美国对中国网络战能力的评估与对策

汪 婧
(深圳职业技术学院 人文学院,广东 深圳 518055)

摘要:近年来,基于国家利益和意识形态的考虑,美国对中国网络战能力的担忧与日俱增。根据对中国网络战能力的评估,美国认为中国可能正利用日益增强的信息技术能力对美发起网络战,对此必须加强对中国的网络防御,寻找网络安全合作伙伴,构建国际网络空间秩序,使网络政策和安全防御一体化,加强网络威慑或击败敌手的能力。美国对华网络空间安全政策充满意识形态偏见和冷战思维,与中国缺乏网络安全战略互信,试图主导网络空间秩序和确保美国网络空间霸权,对中美关系与世界和平造成了危害,因此当务之急是中美建立网络安全战略互信关系及机制,并积极应对两国间出现的网络安全问题。

关键词:中国网络战能力;美国;评估与对策
中图分类号:D771.236 **文献标志码**:A **文章编号**:1000-5315(2015)02-0043-07

随着网络空间和信息技术的急速发展,网络安全问题纷至沓来,美国国家安全局(NSA)甚至宣称"未来战争是网络空间的战争"。2011 年 5 月,奥巴马政府发布"网络空间国际战略"(International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World),称如果遭受的网络攻击威胁到美国国家安全,美国将尽一切所能予以应对[1]。随后美国国防部在是年 7 月发布"网络空间行动战略"(Department of Defense Strategy for Operating in Cyberspace),将网络空间正式列为与陆、海、空并列的第四大行动领域,其战略目的是"有效阻止敌人利用网络对美国发起军事行动"[2]。事实上,自比尔·克林顿总统以来,美国政府颁布了一系列网络安全战略及相关政策,并逐步构建起日臻成熟的美国国家安全战略体系。基于国家利益和意识形态的考虑,美国对中国网络战能力的担忧与日俱增,明确把"假想敌"的矛头对准中国,在国际舆论中渲染"中国网络战威胁论"。本文依据美国国家安全档案馆(National Security Archive)在 2013 年 4 月发布的档案[3]以及美国政府官方发布的国家网络安全战略相关文件,细致分析美国对中国网络战能力的评估和对策,阐述和分析美国对华网络空间安全政策的性质和特点,总结美国国家网络安全战略对中国的启示和借鉴。

一 美国对中国网络战能力的评估

2009 年 10 月,美国国会成立的美中经济与安全评估委员会(US-China Economic and Security Review Commission)发布"关于中国实施网络战和计算机网络开发利用能力的报告"(Report on the Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation)。这份报告利用中方发布的权威公开资料,对中国在和平时期和冲突时期执行计算机网络行动作为战略情报搜集工具的能力作出

收稿日期:2014-04-03
基金项目:本文系国家社科基金项目"冷战及后冷战时期美国对中国的隐蔽行动研究(1949-1999)"(14BSS031)的阶段性成果。
作者简介:汪婧(1982—),女,安徽桐城人,历史学博士,深圳职业技术学院人文学院副教授,主要研究方向为冷战史、思想政治教育。

综合性评估,主要包括五个方面:(一)研究中国人民解放军作战时计算机网络行动战略和整合各种能力的战略水平;(二)弄清在中国计算机网络行动中谁是主要机构和个体行为者,以及民用和军用运营者之间可能存在的联系;(三)考察中国在冲突中针对美国进行计算机网络行动的可能目标;(四)分析中国以美国政府为目标的不间断的网络开发利用行动的特点;(五)梳理中国入侵美国政府和工业网络的大事年表。关于中国的计算机网络行动战略,报告认为,"中国人民解放军正在积极发展计算机网络行动能力,并正在创建战略方针、工具和专门人员以支持传统作战训练";"在战略和作战水平上,获得'制信息权'是中国人民解放军的一个关键目标";"中国已经通过一项名为'网电一体战'的正式信息战战略","这似乎是中国进攻性信息战的基础";"中国可能正在利用其日趋成熟的计算机网络开发能力,实施一场长期的、复杂的计算机网络开发行动,用以搜集美国政府和工业情报"[3]。

