

美国网络空间战思想研究

A STUDY OF U. S. THOUGHT ON CYBER WARFARE

吕晶华 著

军事科学出版社

图书在版编目（CIP）数据

美国网络空间战思想研究/吕晶华著. —北京：
军事科学出版社，2014.6
ISBN 978-7-80237-705-9

Ⅰ.①美… Ⅱ.①吕… Ⅲ.①计算机网络-应用-战争-研究-美国 Ⅳ.①E919

中国版本图书馆 CIP 数据核字（2014）第 117562 号

书　　名：美国网络空间战思想研究
作　　者：吕晶华
责任编辑：方　宁
封面设计：倪春昊
出版发行：军事科学出版社（北京市海淀区青龙桥　100091）

标准书号：ISBN 978-7-80237-705-9
经 销 者：全国新华书店
印 刷 者：北京鑫海达印刷有限公司
开　　本：700 毫米×1000 毫米　1/16
印　　张：17.25
字　　数：229 千字
版　　次：2014 年 6 月北京第 1 版
印　　次：2014 年 10 月第 1 次印刷
印　　数：1～2000 册
定　　价：34.50 元

销售热线：（010）62882626　66768547（兼传）
网　　址：http://www.jskxcbs.com
电子邮箱：jskxcbs@163.com

目 录

前 言

英国战略学家约翰·富勒（John Fuller）指出，“每次武器装备发生变化都必然会导致组织和战术的变化，因此必须决定哪一种武器是占据绝对支配地位的（主战武器），围绕这种武器来使用其他的武器”[①]。历史上，无论是双轮马车、火药、飞机，还是雷达、核武器，每次新技术的发展和新装备的出现都会导致战争方式发生巨大变化，网络技术也概莫能外。

20世纪90年代以来，人类社会逐步迈入网络化时代的门槛，信息成为推动社会生产力和军队战斗力发展的主导元素，而承载信息的载体就是纵横交错、连通全球的各种网络。由此，国家利益涉及的范围逐渐超出传统的领土、领海和领空，开始向网络空间延伸，网络空间成为国家安全的“新高地”[②]。它是交流沟通的重要渠道，保证其良性运用是国家政治稳固的基本前提；是社会进步的重要动力，确保其稳定运行是国家经济发展的重要保障；是军力角逐的关键领域，掌握其制权是维护国家安全的关键环节。

---

① ［英］约翰·富勒：《美国内战期间的机动研究》，载《陆军季刊》1935年1月。转引自［美］约翰·阿奎拉、戴维·伦菲尔德等著译：《决战信息时代》，第92～93页，吉林人民出版社2001年版。

② 在诺斯罗普·格鲁曼公司为美国会美中经济与安全审查委员会准备的报告《占领信息高地：中国计算机网络行动与网络间谍能力》报告中，美国将网络空间称为“信息高地”，具体参见：Bryan Krekel, Patton Adams, George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, Prepared for the U. S. – China Economic and Security Review Commission by Northrop Grumman Corp, March 2012.

在当今世界各国军队中，美军无疑是从网络信息技术中受益最多的军队。在作战行动中，美军以远超出其他军队的能力广泛运用网络传输信息，将飞机、舰船等各种作战平台甚至是单个士兵连接在一起，形成稳定和高效运转的庞大战争机器。弹药可以借助定位系统实现精确制导，无人机可以通过远程操控在世界各地执行任务，军舰本身就是一个巨大的数据处理中心，从发现目标、作出决策、打击目标到效果评估，整个战斗过程都高度依赖于网络和网络上所传送的信息。这使美军拥有了明显的军事优势。但网络技术也是一把双刃剑，高度依赖于网络的美国军队，在网络攻击面前显得格外脆弱。一旦网络遭受攻击或破坏，整个军队的作战行动，包括火力配置、目标选择打击、力量调整部署等，都将陷于混乱，军队将遭受不可估量的损失。2009 年，时任美国国防部长的罗伯特·盖茨（Robert Gates）总结道，美军“陆地、海上和空中的全频谱军事能力均依赖于数字通信、卫星和数据网络”①，“网络空间及相关技术为美国提供了前所未有的机遇，对美国安全至关重要，也对军事行动的所有方面至关重要。然而我们对网络空间依赖性的日益增强，加之网络空间威胁和漏洞的增多，也给国家带来了新的风险”②。保护网络空间安全，成为美国军队的一项重要任务。更重要的是，网络空间相关技术作为改变战争形态的新技术③，为各国军事较量提供了新的空间。作为军事变革的领跑者，在传统军事领域拥有强大优势的美国军队，当然要把握先机，在网络空间继续占据

