奥巴马政府网络空间安全政策述评*

吕晶华

摘　要：奥巴马就任美国总统以来，高度重视网络空间安全问题，发布了一系列强调维护网络空间安全的战略文件，并采用领导指挥体制调整、军事力量建设、促进国际合作等多种手段，全面提升美国在网络空间的实力与地位，企图构建强大的网络空间力量与体系，谋求网络空间新霸权。奥巴马网络空间政策的推行，加剧了国际形势的不稳定性，也使我国的网络空间安全形势空前严峻。

关键词：美国　奥巴马　网络空间　政策

中图分类号：D83　文献标识码：A　文章编号：1005-4812(2012)02-0023-0029

随着当前网络信息技术水平的高速发展和影响领域的快速拓展，美国政府对网络空间的重视程度也不断提高。奥巴马总统 2009 年上任以来，比前任更强调网络空间安全问题的重要性，发布了《网络空间政策评估报告》、《网络空间国际战略》、《网络空间行动战略》等一系列重要战略文件，为美国建构了一个立体的网络安全战略，也使网络安全成为美国国家安全战略的核心部分之一。在此框架下，美国政府相关部门采取了多项举措，重新安排网络空间的权力和规范，谋求更高程度的网络空间霸权，以确保美国政府所确定的繁荣、安全、价值观三大核心利益。奥巴马政府强力推行网络空间国际战略，对国际政治和国际安全局势产生了重大影响。本文拟从分析奥巴马推行网络安全政策的动因入手，讨论美国相关战略和政策的主要内容和特点，并就奥巴马网络空间安全政策对国际形势以及中国安全形势产生的影响提出见解。

一、奥巴马政府推行网络空间安全政策的动因分析

（一）适应国际环境变化，确保美国安全利益

科学技术作为一种至关重要的因素，其进步与发展长久以来始终深刻影响着国际体系的运转和变迁。可以说，国际体系的每一个时代都有一种占据主导地位的技术体系。[1] 冷战结束以来，信息与网络技术取得爆炸性发展，成为 20 世纪对人类影响最大的科技成果，也引领着世界体系由两极格局向新格局过渡。一方面，信息技术推动了全球化进程的加速，各国间交流互动频繁，无论是传统盟国还是以往的敌对国家，相互之间都表现出既竞争又合作、既对抗又联合的复杂关系；另一方面，国际社会的行为体类型日益多样，美国著名学者约瑟夫·奈甚至提出，随着信息革命的发展，占据主导的主权国家开始走向衰落，而互联网上迅速兴起的虚拟社团，则将拥有跨越领土边界的权利，以更为现代化、更为文明的方式监管社会。[2] 在这样一种新的国际环境中，美国虽然以冷战胜利者的姿态出现在世界舞台上，实力远高于其他国家，却不可能单纯依靠传统力量有效控制其他所有行为体，确保本国不受安全威胁。

* 上海国际问题研究院杨剑副院长对本文修改提出了宝贵意见，在此表示谢意。

“ 9 · 11 ” 事件的发生也对美国的安全观造成了深远而持续的影响，使其意识到，美国再也不是孤悬海外的乐土，再也无法享受天然的 “ 安全边疆保障剩余 ” [3]，相反，其本土安全随时可能遭到威胁和侵犯。在 “ 9 · 11 ” 事件发生一个月后颁布的《2001 四年防务评估报告》中，时任国防部长的唐纳德 · 拉姆斯菲尔德无奈地宣称，“ 我们无法也不可能准确地知道，美国利益将在何时、何地受到攻击，或者美国人可能在何时因侵略而丧生。” [4] 安全观的转变，使得美国对所有可能威胁其安全的因素都表现出了极高敏感度。而网络空间不受地理因素的限制，更使美后方直接暴露在外，因此受到了高度关注。加之 2007 年爱沙尼亚遭受网络攻击、2008 年 8 月俄格冲突期间发生网络对抗等事件的影响，美国这一严重依赖于网络的国家产生了深刻的危机感，网络空间安全由此被提升至前所未有的高度。

