



上海市美国问题研究所
SHANGHAI INSTITUTE OF AMERICAN STUDIES

上海美国评论

Shanghai Review of American Studies

第一辑

中西書局



上海市美国问题研究所
SHANGHAI INSTITUTE OF AMERICAN STUDIES

上海美国评论

Shanghai Review of American Studies

第 一 辑

中西書局

图书在版编目(CIP)数据

上海美国评论·第一辑 / 上海市美国问题研究所编.
—上海: 中西书局, 2015. 1
ISBN 978-7-5475-0753-7

I. ①当… II. ①上… III. ①美国-研究-文集
IV. ①D771.2-53

中国版本图书馆 CIP 数据核字(2014)第 263261 号

上海美国评论(第一辑)

上海市美国问题研究所 编

责任编辑 李 梅

装帧设计 梁业礼

出版 上海世纪出版集团

中西书局(www.zxpress.com.cn)

地址 上海市打浦路 443 号荣科大厦 17F(200023)

发行 上海世纪出版股份有限公司发行中心

经销 各地新华书店

印刷 上海港东印刷厂

开本 700×1000 毫米 1/16

印张 17.5

版次 2015 年 1 月第 1 版 2015 年 1 月第 1 次印刷

书号 ISBN 978-7-5475-0753-7 / D.028

定价 36.00 元

序 言

上海市美国问题研究所作为一个“年轻”的美国问题研究机构,一直致力于美国问题研究并关注学界的最新成果,并与上海国际关系学界保持密切的联系。近年来,该所的研究力量和影响力不断增强,并已出版了多部美国问题与中美关系研究方面的学术专著和论文集。

此间,上海市美国问题研究所一直酝酿编辑出版《上海美国评论》,力争将其打造成该所的品牌刊物。该丛刊的宗旨意在勾勒我国国际关系学界在当代美国问题研究与中美关系研究领域的大致面貌和研究重点,并通过转载稿件或刊登原创稿件,致力于为国际关系学界提供一个新的成果载体和交流平台。在此意义上,《上海美国评论》第一辑的出版是上海市美国问题研究所为美国研究学界做出的一份重要贡献,因此我愿意向读者推介此书。

当前,中美关系已成为国际社会普遍公认的最重要的双边关系。

伴随着中美两国在政治安全领域的互动和经济领域相互依赖不断深化,在中国的国际关系学界,美国问题与中美关系研究渐趋深化,选题日益丰富,而成果亦可谓卷帙浩繁、蔚为大观。这也为《上海美国评论》的编辑工作提供了有益的启发和丰富的选择素材。

此次出版的《上海美国评论》第一辑在栏目的设计方面,考虑到当前国内美国问题与中美关系研究的基本概况并兼顾热点问题,主要设立了“美国国家安全”、“美国外交”、“美国社会与文化”、“美国经济”、“美国网络安全战略”等栏目。今后,该所会根据美国国内政治、经济议题以及中美关系的发展态势,适当调整丛书的栏目设置,进一步突出对热点问题的关注和讨论。

该书的问世也是上海国际关系学界通力合作的结果。在该书的策划、选稿和编辑过程中,来自复旦大学美国研究中心、上海国际问题研究院、同济大学政

治与国际关系学院、上海外国语大学国际关系与公共事务学院、上海社科院等科研单位的国际问题研究专家参与了策划讨论,并提供了宝贵的意见。

当然,由于在版面、选题侧重、栏目设置以及作者联系渠道方面所存在的种种限制,《上海美国评论》无法全面收录国内美国研究领域的优秀论文,因此不免有挂一漏万的遗憾。相信这些不足将在今后的丛书编辑过程中得到改进。

《上海美国评论》第一辑只是上海市美国问题研究所在编辑特色出版物方面迈出的小小一步。相信在学界同仁的大力支持下,《上海美国评论》将不断增加原创论文的比重,以期更好地发挥该丛书的学术平台作用,并为推动我国的美国问题和中美关系研究贡献一份微薄之力。



上海国际问题研究院学术委员会主任

2014 年 11 月

目 录

第一章 美国网络安全战略

美国网络空间战略研究/崔建树	3
美国网络空间先发制人战略的构建及其影响/蔡翠红	22
美国社会化媒体外交评析/杨建平 赵 磊	35
社交媒体在美国对华外交中的运用/汪晓风	46