① 盖茨 2009 年 1 月 27 日向参议院武装力量委员会提交报告时的讲话，转引自 Major Gen. William T. Lord, *Cyberspace Operations: Air Force Space Command Takes the Lead*, *in High Frontier*, Vol. 5, No. 3, 2009。

② Kyle Flaherty, *Four Critical Priorities for USCYBERCOM*, July 9, 2009, available at: http://www.breakingpointsystems.com/community/blog/four-critical-priorities-for-uscybercom.

③ James Andrew Lewis, *Cyber Attacks, Real or Imagined, and Cyber War*, July 11, 2011, available at: https://csis.org/publication/cyber-attacks-real-or-imagined-and-cyber-war.

主导地位。

为实现上述目标，美国采取了一系列旨在提升网络空间战能力的措施，从2003年出台《确保网络空间安全国家战略》（National Strategy to Secure Cyberspace）到2011年接连发表《网络空间国际战略》（International Strategy for Cyberspace）和《网络空间行动战略》（Department of Defense Strategy for Operating in Cyberspace），从任命“网络沙皇”（cyber czar）到建立网络空间司令部，从招募网络空间人才到举行应对大规模网络空间攻击演习，涉及战略指导、机构设置、力量建设等方方面面。其中，有关网络空间战思想的激烈争鸣尤其引人关注。

众所周知，军事思想既来源于军事实践，又用于指导军事实践，是引领军队建设的指南，夺取军事斗争胜利的思想武器。网络空间是唯一的一个由人建造的空间，[①] 在这一空间发生的战争有许多不同于以往的新特性。如何正确认识其性质，准确预测其发展趋势，恰当设定其发展框架，直接决定着能否掌握主导权。基于这种认识，在信息化时代军事理论创新大潮中始终担当“领头羊”的美国，在网络空间战思想研究方面同样占据了领导者地位。美国政界要员、军方将领、民间学者、技术专家等纷纷参与其中，就网络空间战相关问题进行了广泛而深入的探讨，内容涉及网络空间与网络空间战的基本含义，网络空间战的主体、目标、类型、特点与行动准则，网络空间战力量的结构、编成与发展方向，当前美国存在的网络空间安全漏洞与可能面临的威胁等诸多方面。

对于当前美国已有的数量众多、范围广泛的网络空间战研究成果，从哪些方面进行分析研究与归纳提炼，才能最大限度地全面反映美国网络空间战思想的全貌和最新发展趋势？新的历史条件下，建设什么样的军队、怎样建设军队，未来打什么样的仗、怎样打仗，是军事理论要回答的根本问题。以此为指导，本书致力于理清

① Martin C. Libicki, *Cyberdeterrence and Cyberwar*, p. 11, RAND Corporation, 2009.

美国网络空间战思想对以下问题的解答：网络空间战是什么？网络空间战怎么打？网络空间战需要什么样的力量和如何建设这种力量？这3个问题，虽然是从不同角度出发剖析网络空间战，但彼此之间存在着清晰的逻辑关系。对于这些问题的解答，也就构成了本书的基本架构。