（二）维持信息技术优势，促进美国持续繁荣

美国被誉为信息时代的领跑者，是最早发明和应用信息技术的国家。1993 年，时任美国总统的克林顿正式宣布实施 “ 信息高速公路 ” 计划，其目的是将美国乃至世界的各个领域以网络系统连接起来，组成遍布全球的“ 信息高速公路 ”，利用信息产业推动美国经济持续走强。事实证明，信息技术在美国经济全面复苏中发挥了无可替代的重要作用：美国的传统产业得到适当改造，生产能力获得新的提高，竞争力于 1994 年再次位居世界首位。信息技术产业也成为美国最大的产业，1995-1998 年期间对美国经济增长的实际贡献率达 35%以上。[5] 美国新安全研究中心最新发布的《美国网络未来：信息时代的安全与繁荣》报告评估认为，如果没有信息技术革命，美国每年的国内生产总值（GDP）将比现在的实有数目少 2 万亿美元，互联网为美国 GDP 做出的贡献多达人均每年 6500 美元。[6]

作为全球信息技术革命的核心国家，美国当然不希望其他国家，特别是新兴技术发展国家，在当前技术创新速度有所减缓的情况下，过多地分享由此带来的巨大利益。美国自认为有必要运用各种市场的、政治的和技术的权力，竭力维持一个有助于美国保持其技术优势和经济优势的国际环境。为此，美国需要继续实施网络经济安全战略，继续强化与信息技术相关的知识产权制度。正如美国学者所说，“ 人们认识到信息产业正在变得越来越重要，但却没有看到信息已经作为一种商品出现了……（信息）从一种我们借以获得和管理其他资产的工具，变成了一种重要的资产。” [7] 在此过程中，制定新的游戏规则，保住美国在网络空间中分配财富的权力，对美国政府来说成为了十分紧迫的任务。因此，继续保持世界财富向美国积聚，同时减少美国财富的流出，“ 在一个促进机遇与繁荣的开放国际经济体系中建立强大的、不断增长的创新型美国经济 ” [8]，就成为美国政府推行网络空间安全政策的另一个重要动因。

（三）运用新型网络力量，扩展美国价值观念

价值观在美国对外政策中一直占据着特殊的重要地位。约瑟夫 · 奈指出，“ 自从建国初期开始，美国人就一直为将我们的价值观与我们的其它利益相结合而胶尽脑汁。”[9]冷战期间，美国在全面与苏联展开政治、经济与军事较量的同时，也确立了 “ 和平演变 ” 和 “ 人权外交 ” 政策，以此颠覆社会主义阵营。此后的美国各届政府虽然出台了不同的国家安全战略，但都继承了美国外交中持久不变的这种基本观念，即把美国的社会制度和价值观扩展到世界各个角落，使越来越多的国家加入 “ 民主阵营 ”，从而继续维护并强化美国的冷战胜利果实。

小布什总统执政期间，执意奉行极端单边主义政策和强硬外交路线，直接导致美国作为 “ 负责任大国 ” 的国家形象急剧下滑，推广美国价值观的进程也严重受挫。为扭转这种被动局面，奥巴马执政以来强调以多边协商取代单边主义，并提出了软硬并蓄的 “ 巧实力 ” 外交

路线。蓬勃兴起的信息技术，恰好为急切寻找新途径来维系其全球霸权的奥巴马政府提供了便捷、好用的新工具。网络空间力量既具有硬实力的作用，能够制造物理毁伤，又表现出软实力的特点，能够在不造成实际毁伤的情况下引发社会混乱，进而影响他国意愿与决策，因此兼具了两者的优势。可见，奥巴马政府加快推行网络空间安全政策的另一目标是，继续有效控制网络空间，抢夺网络话语权，以同化、吸引等软性力量手段实现意识形态的输出与渗透，影响和吸引其他国家，进而将本国的价值观树立为全球共同准则，真正成为全球霸主。