第二章 美国国家安全

嵌入与冲突——美国军事制度改革的动力与机制/左希迎	67
美国国家安全委员会的模式变迁及相关思考/孙成昊	98

第三章 美国外交

试析当今中俄美三角关系的若干特点/李 兴	115
美国的亚太同盟体系与中国的应对/周方银	127
美国亚太安全战略论析：“聚合安全”视角/王联合	151

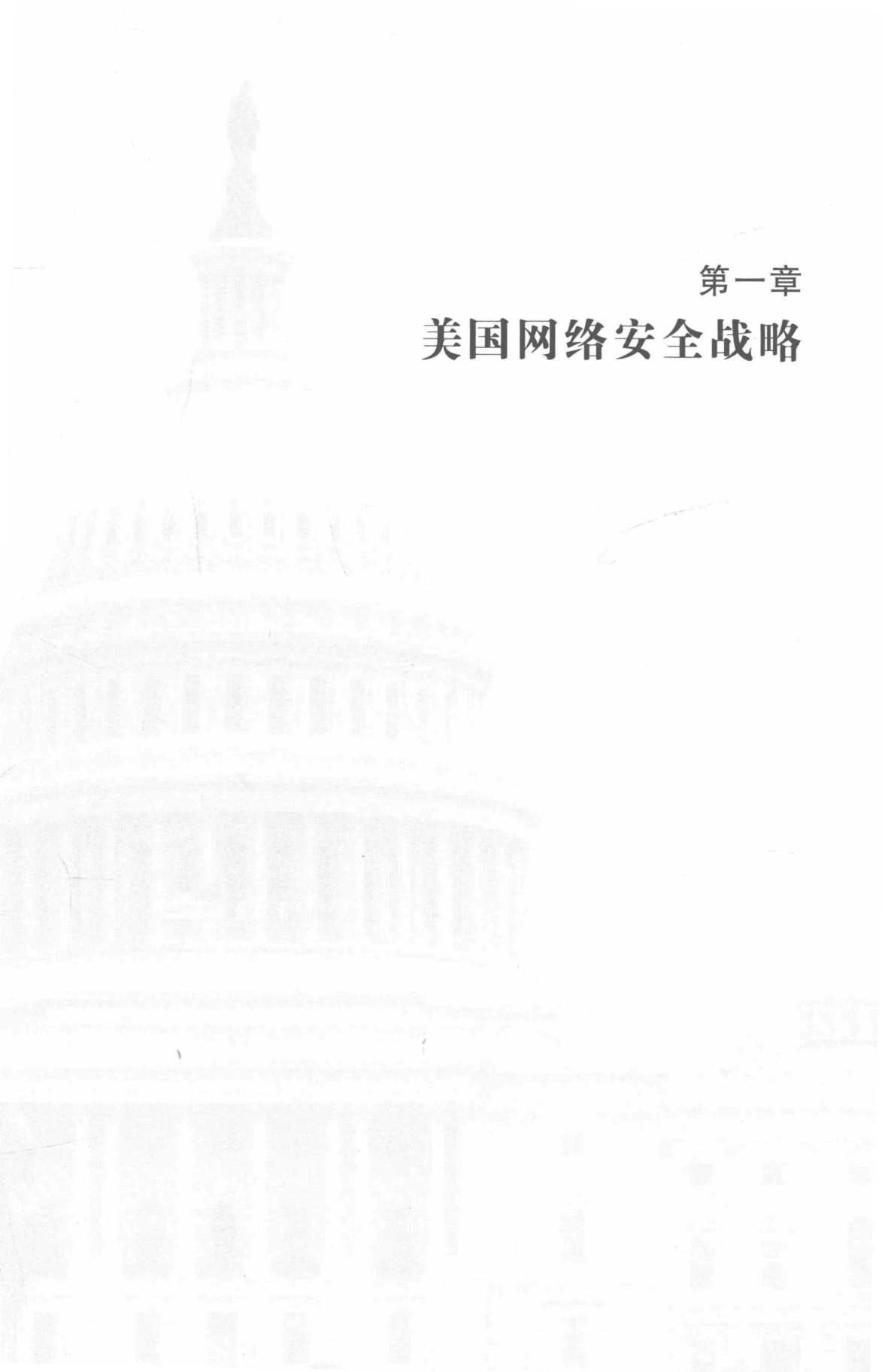
第四章 美国社会与文化

NGO 参与美国“普世价值”推广的路径分析/马方方	177
美国非法移民立法改革与利益集团因素研究/唐慧云	186

第五章 美国经济

再工业化与美国经济增长/宋国友	207
奥巴马政府经济外交评析/张继业	222
中美债务关系的相互依赖及影响/孙海泳	235
中美商务外交的经济性制约研究/张丽娟 [美]吴 鹰	251

后记



第一章

美国网络安全战略

美国网络空间战略研究

◆ 崔建树

[内容提要] 作为“人造空间”的网络空间是继陆、海、空、天之后的人类第五维空间。从美国近几年通过的相关战略报告来看,美国制定了一整套网络空间战略,其中包括争夺制网权战略、通过网络赋能提高武器打击效果的“网络中心战”战略、网络空间安全战略以及利用网络空间对他国进行政治和思想渗透的战略。美国制定的网络空间战略已经取得明显效果,为其谋取了重大的政治、安全、经济和军事利益。但是,网络空间的开放性也同样增加了美国的脆弱性,如美国为维持网络空间霸权开发的数千种计算机病毒,即所谓的“逻辑炸弹”,一旦被恐怖分子所掌握,后果将不堪设想。

[关键词] 美国 网络空间 战略

[作者简介] 崔建树,解放军国际关系学院国际战略研究中心副教授

网络空间(Cyberspace)或更准确地称为网络电磁空间,是加拿大科幻小说家威廉·吉布森(William Gibson)在其1984年出版的小说《神经漫游者》(Neuromancer)中提出的名词,意指计算机信息系统与人的神经系统相连接产生出的一种虚拟空间。^①随着计算机技术、传感器技术的飞速发展及网络和网格技术的突破,网络空间已成为一个新兴的真实存在的客观领域。“该领域以使用电磁能量的电子设备、网格,以及网络化软硬件系统为物理载体,以信息和对信息的控制力为主要内容,通过对数据的存储、修改和交换,实现对物理系统的操控”。^②由此可见,网络空间是一个新兴的“控制域”。^③它对各个行业和领域运转的控制就如人的神经系统对人的行为的控制一样有效。作为世界上