全文除前言和结语外共分为6章。第一章和第二章解决网络空间战是什么的问题。第一章是对美国网络空间战思想历史发展的回顾，分为4个阶段，分别从技术发展、国际环境、军事形势等角度概要介绍历史背景，指明网络空间战思想的发展演变过程、代表性著作和观点、成就与不足。第二章着重于概念的解析，内容包括网络空间的概念追溯、构成要素和性质特点，网络空间战的基本概念及与其他相关概念的异同，网络空间战的主要特点。第三、第四、第五章解决网络空间战怎么打的问题。第三章采用要素分析法探讨网络空间作战的实施问题，内容包括网络空间作战的行为主体、打击目标，网络空间的进攻、防御和利用3种行动类型，以及网络空间作战在军事行动中的地位作用和应遵循的基本原则。第四章研究网络空间威慑问题。有学者指出，“在战争舞台上，威慑和实战是两个互为补充的重要角色”[①]，“两者互为作用，相得益彰”[②]。因此，研究网络空间战，不能不认真探讨网络空间威慑问题。本章简述了美国网络空间威慑思想的提出和面临的障碍，并对美国学者提出的诸多解决方案进行了总结与归纳。第五章专门研究国际法在网络空间战中的适用问题。法律是美国军事理论中的重要组成部分，在网络空间军事化发展明显加速的背景下，调整并运用国际法规范网络空间军事行为，势必成为网络空间国际竞争的焦点之一，其中的斗争将日益广泛、复杂、激烈。本章分别论述了“诉诸战争权”

① 张云义：《世界战争新形态》，第51～52页，解放军出版社1990年版。

② 邓光荣、王文荣：《毛泽东军事思想辞典》，第358页，国防大学出版社1993年版。

“战时法”在网络空间的适用问题以及网络空间战国际立法问题，内容涉及可行性、面临障碍和美国学者提出的解决方案。第六章回答网络空间战力量如何建设的问题。网络空间战涉及多个领域，只有将各种力量整合起来，才有可能为未来的网络空间战做好准备。本章从国家、军队和国际3个层面，总结了美国学者所指出的当前网络空间战力量整合面临的问题及所提出的解决方案，并阐述了美国网络空间人才培养的现状、问题与构想。结语部分以前文关于美国网络空间战思想的详细描述为基础，希望探讨3个问题：美国发展网络空间战所要达到的目标、对国际网络空间安全形势的影响、中国在网络空间面临的威胁与挑战。此外，为方便读者了解美国相关部门对网络空间战的官方立场，附录部分还收录了美国政府和军队的7份最具权威性的文件，以供参考。

需要说明的是，“网络空间战”所对应的英文是cyber warfare。目前，国内学术界在如何翻译cyber一词方面有着较大的意见分歧，有的主张直接音译为“赛博”，以免与原有各种概念混淆；[①] 有的将其译为“网络电磁空间”，以表明网络与电磁是这一空间中最重要的两个组成部分；也有学者使用“网际”一词，以表明这一领域是物理世界和逻辑世界的融合体……本文采用了更多学者使用的“网络空间”这一术语，因为就目前而言它已经得到了较普遍的应用和认可，与其他译法相比更易理解和接受。为将其与以往所提的“网络战”（network operation）相区别，本文在论及与cyber有关的术语时，统一使用“网络空间”一词。在使用“网络”一词时，除个别情况下是为尊重已有中译本而使用外，多数用以指代network。[②] 另外，从美国学者研究的情况看，他们在论述cyber warfare时，所使

① 使用“赛博”一词的著作和文章较多，例如曾国屏等：《赛博空间的哲学探索》，清华大学出版社2002年版。

② “网络空间”一词的具体含义，将在第二章第一节“网络空间基本概念”中进行专门探讨。

用的 cyber 一词在含义上与 cyberspace 并无区别。[①]

“战争”作为国际法及其战争法中的专门法律用语，在较为严谨的学术研究成果中通常只在特定情况下使用，人们更多地使用的是“武装冲突”一词。以此为出发点，虽然本文的研究对象是“网络空间战”，但由于真正意义上的网络空间战争少之又少，[②] 为保证研究能够从当前网络空间已发生的实际案例出发，并具备实际应用价值，本书所指的并非严格法律意义上的“战争”，而是将武装冲突也包括在内。[③]