二、奥巴马政府网络空间安全政策的主要内容与特点

（一）以网络空间安全威胁为借口，高度重视关键基础设施防护

“ 威胁 ” 可谓是美国网络空间安全政策中出现频率最高的词汇。美国认为，自己在网络空间中正面临着一场新的看不见硝烟的战争，且已处于劣势，其原因有三：一是美国的社会运转对计算机网络的依存程度远超过全球平均水平，一旦网络空间受到威胁，极有可能导致整个社会陷于瘫痪。特别是美军 “ 陆地、海上和空中的全频谱军事能力均依赖于数字通讯、卫星和数据网络 ” [10]，一旦网络遭受攻击，将给军队造成不可估量的损失。二是美国认为自己的网络空间安全战略、安全观念和机制仍停留在工业时代，已不适应形势的发展变化。特别是关键基础设施多由私营企业掌管，政府借助行政渠道强制这些公司弥补安全漏洞的能力有限，因此给敌人留下了可乘之机。三是网络本身的松散结构决定了其薄弱环节众多，且网络空间进入门槛低，攻击技术和工具易于获取，而防范技术发展则相对滞后。一旦网络攻击技术为未来的对手特别是某些恐怖分子所掌握，将严重危害美国及其盟友的安全。

出于以上原因，美国一直担心未来可能爆发 “ 网络珍珠港 ” 或是 “ 网上 ‘ 9 · 11 ’ ” 事件。为此，奥巴马上台后不断强调，应把网络安全作为国家安全战略的一部分，把网络从基础设施上升为战略资产加以保护。2009 年 3 月，美国战略与国际问题研究中心提交的《确保新总统任内网络空间安全》报告提出的第一条建议就是，网络是国家的重要财富，“ 美国将不惜动用一切国家力量之手段确保网络空间安全 ” [11]。《网络空间政策评估报告》发布当日，奥巴马发表讲话称，网络威胁是 “ 美国经济和国家安全所面临的最严重的挑战之一 ”，网络设施将被视为战略性国家设施 “ 保护该设施将成为国家安全的优先课题 ” [12]。可以说，美国所有网络空间安全政策都是以此为出发点出台和实施的。

（二）以完善领导指挥体系为着力点，全力加强军事能力建设

奥巴马政府认为，美国政府网络空间安全机构存在着战略重心不明、工作职能重叠、缺乏协调配合等问题，因此必须从最高层实施领导[13]，全面协调网络安全机制。2009 年 5 月，白宫宣布组建网络空间安全办公室，负责为总统提供网络空间安全方面的决策方针，协调政府相关政策与活动。一个月后，国防部宣布创建网络空间司令部，负责协调美军网络安全策略及部署，统一指挥美军网络战。由此，美国打造了一体化的综合性国家网络安全领导体制：在网络空间安全办公室统一协调下，国土安全部主管政府机构、社会团体、大型企业等的网络安全政策及其实施与保障；网络空间司令部负责军方网络安全政策和网络战指挥。通过建立新机构和划分职能，美国政府在网络空间的全盘统筹和有机协调水平得到了提升。美国军队也采取了一系列网络空间军事能力建设措施，包括出台陆军《网络空间作战概念能力计划》等军种网络空间作战构想，与政府机构、私营企业及其他国家合作开展 “ 网络风暴 ” 演习，广泛招募网络空间作战人才和加快相关武器装备建设等。2010 年 7 月公布的《网络空间行动