① William Gibson, *Neuromancer*, New York: Ace Books, 1984, p. 69.

② 吴巍. 赛博空间与通信网络安全问题研究[J]. 中国电子科学研究院学报, 2011年第5期, 第474页。

③ 刘兴. 赛博及其相关术语的来源与概念[J]. 指挥信息系统与技术, 2010年第2期。作者认为, “cyber”源自希腊语, 是“掌舵和调节”的意思, 可以理解为统治与管理、控制与调整。所以有学者主张将“Cyberspace”译为控域。

的唯一超级大国,美国要维护自己的霸权地位,自然不会放过这一新兴的“控制域”。^①为此,美国制定了一套完备的网络空间战略。这一战略包括争夺制网权战略、通过网络赋能提高武器打击效果的“网络中心战”战略、网络空间安全战略以及利用网络空间对他国进行政治和思想渗透的战略。

一、美国的制网权战略

现代互联网的前身是美国国防部构建的“阿帕网”(ARPA Net)。1969年,美国国防部为确保美国重要的计算机系统在发生核大战时仍能正常运作,下令其下属的高级研究计划局(Advanced Research Project Agency, ARPA)研究计算机联网问题。到20世纪70年代末期,国防部高级研究计划局又建立了若干个计算机局域网并投入使用。为解决局域网之间的通信问题,高级研究计划局着手研究将不同局域网联结起来形成广域网的新方法,并建成了一个广域的计算机互联网。自互联网问世以来,它在技术方面的突破可谓一日千里,网络连接及全球的每一个角落,“展现出史无前例的力量”。^②特别是随着微机电系统(micro-electro-mechanism system, MEMS)的迅速发展,出现了众多具有通信和计算能力的微型传感器。这些传感器可以通过自组方式时时对探测区进行精确探测,并将探测结果通过有线或无线网络传输给实施者。由于这一技术的应用前景无限广阔,美国自然科学基金会于2003年拨出巨资,研究传感器网络技术,美国国防部也设立了一系列军事传感器网络研究项目。