① 姚红星等在撰写《美军网络战》一书时指出，网络战应译作 cyberspace warfare，但由于美军正式的组织机构都写作 cyber，因此可将其译为 cyber warfare。详见姚红星、温柏华：《美军网络战研究——从系统工程学角度探讨美军网络战》，第 32～33 页，国防大学出版社 2010 年版。

② 例如，杀毒软件公司 F－Secure 首席研究员米可·海伯伦表示，当前人们在数据安全方面所做的大量工作并非是网络空间战，而是与网络空间犯罪作战，参见 Robert Lemos, *Coming to Terms with Cyber Warfare*, June 17, 2009, available at: http://www.securityfocus.com/brief/972。

③ “网络空间战”一词的具体含义，将在本书第二章第二节“网络空间战基本概念”中进行专门探讨。

第一章　美国网络空间战思想的历史发展

“摩尔定律”（Moore’s Law）指出，集成电路芯片上的晶体管数目每18个月将翻一番。[①] 几十年来的发展表明，这一论断适用于几乎所有与信息技术相关的领域。[②] 信息技术的发展和网络系统的普遍应用，为美国成为世界唯一的超级大国奠定了重要基础，确保了美国不可匹敌的国际地位。但与此同时，美国对网络的依赖程度不断提高，因此受到的威胁也就不断增大。美国发现，要继续推动本国经济持续发展，维护社会繁荣稳定，确保军事力量绝对优势，并保持在国际社会中的霸权地位，就必须因应网络空间的形成与发展，牢牢地掌握对网络空间的控制权。为此，美国在全世界率先提出网络空间战概念，并不断发展完善相关思想，为美国提升网络空间战能力发挥了重要的理论引导作用。

① 1965年，时任Fairchild半导体公司研发部主任的高登·摩尔发现，半导体制造厂在1959～1964年间每隔一个固定的阶段便使集成电路的晶体管密度增加1倍；10年后，他将这一固定阶段确定为18个月。由此带来的结果是，计算机芯片的性能每隔18个月也提高1倍。详细论述见：［美］戴维·阿博特、［英］詹姆士·莫萨特等：《网络中心战与复杂性理论》，第173页，电子工业出版社2004年版。

② 详细论述见Kenneth Geers, *The Cyber Threat to National Critical Infrastructures: Beyond Theory, in Information Security Journal: A Global Perspective*, Volume 18, Issue 1, January 2009。

第一节　早期酝酿阶段（20 世纪 70 年代至 1990 年）

美国是使用信息技术最广泛的国家，也是信息时代的领跑者。1946 年，全世界第一台计算机“埃尼阿克”（ENIAC）在美国宣告诞生。自那时起，以计算机技术为代表的信息技术开始逐渐发展，信息安全随之受到关注。20 世纪 70 年代末期，众多学者就信息社会的特性展开讨论，“信息战争”理论随之诞生，成为网络空间战思想的前身。

一、信息技术初步发展

1957 年 10 月和 1958 年 1 月，苏联和美国分别发射人造地球卫星，人类进入了全球卫星通信的新时代。美国学者奈斯比特指出，这两次卫星发射是“正在成长中的信息社会所缺少的技术催化剂”[①]。1958 年，美国国防部成立高级研究规划署（Advanced Research Projects Agency，ARPA），除负责美国的太空开发项目外，还重点研究军队通讯网络的改进问题，以便在遭到苏联首次核打击的情况下，保障美军通信联络畅通。该机构的建立，大大推动了美国通信技术的发展。1969 年，在麻省理工大学、斯坦福大学及兰德公司等的协助下，国防部高级研究计划局组建名为“阿帕网”（ARPANET）的计算机网络，成为互联网的前身。最初，“阿帕网”只有 4 台主机和 4 个节点，即加州大学洛杉矶分校、斯坦福研究所、加州大学圣巴巴拉分校和犹他大学计算机科学系。研究人员建立“阿帕网”的初衷，是通过电话线使用其他单位的计算机，但是科研人员很快就开始用其进入数据库和传递信息，网络的巨大价值初步展现。