战略》，作为美国防部首份有关网络空间作战行动的综合战略，更为美军有效开展网络空间行动提供了指南和路线图，标志着美军网络空间军事行动已正式转入部署与实施阶段。

虽然美军不断通过各种渠道表态，宣称美军网络空间行动的“ 核心是防御网络攻击行为，防御能力是其他一切作战能力的基础 ”[14]，但稍加分析即可看出，美军在网络空间要达成的目标是，攻防结合，构建网络威慑体系，在军事上巩固自己的“ 制网权 ”。美军参谋长联席会议副主席詹姆斯 · 卡特赖特表示，目前美军将 90%的精力集中在防御层面，只用了 10%的精力对网络攻击者实施威慑，这种战略是不可能持久的，未来美军应将重点逐步转向进攻[15]。美国国防部副部长林恩也明确表示，美方将保留回应严重网络攻击的权利，会在“ 我们选择的时间和地点作出相称且正当的军事回应 ”[16]。新任国防部长帕内塔同样指出，“ 现在我们生活在一个完全不同的世界里，要面对可与珍珠港可比拟的网络空间攻击 ”，“ 我们必须做好应对准备，在网络空间，我们要同时拥有良好的网络进攻与网络防御能力 ”。[17]这些讲话充分显示了美军注重网络空间威慑效应、在网络空间强调攻防结合、必要时不惜主动发动网络攻击的心态，其军事目标绝不仅仅是保证自身网络安全，而是要通过提升网络攻击能力劝阻和威慑所有不利于己的网络攻击行为，实现其在网络空间的绝对自由、绝对优势、绝对安全。

（三）以强调国际网络空间合作为手段，力求维护美国霸权地位

《网络空间国际战略》的出台，表明美国首次将其外交政策目标与互联网政策结合在一起[20]，标志着其关注重点已公开由自身扩展到全球范围。此后出台的国防部《网络空间行动战略》更是引入“ 集体防御 ”理念，展现了美国要在网络空间建立新军事同盟的意图。奥巴马政府之所以一改美国多年来的抵制态度，高调宣传网络空间国际合作，一方面是因为它认识到，即使是美国这样的超级大国，也不可能凭一己之力解决网络空间存在的种种问题，更重要的是，美国希望利用自己雄厚的互联网资源，通过在网络空间的国际行动掌控全球网络发展主导权，改变和影响其他国家的政治体系和价值观念，巩固自身的霸权地位。

首先，美国以“ 互联网自由 ”为借口，对不同意识形态国家的互联网政策大加抨击，借机推行美国青睐的新自由主义思想。例如，2009 年 5 月，微软公司切断古巴、伊朗、叙利亚、苏丹和朝鲜等 5 国 MSN 即时通讯服务；2010 年初，谷歌公司以退出中国市场相威胁要求中国政府停止对其进行的网络审查等行为，都是美国大公司在政府支持甚至鼓动下，企图利用互联网潜能“ 打破封闭的社会 ”[18] 所采取的行动。其次，美国以互联网为工具开展各种外交活动，直接干涉他国内政。2009 年 4 月，摩尔多瓦发生的一场未遂“ 颜色革命 ”因有“ 推特 ”网的参与鼓动而被称为“ 推特革命 ”。同年 6 月，伊朗总统大选后，美国的“ 推特 ”、“ 脸谱 ”等社交网站为伊朗改革派支持者提供了抗议活动的平台，被时任美国防部长盖茨称为“ 美国的重要战略资产 ”[19]。此后，突尼斯、埃及等中东国家政治局势相继陷入动荡，网络媒介同样因具有开放性强、普及度高、实时联络等特点而发挥了独特的作用，也为美国政府介入其中提供了最为便捷的工具。最后，美国企图主导网络空间国际规则制定，从而确立其在网络空间的霸权地位。2010 年 6 月 25 日，白宫宣布启动“ 网络空间可信身份标识国家战略 ”(NSTIC)，建立综合身份标识生态系统框架。这一涉及全球的巨大信息技术工程不仅蕴藏着巨大商机，对于美国摆脱经济低谷、重新占据全球经济制高点具有重要意义，还将使美国借机将增强网络空间安全和打击网络犯罪的通行标准推广到世界其他国家和地区，进而主导国际网络空间安全标准的制定。