当前,连接计算机和海量传感器的网络是已经融为一体的世界的神经,而掌握住制网络电磁空间权就等于控制了这个世界的神系统,其意义甚至大大超过19世纪的制海权、20世纪的制空权。所以,世界主要国家无不高度重视对网络电磁空间权的争夺。如德国近几年制定了《德国网络安全战略》,英国也发布了《国家网络安全战略》。这些报告虽然名为加强“网络安全”,实为争夺制网络电磁空间权。为了牢牢把握制网络电磁空间权,美国政府可谓多管齐下。

① 美国高边疆战略的提出者丹尼尔·格雷厄姆提出,在整个人类历史上,凡是能够最有效地从人类活动的一个领域迈向另一个领域的国家,都会取得巨大的战略优势。参见[美]丹尼尔·奥·格雷厄姆:《高边疆——新的国家战略》,张健志、马俊才、傅家祯译,北京:军事科学出版社,1988年版,第5页。

② Jose Vericat, "Is the Google World a Better Place," Journal of International Affairs, Vol. 24, No. 1, 2010.

首先,美国坚决把持全球互联网的域名解析权。互联网的域名是对应互联网数字地址的层次结构式网络字符标志,是网络世界的门牌号,具有唯一性和排他性的特点。由于域名与企业名称、商品标识或商标紧密相联,美国可以从中谋取重大经济与战略利益。如2000年,深圳金智塔软件公司、上海美亚在线、深圳润迅等公司注册的域名遭到美国相关公司的反对,结果在域名争议仲裁中输给了既是“裁判员”又是“运动员”的美国企业,经济损失惨重。为控制域名解析权,美国早在1998年9月就成立“互联网域名与地址管理公司”(ICANN)。ICANN的董事会成员来自美国、巴西、保加利亚、德国、日本等国家,但美国商务部拥有最终否决权。美国为维持其域名控制权,2005年11月,在突尼斯召开有关互联网问题的会议上,时任国务卿的赖斯专门写信给当时的欧盟轮值主席,要求他支持ICANN管理互联网。美国国会还以423票对0票通过决议,要求美国政府控制互联网。2012年12月,在阿联酋迪拜召开的国际电信世界大会上,东道国阿联酋提交了一份要求分离互联网管理权的文件,遭到美国代表克雷默的坚决反对,声称这次会议“要讨论的是电信问题,跟互联网不相关”。^①

其次,把互联网根服务器控制在自己手里。由于域名解析系统的管理模式呈根状分布,因此根服务器在域名管理中起着决定性作用,哪个国家控制根服务器,这个国家就会在互联网领域拥有巨大权力。目前全球共有1个主根服务器和12个副根服务器。放置在美国弗吉尼亚州杜勒斯市的主根服务器由美国的VeriSign公司负责管理。12个副根服务器中,有9个放置在美国,美国军方使用2个,美国国家航空航天局使用1个。另外3个副根服务器放置在英国、瑞典、日本等美国盟友手里。换句话说,美国拥有对根服务器的直接和间接控制权。只要美国愿意,只需将根服务器与二级域名服务器断开,美国便可瘫痪某个与之敌对的国家在互联网系统。2009年,应美国政府要求,微软公司曾切断古巴、叙利亚、伊朗、苏丹和朝鲜五国的MSN服务,导致这五个国家的MSN用户无法登录该即时通信系统。

第三,美国利用其在网络软件、硬件制造能力和技术方面的绝对优势地位谋取政治利益。据相关机构的统计数据,全世界18个互联网软件公司中,有10个是美国公司,其中微软公司(Microsoft)是世界最大的软件公司,该公司生