① 王保存：《世界新军事革命》，第 63 页，解放军出版社 1990 年版。

1970 年，该网络向非军用部门开放，多个美国大学和商业部门接入其中，形成包括不同网络的互联网。为实现网络间的互联互通，需要开发一种软件，将持不同“语言”的计算机网络联系起来。1974 年，美国国防部高级研究规划署人员罗伯特·卡恩（Robert Kahn）和斯坦福大学的温登·泽夫（Vinton Cerf）合作，提出“传输控制协议/因特网互联协议”（TCP/IP），定义了在电脑网络之间传送信息的方法，为“阿帕网”的迅速膨胀提供了条件。

1983 年，“阿帕网”分为两个部分：民用的 ARPANET 和军用的 MILNET。同年，美国国防部正式将“传输控制协议/因特网互联协议”确认为“阿帕网”的核心协议，并正式命名为“Internet”。1986 年，在美国国家科学基金会资助下，建成了基于 TCP/IP 技术的主干网 NSFNET，1990 年彻底取代 ARPANET，成为互联网主干网。这是世界上第一个互联网，它连接了美国若干超级计算中心、主要大学和研究机构，并迅速扩展到世界各地，形成全球性的教育科研网络。这一时期，Internet 开始以惊人的速度增长。1983 年，Internet 连接的计算机共有 562 台，到 1989 年突破 10 万台。[①] 1986～1991 年，并入其中的计算机子网由 100 个增加到 3000 多个。[②] 到 90 年代初期，Internet 已成为真正意义上的互联网，供人们通信和交换信息。

在这 40 余年间，计算机和网络主要由政府出资建设，用户主要是军队和部分精英机构中的科研人员，没有受到普遍民众的关注，也未直接影响到人们的日常生活。但是，信息对于经济发展的巨大影响，自 20 世纪 70 年代以来开始显现。据统计，70 年代美国新增加工作岗位 1900 个，其中 5% 在制造业，11% 在商品生产部门，84% 在与信息有关的服务业。到 1980 年，信息产业部门在美国国民

① 参见梅军：《网络战——信息时代的新战争》，载《解放军报》2002－04－10。

② 参见戚建国等：《网络战——信息作战的生命线》，第 20 页，军事谊文出版社 2000 年版。

生产总值中的贡献率已达76%。[①] 1980年，美国学者阿尔文·托夫勒（Alvin Toffler）出版《第三次浪潮》（The Third Wave）一书，认为世界正在开展“第三次浪潮革命”即“信息革命”，人类社会将由此从工业社会进入信息社会。

二、计算机病毒威力初显

与计算机网络技术的快速发展和初步应用相伴随，严重威胁信息安全的各种病毒开始成为全人类共同面对的挑战。最初，美国麻省理工学院的一些年轻科学家，为了娱乐消遣而编写了一种计算机内核代码，用以在调度数据时销毁其他人的游戏程序，成为病毒的前身。1972年，威斯·理萨卡（Veith Risak）发表学术论文，描述以西门子4004/35计算机系统为目标、用汇编语言编写、具有完整功能的计算机病毒。20世纪70年代初期，一种名为“爬行者”（creeper）的病毒开始在“阿帕网”上传播。1981年，高中生理查德·斯克伦塔（Richard Skrenta）编写了病毒Elk Cloner，这是第一个已知被广泛传播的计算机病毒。1984年，美国计算机安全专家弗里德里克·科恩（Frederick B. Cohen）在国际会议上发表题为“计算机病毒——理论与实验”（Computer Viruses – Theory and Experiments）的论文，首次将这种自我复制的程序称为“计算机病毒”（computer viruses）。1986年，一对巴基斯坦兄弟编写了C – Brain病毒，只要有人盗拷他们的软件，这种病毒就会将盗拷者的硬盘剩余空间吃掉。这被认为是真正具备完整特征的电脑病毒始祖。此后，接连出现了一些病毒，如可导致系统速度下降、打印障碍和系统崩溃的Score病毒，感染达一定次数后可破坏计算机系统的BOOT和FAT区的Lehigh病毒，用于攻击IBM国际通信网络BITNET的IBM终端的“圣诞树”（Christmas Tree）病毒等。1987年11月，在以色列的希伯来大学发现PLO病毒，于1988年5月13日以色列占领巴