三、奥巴马政府网络空间安全政策产生的影响

（一） 围绕网络空间国际规则建构，国际斗争加剧

美国有意主导全球网络空间“ 规范 ”的建立，“ 为所有国家提供一份路线图，使它们清楚应如何作为才不会违反网络空间的国际义务，并在任何环境下始终履行自身责任。 ”[20]有些美国学者将当前的网络空间与 19 世纪的美国西部相提并论，[21] 认为两者的不同之处只在于，键盘取代了左轮手枪，而黑客则成了新的枪手。[22] 在这种局面下，美国急欲建立以美国价值观为核心的网络国际规则。在《网络空间国际战略》中列举的规范和原则包括：支持基本自由、尊重财产权、尊重隐私、预防犯罪、自卫权、全球互通、网络稳定性、可靠访问、利益攸关者共同治理、稳妥处理网络安全等。建立规范是美国网络安全国际战略的一个重点。

美国智库建议美国政府设立一个国际协调一致的计划，并使用一切可以使用的国际工具来助其实现。网络安全的国际战略应当包括主张（advocacy）、合作（cooperation）、规范（norms）和遏制（deterrence）等环节。[23]美国提议建立规范并要求世界各国接受这些规范，它第一步是谋求西方盟国的支持，继而在国际组织中推行美国的主张。在规范得到确立并得到伙伴国支持的基础上，对潜在的违规者予以劝阻、威慑和遏制。如今的美国正如当年美国建立防止大规模杀伤性武器扩散机制那样，利用一切可以利用的机会将网络安全任务植入到各种各样的双边和多边的国际项目和计划之中。

美国在网络空间国际规则建构的过程中，绝不希望自己的这些既有优势遭到削弱，而是要千方百计地将原来的技术优势转化为规则优势，从而进一步维护和巩固其在网络世界的垄断地位。然而，网络空间作为与陆、海、空、天并列的第五维空间，其对世界各国的重要性不言而喻。各个国家都有义务制定严格的法律，并携手合作，共同维护互联网络秩序；但与此同时，各国政府也有权利制定和管理本国网络政策，有义务充分维护本国公民和企业的利益。显然，这与美国的政策取向之间存在着明显的矛盾，各国间围绕国际规则制定的斗争日趋白热化，世界局势因此而面临着新的挑战。

（二）中国成为美国网络空间假想敌，安全形势更加严峻

为确保网络空间安全政策的推行，依据冷战思维的逻辑，美国自然要为自己寻找一个假想敌。由此带来的结果是，美国近年来掀起了一轮渲染“ 中国网络威胁 ”的浪潮，指责中国的互联网政策，夸大中国的网络攻击能力，在没有充足证据的情况下将攻击事件归诿于中国。

2009 年 10 月，美国国会下属的“ 美中经济安全审查委员会 ”发布题为《中国实施网络战和计算机网络应用能力》的评估报告，宣称中国正利用不断发展的信息技术能力，对美国展开“ 长期的、尖端的计算机攻击行动 ”，并搜集美国情报，以便“ 形成对敌人信息流的控制并维持战场空间的控制权 ”。“ 谷歌事件 ”发生后，希拉里公开表示“ 美国政府敦促中国就迫使谷歌公司宣布撤出中国的网络攻击事件展开彻底调查 ”，此后又多次以“ 互联网自由 ”为借口对中国横加指责。对此，英国《卫报》发表名为《在美国的网络战场上，谷歌站在前线》的文章，从时机，动机等多个角度进行探讨，分析谷歌到底是中国网络战的受害者还是美国网络战的“ 领头羊 ”[24]。应该说，谷歌事件并不是单纯某家公司的行为，而是对美国政府网络空间战略的落实与推行。以此为代表的一系列针对中国的行为意味着，美国已经将网络空间的主权、利益与安全问题推到了我们面前。作为在网络空间明显处于劣势的中国，我们必须认清和把握网络空间国际战略形势，应尽快从国家层面制定具有符合我国国情的具有统筹性和前瞻性的网络空间发展战略，建设强大的网络安全防护力量；积极推动国际合作与对话，