① 美国继续把持全球互联网管理权[EB/OL]. <http://damin0728.blog.sohu.com/248698464.html>。

产的操作系统广泛应用于个人电脑和服务器的上。思科公司(Cisco Systems)是网络硬件生产领域的龙头老大,该公司生产的路由器、交换机、中继器等在国际市场上占有重要地位。瞻博网络(Juniper Networks)和博科通信系统(Brocade Communications Systems)是世界著名的网络设备制造商,其路由器技术和存储交换机技术领先全球。先进的网络软、硬件制造技术和强大的生产能力是美国争夺网络电磁空间霸权的王牌之一,必要时可以威胁停止或实际终止向对手提供商品,陷对方于困境。此外,美国的主要软件商与美国政府均有密切关系。在政府的授意下,美国软件商往往在它们制造的软件上嵌有后门,以便在必要时服务于美国的政治、经济和国家安全目的。1999年,轰动一时的微软“NSA密钥”事件让美国窃取别国机密的企图大白于天下。

第四,美国掌握着全球IP地址的分配权。在网络世界,IP地址的多寡犹如现实世界中一个国家地理版图的大小。由于美国控制了IP地址的分配,它将绝大多数的IP地址留给本国及其盟国的公司和民众使用,其他国家只能分得一点残羹冷炙。例如中国虽是网络大国,但IPv4/IPv6的地址和域名是从美国租借来的,严重受制于人。

通过掌控网络的域名与地址管理,再加上它超强的网络软、硬件制造能力与先进技术,美国已经牢牢掌握着国际互联网的控制权。尽管如此,美国仍然具有强烈的忧患意识。美国国防部2006年出台的报告中称,“尽管美国目前在网络电磁空间领域享有优势,但这些优势正在受到侵蚀。……与其他作战领域不同,美国在网络电磁空间领域有与对手平分秋色之虞”。^①

为进一步强化美国在网络空间领域的霸主地位,美国政府多管齐下。在军事领域,美国国防部将网络电磁空间视作与陆、海、空、天同类的第五个领域,并认为掌握制网权对维持其在其他四个领域内的霸权具有决定性意义。在2004年发布的《国家军事战略》报告中,美国国防部提出“美国武装部队必须拥有在整个天空、陆地、海洋、太空和网络电磁空间展开行动的能力”。^②2006年,美军发布《国家网络电磁空间军事行动战略》。这项战略的宗旨是确保美军“在这个激烈竞争的领域行动自由,同时剥夺我们竞争对手的行动自由”,即“确保美

① The Department of Defense, The National Military Strategy for Cyberspace Operations (2006), p. 10.

② The Department of Defense, National Military Strategy (2004), p. 18.

国在网络电磁空间的军事优势”。^① 该文件提出要在四个方面加强建设：(1) 在竞争对手决策周期里获取和维持主动行动优势。美军官兵应利用网络电磁空间缩短决策周期,同时削弱竞争对手的决策周期。这需要维持一个强大的网络防御,同时利用竞争对手的网络电磁空间的弱点,搞清竞争对手的决策周期和防御弱点。(2) 利用网络电磁空间使整个军事行动领域进一步整合军事能力。国防部的各个部门必须将网络电磁空间整合得更加精致。作战指挥人员必须与支援部队和国防部的各个机构紧密协同,最大限度地提高战斗力,遂行军事行动。尽管作战部队被部署在各个不同战区,但他们必须与现存的军事行动相配合,与不同政府部门、联合指挥部门、盟军及工业伙伴实现无缝对接。(3) 建设网络行动能力。包括持续不断地培训人员、基础设施和组织机构。通过富有进攻性的测试、演习以及不断改良,创造新的网络行动能力。(4) 管理网络电磁空间行动的风险。^②

实际上,早在这些文件颁布之前,美国就已开始着手培养网络战电磁空间战能力。据报道,1995年6月,美军16名“第一代网络空间战战士”从美国国防大学毕业。同年10月1日,美军在南卡罗来纳州空军基地组建了第一支网络电磁空间战部队,即第9航空队第609中队。1998年10月,美国国防部正式将信息战列入作战条令,同时批准成立“计算机网络防御联合特种部队”。2006年初,美国空军建立研究网络电磁空间问题的“网络特别小组”,由空军参谋长特别助理拉尼·卡斯博士任组长。同年底,美国空军正式宣布成立一个8000人的临时网络电磁空间司令部,罗伯特·J·埃尔德中将担任司令之职。^③ 2007年,美国空军以第8航空队为依托,组建了空军网络电磁空间战司令部,海军也组建了“海军计算机应急响应分队”,西点军校成立了网络电磁空间科学中心。2009年,美国国防部部长盖茨宣布正式成立“网络电磁空间战司令部”,美国国家安全局长基思·亚历山大上将被提名担任司令。据美国国防部副部长阿什顿·卡特在2013年7月18日举行的阿斯彭安全论坛上称,美国网

① The Department of Defense, The National Military Strategy for Cyberspace Operations (2006), p. v.