① 参见王保存：《世界新军事革命》，第64～65页，解放军出版社1990年版。

勒斯坦40周年纪念日当天发作，导致希伯来大学数千台计算机感染病毒，速度减慢。此后，该病毒的许多变种在世界各地传播，每逢13日周五就会发作。

当然，真正引起世界轰动的，还是1988年发生的“莫里斯蠕虫”（Morris）事件。该年11月2日晚，互联网管理人员发现网络中出现不明入侵者。这是一个可快速自我复制和传播的小程序，进入系统中就会不断消耗系统资源。据统计，截至11月12日网络恢复正常，这一程序在10天时间里总计感染了6000多台计算机，导致近4000台计算机因资源耗尽而被迫关机，美国国防部、军事基地、宇航局及多所大学、研究机构的计算机网络均受到影响。调查结果表明，病毒是由康奈尔大学一名计算机专业的研究生罗伯特·莫里斯（Robert Morris）编写和发布的，被称为“莫里斯蠕虫”。美国计算机专家认为，莫里斯制造和释放病毒并非“蓄意攻击”，这种“蠕虫”并未删除计算机内部的数据，未对计算机构成实质性破坏。计算机大面积瘫痪的根本原因，是整个网络缺乏必要的安全防护机制。法庭据此对莫里斯做出了相当宽松的处罚。但这一事件激起了全世界舆论界和科技界的普遍关注，也给美国政府和军方敲响了警钟。人们认识到，虽然人类社会已经开始享受网络带来的便捷的信息交流，但并没有做好应对意外事件的足够准备。

三、信息安全问题开始受到关注

在这一时期，美国政府开始关注到信息安全，并发布了一些政策文件。从这些文件看，美国在信息安全问题上主要关注以下3个方面的内容：

（一）对信息自由流动和隐私的保护

自由主义传统在西方源远流长，在信息时代到来后，这一传统的影响表现为：关注民众自由获取和使用信息的权利，关注民众所应享有的隐私权，并通过法律手段提供保障，防止行政部门过度控制信息流动或获取公众隐私。在这一时期，美国政府发布的相关重

要政策法规主要有：

一是《信息自由法》（Freedom of Information Act）。该法规于1966年通过并由林登·约翰逊（Lindon Johnson）总统签署，规定除9类可免予公开的政府情报外，联邦政府的记录和档案原则上向所有人开放，公民可向任一级政府提出查阅和索取复印件的申请。如申请被拒绝，公民可向司法部门提起诉讼，并得到法院的优先处理。①

二是隐私权系列法案。美国是隐私权的发源地，保护个人隐私的观念在美国根深蒂固。1974年，美国颁布《隐私法案》（Privacy Act），对政府机构应如何搜集个人信息、哪些内容的个人信息能够储存、搜集到的个人信息如何向公众开放及信息主体的权利等都做出了比较详细的规定，以规范联邦政府处理个人信息的行为，平衡隐私权保护与个人信息有效利用之间的紧张关系。但是，互联网的出现对隐私权保护构成巨大冲击。在网络环境下，人们在使用网络的过程中，将大量个人信息提供给网站和网络服务供应商。部分商家将个人数据搜集起来，形成有价值的商业信息，或出售给其他公司。有些黑客甚至是政府，还会出于经济、政治、安全等多方面的考虑，通过网络搜集个人信息。为满足民众保护隐私权的要求，美国政府1986年制定《电子通信隐私法》（Electronic Communications Privacy Act），规定了有线通信、电子和语音通信的截取侦听规则，主要目的是防止政府在未经允许的情况下截取和监听私人的电子通信。

（二）对计算机安全的保护

美国于20世纪80年代初开始着手制定计算机安全规则。1985年，美国国防部国家计算机安全中心（National Computer Security Center，NCSC）出版“可信计算机评估标准”（Trusted Computer

① *Freedom of Information Act*, 1966, available at: http://www.sourcewatch.org/index.php?Title=Freedom_of_Information_Act.