倡导和参与构建应对网络空间恶意行为的国际法律框架，及打击跨国网络犯罪的协调机制与技术协助体系，提高我国在未来网络空间新格局中的话语权与分量；加强平时网络舆论战的对抗与反击能力，改变以往我们在国际社会舆论战中的被动局面，赢得更多的国际支持。

（三）美国的政策规划尚不全面，未来发展仍面临诸多障碍

一是安全构想难以落实。虽然奥巴马政府建立了网络空间安全政策的协调与领导机制，但美国现有的相关部门结构非常复杂，各部门间在职能上有着较大的冲突，且都设立有名目繁多的网络安全项目，以此争取研发经费与预算。因此，网络安全职能划分牵涉着巨大的部门利益，短期内尚不可能完全解决。而且，网络空间安全政策的实质，是美国将网络主导权由民间收归政府，因此触及了一系列政治敏感问题。例如，在紧急情况下归私人公司所有的“关键基础设施”能否由政府接管、美国总统能否下令限制或者关闭被攻破的政府机构或网络的互联网通讯等问题上，政府与民间形成了尖锐的对立，从而直接影响了其未来网络空间安全政策的贯彻与落实。

二是网络威慑体系短期内难以构建。威慑战略的基础是能够识别攻击者、进而迅速给予其报复性打击。但从目前来看，由于难以迅速、有效、准确地判定网络空间中的攻击者，因此在应对针对美国信息基础设施发起的攻击时，威慑战略作用可能并不明显[25]。此外，完善的威慑战略需要迫使挑战者在考虑运用武力时，不得不对达成目标的可能收益与需要付出的代价孰轻孰重作出评估，而网络空间特有的难守易攻的特点，以及美国因对网络空间依赖程度极高而相对其他国家形成的战略劣势，都使其威慑难以奏效。

三是网络空间行动规则难以完全按照美国的意愿制定。从美国发布的战略文件看，美国缺乏关于网络空间行动规则的全盘细致规划。例如，在网络空间军事行为合法性的判定方面，关于哪些行为属侵犯他国领土主权、哪些行为达到了使用武力的程度以及哪些行为体应为攻击行为负责等国际法学界的难点问题，美国都未给出解答。在交战规则运用方面，如何将必要、区分和相称等重要原则落实在新型网络空间军事行为当中，美国也未作出说明。虽然有学者认为，在这些问题上保持模糊性可为其今后随意开展网络空间军事行动提供便利[26]，但对世界而言，这极易导致误判对手意图、擦枪走火等事件发生；对美国而言，规则的缺失或是不透明，也不利于其在平时有针对性地开展训练和在紧急事件中迅速开展行动。

对于美国企图通过推行网络空间安全政策在新领域谋取霸权的做法，我们务必有清醒的认识，及时呼吁国际社会展开合作，以《联合国宪章》及其他国际公认的基本准则为指导，以维护本国信息领域国家主权、利益和安全为前提，共同制定和平利用国际信息网络空间的规则与章程，共同解决网络安全问题，维护世界的和平与繁荣。

注释：

[1] Herrera Lucas Geoffrey, *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change*, Albany: State University of New York Press, 2006, pp.3-8.

[2] Joseph S. Nye, Jr., *Cyber Power*, Cambridge: Harvard Kennedy School, 2010, p.1.

[3] 蔡翠红：《美国国家信息安全战略》，上海：学林出版社，2009 年版，第 38-40 页。

[4] US Department of Defense, *Quadrennial Defense Review Report*, Washington, DC , Sepetember 2001, foreword, p.3.