② The Department of Defense, The National Military Strategy for Cyberspace Operations (2006), pp. 19-20.

③ Thomas Rid and Marc Hecker, War 2.0: Irregular War in the Information Age, Westport: Praeger Security International, 2009, p. 58.

军即将部署到位。^① 这标志着美国已经吹响了争夺网络空间霸权的号角。

主导网络空间需要有比其他国家先进的“网络空间武器”。“网络空间武器”属于新概念武器范畴,当前世界主要国家无不投入巨资研究开发这种武器。据美国技术分析研究所披露的数据,目前世界各国在网络电磁空间武器方面的投入已超过1.7万亿美元。^② 美国是网络空间武器研制的先驱与引领者。如美国空军正在推进“赛博飞机”(Cybercraft)项目,旨在研制出一种能在第一时间侦察到对手在网络电磁空间里的作战意图的武器。^③ 据有关报告披露,网络空间飞机的作战理念非常先进,它可以安装在任何电子介质中,能主动对所有软件和硬件设备进行Ping扫描、端口扫描、操作系统辨识、漏洞扫描和查点,保证作战指挥员能对大到整个网络电磁空间,小到任意一台计算机进行瞬间感知与控制。^④ 2008年5月,美国政府启动了一项更加雄心勃勃的计划——“赛博靶场”(NCR)计划。这一计划号称美国的“电子曼哈顿工程”,企图通过研发“革命性”的新技术,来赢得网络电磁空间这一“太空竞赛”。

二、利用网络空间技术实现基于“网络中心战”的国防转型战略

在因特网构建形成之初,美国相关部门和智库就敏锐地意识到因特网的巨大军事意义,认识到美国未来的军事战略必须适应信息技术的发展。1995年8月1日,美国陆军训练与条令司令部颁发了题为《信息战概念》的《525-69手册》,提出将所有维度(海、陆、空、天)的作战空间和战场系统(指挥控制系统、机动系统、火力支援系统)用数据链连接起来,建立态势感知共享加上具有连续作战能力的“21世纪部队”,使之能够比敌人更迅速、更精准地实施侦察、制定决策、展开行动。^⑤ 1998年10月,美军发布了《信息作战联合条令》,称信息

① 美国网军即将部署到位[N]. 参考消息,2013-07-20,第5版。

② TECHNOLYTICS, Cyber Commander's Handbook. 转引自王源. 赛博武器的现状与发展[J]. 中国电子科学研究院学报,2011年第6期。

③ Shane P. Courville, Air Force and the Cyberspace Mission Defending: the Air Force's Computer Network in the Future, 2007.

④ 刘红军. 赛博空间武器——赛博飞机[J]. 中国电子科学研究院学报,2011年第6期。

⑤ Thomas Rid and Marc Hecker, War 2.0: Irregular War in the Information Age, p. 37.

战就是影响敌方的信息和信息系统,并保护己方的信息和信息系统。……信息优势就是使用信息并阻止敌人使用信息的能力。^①

2001年5月25日,美国前总统小布什在美国海军学院毕业典礼上发表讲话,强调“我们必须利用战争技术的革命性进步来建设我们的军队,使我们能用我们所定义的战争方式来维护和平。我们将致力于建设一支主要以机动性和快速性而非规模和人数来衡量实力的未来军队,建设一支更易于部署和保障的军队,建设一支更依赖于隐身精确制导武器和信息技术的军队”。^② 围绕小布什提出的建设数字化部队的要求,美国国会和国防部提出了以信息技术为依托的国防转型计划。

美国国防转型的目标是利用网络赋能,使目前已达到物理技术极限的武器装备打击效果倍增。美国空军组织的F-15C飞机执行空中对抗任务的演习表明,使用数据链的F-15C飞机的杀伤率提高了1倍以上。原因是“战术数据链的使用使飞行员极大地提高了对作战空间的感知,最终导致了战斗力的增强”。^③ 利用网络赋能的前提是加强国防信息基础设施建设。就如发达的交通离不开四通八达的高速公路一样,要取得信息优势,也离不开无所不至的宽带网络。1993年1月,克林顿政府出台《国家信息基础设施:行动计划》文件,提出在美国建立高速光纤通信网,即“信息高速公路”,把每一个办公室和家庭都用网络连接起来,形成四通八达的信息高速公路。在启动“信息高速公路”后不久,美国军方也开始着手设计国防信息基础设施(DII)建设。1995年,美军提出C4I概念,启动国防信息基础设施公共操作环境(DII-COE)建设,意在为军事行动提供及时、准确的安全信息。1996年,美国军方进一步提出对各类侦察、监视传感器进行整合,打破军种之间“烟囱”林立的状况,建设指挥、控制、通信、计算机、情报、监视和侦察系统(C4ISR),真正实现“从传感器到射手”的作战能力。

美国国防部在推进军用网络带宽建设的同时,还在大力发展信息网格

① Thomas Rid and Marc Hecker, War 2.0: Irregular War in the Information Age, p. 57.

② 美国国防部呈国会报告. 网络中心战[R]. 第11—12页。

③ David S. Alberts, John J. Garstka, Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, CCRP Publication Series, 2000, p. 100.

(Grid)^①技术。1999年,美国国防部提出建设“全球信息网格”(Global Information Grid, GIG)。2003年,该部又公布了《全球信息网格体系结构》(2.0版),规划以国防信息系统网(DISN)为骨干整合美军各军种的军事信息系统,建成符合“全球信息网格”要求的“系统之系统”式公共操作环境(GIG SoS-COE)。目前“全球信息网格”带宽扩展计划(GIG-BE)已完成,近100个骨干节点实现了无缝宽带高速互联。2008年,美军将国防信息基础设施从狭义信息域扩展到广义认知域,实现从信息域到网络电磁域(Cyber)的跨越。

美军将信息技术作为军队转型的支撑,也就意味着将网络作为军队转型的核心,实现从“以平台为中心”向“以网络为中心”转型。网络中心战概念最早由美国人阿瑟·切布罗夫斯基和约翰·加斯特卡提出。^②他们在《网络中心战:起源与未来》一文中认为,在20世纪末人类进入了一个新的战争时代,“社会业已变化,潜在的经济和技术业已改变,美国的商业也发生了变化,如果美国的军事不发生变化,我们就应该诧异和震惊了”。^③

两位作者提出的“网络中心战”概念被美国官方迅速采纳。2002年,美国国防部向国会提交《网络中心战》(Network-Centric Warfare)报告,提出将网络中心战作为国防转型的指南。该报告称,“以网络为中心的部队是一支能够创造并利用信息优势,从而大幅度提高战斗力的部队,它能够提高国防部维护全球和平的能力,并在需要其担负恢复稳定的任务时在所有各种类型的军事行动中占据优势地位”。^④

① 在网络带宽迅速增加的同时,网上的IP地址和资源更呈几何级数增加,再加上传感器网络提供的图像或数据,使网上资源或信息极其丰富。第三代互联网技术开发出来之前,人们使用网上资源要么是通过直接访问网站,要么是通过搜索引擎来查找资源。对于前者来说,就如用户打开电灯开关时需要指定一个发电厂一样;而对于后者来说,输入一下查询关键词可能有数万乃至数十万个结果,查找不便,效率低下。网格(Grid,也译成信息栅格)技术,彻底改变了这种效率低下的状况,真正实现了网络用户之间的互联、互通和互操作。这一技术将散布在网络上的资源虚拟为一个极其强大的信息系统,实现了计算、存储、数据、信息、软件、通信等各种资源的全面共享。参见刘鹏、王立华主编.走向军事网格时代[M].北京:解放军出版社2004年版,第7页。

② Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," Proceedings, January 1998.

③ Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," Proceedings, January 1998.

④ 美国国防部呈国会报告.网络中心战[R].第11页。