[5] 邬贺铨：《通信技术产业化前景》，引自：中国科学院编：《2000 高技术发展报告》，北京：科学出版社，2000 年版，第 204 页。

[6] Kristin M. Lord and Travis Sharp ed., “America ’s Cyber Future ：Security and Prosperity in the Information

Age", *Report of the Center for New American Security*, June 2011, p.22.

[7] Anne Wells Branscomb, *Who Owns Information?* , New York: Basic Books, 1994, p. 1.

[8] Kristin M. Lord and Travis Sharp ed., "America ’s Cyber Future ：Security and Prosperity in the Information Age", *Report of the Center for New American Security*, June 2011, p.12.

[9] [美]约瑟夫·奈：《美国霸权的困惑——为什么美国不能独断专行》，北京：世界知识出版社，2002 年版，第 158 页。

[10] Major Gen. William T. Lord, "Cyberspace Operations: Air Force Space Command Takes the Lead", *High Frontier*, Vol.5, No.3, 2009, p.3.

[11] 美国战略与国际问题研究中心，《确保新总统任内网络空间安全》，引自：中国国际战略学会军控与裁军研究中心，《美国网络空间安全战略文件汇编》，北京：军事谊文出版社，2009 年版，第 91 页。

[12] 奥巴马《保护美国网络基础设施》讲话，引自：中国国际战略学会军控与裁军研究中心，《美国网络空间安全战略文件汇编》，第 197 页。

[13] 奥巴马政府《网络空间政策评估报告》，引自：中国国际战略学会军控与裁军研究中心，《美国网络空间安全战略文件汇编》，第 163 页。

[14] William J. Lynn, "Remarks On the Department of Defense Cyber Strategy", July 14, 2011, http://www.defense.gov/Speeches/Speech.aspx?SpeechID= 1593

[15] Fahmida Y. Rashid, "Marine General Calls for Stronger Offense in Cyber-Security Strategy", July 15, 2011,http://mobile.eweek.com/c/a/IT-Infrastructure/Marin-General-Calls-for-Stronger-Offense-in-US-Cbersecurity-Strategy-192629

[16] William J. Lynn, "Remarks On the Department of Defense Cyber Strategy", July 14, 2011. http://www.defense.gov/Speeches/Speech.aspx?SpeechID= 1593

[17] Tyrone C. Marshall Jr., "Panetta Discusses Security Challenges in Stratcom Visit", August 5, 2011, http://www.defense.gov/news/newsarticle.aspx?id= 64946

[18] Landler Mark, "U.S. Hopes Internet Exports Will Help Open Closed Societies", *New York Times*, March 7, 2010.

[19] Michelle Levi, "Gates Calls Twitter ‘A Huge Strategic Asset’", June 18, 2009, http://www.cbsnews.com/8301-503544_162-5096183-503544.html

[20] The White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World", May 2011, p.10.

[21] James A. Lewis, "Cyber War and Competition in the China-U.S. Relationship", May 2010, http://csis.org/publication/cyber-war-and-competition-china-us-relationship.

[22] Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower", in Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz eds., *Cyberpower and National Security*, Copublished by Washinton, DC: NDU Press and Dulles: Potomac Books, Inc., 2009, p.254; 另见：Jeffrey Carr, *Inside Cyber Warfare*, Sebastopol: O’Reilly Media, Inc., 2010, p.40.

[23] Center for Strategic and International Studies (CSIS), "Securing Cyberspace for the 44th Presidency : A Report of the CSIS Commission on Cybersecurity for the 44th Presidency", Washington, DC , December 2008, p.20.

[24] Misha Glenny, "In America’s New Cyberwar Google is on the Front Line", *The Guardian*, January 18, 2010.

[25] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica: Rand Corporation, 2009, pp41-52.

[26] Mark Clayton, "A US Cyberwar Doctrine? Pentagon Document Seen as First Step, and a Warning", *The Christian Science Monitor*, May 31, 2011.

（作者简介：中国人民解放军军事科学院美国军事思想专业博士研究生，北京，100091）

收稿日期：2012 年 1 月