2012 年 3 月,美中经济与安全评估委员会再次发布评估报告,题为"占领信息高地:中国计算机网络行动和网络间谍能力"(Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage)。这份报告在 2009 年评估报告基础上进行了详尽的跟踪和扩充,对六个方面的问题进行了评估:(一)中国网络战战略的发展态势;(二)中国用以支持对美国通信网络进行情报渗透和采集的计算机网络开发利用能力的新发展;(三)中国网络攻击美国系统和基础设施,对美国在西太平洋地区和美国本土军事力量的潜在影响;(四)中国进行计算机网络行动和计算机网络开发的主要行为人;(五)中国最杰出和最有影响力的远程通信研究机构、公司和财团的活动和研究方向,美国通讯供应链的潜在风险和美中信息安全公司之间合作的风险和现实;(六)对当代网络罪犯和中国政府资助行动的工具和技术进行比较评估[3]。报告认为,随着中国联合行动和信息战能力的增强,中国有能力利用其防御工具或真正的进攻性武器,给美国及其盟国领袖在决定是否干涉中国发起的冲突中提供更为复杂的风险变量;一旦发生冲突,中国计算机网络行动能力将会给美国的军事行动带来真正的风险;支持中国计算机网络行动的关键实体和机构如中国人民解放军总参谋部第三部和第四部等,商业 IT 公司如深圳华为技术有限公司和中兴通讯股份有限公司等,以及一些开展相关研究的普通高校和军事院校[3]。报告认为,中国人民解放军正在寻找占领现代战争中"信息高地"的途径,计算机网络行动(攻击、防御和开发利用)已经成为中国人民解放军获取初期信息优势和支持其他行动的基础;计算机网络行动对中国领导层来说已经超越单纯的军事含义,而是具有战略意义,并将广泛用于促进中国国家发展的长期战略[3]。2012 年 11 月 9 日,该委员会在给美国国会的年度报告中声称,中国已经成为"网络世界最具威胁性的国家",美国政府应该深入评估中国的"网络间谍"活动,考虑对从中渔利的中国企业加大处罚力度[4]。

2012 年 5 月,美国陆军军事学院(U.S. Army War College)出版专题论文"信息即力量:中国网络力量和美国国家安全"(Information as Power: China's Cyber Power and America's National Security)。该论文认为,"中国人民解放军正在为总体网络战争作准备",包括"进行网络侦察,打造经济损害和破坏关键基础设施的能力,准备破坏常规武装冲突必需的通讯和信息系统,准备实施心理战以影响美国人的决心"[3]。文章考察了中国网络力量的发展状况和网络能力,以及中国如何利用网络力量支持国家安全目标,推究中国网络力量对美国国家安全的威胁程度,并为改善美国网络安全和防御政策提出建议。文章指出,虽然美国必须看到其超级大国地位正遭到中国网络力量的挑战,但是并不意味着网络战不可避免;对此,美国应该认识到网络安全和防御是国家安全和防御问题,不断增强美国的网络防御,与中国直接建立联系和互信,确立网络空间行为准则,还要将北约、印度作为美国的网络安全合作伙伴,制定国际认可的网络空间行为规范;与此同时,美国应该努力使网络政策和安全防御一体化,必须拥有在网络空间威慑或击败其敌手的能力[3]。

2012 年 10 月,美国智库"2049 项目研究所"(Project 2049 Institute)发布题为"对抗中国网络行动:对美国利益的机遇和挑战"(Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests)的评估报告。报告认为,由于政治上的不安全感和全面信息识别的需要,据称中国共产党、中国国家权力机关和中国人民解放军正在针对广泛的国际目标开展一项计算机网络协同行动,而中国的"网络间谍活动"对美国国家和经济安全造成了先进的持续的威胁。报告主要考察的是中国人民解放军总参谋部第三部作为计算机网络开发利用执行机构的基本情况。报告建议,为了应对中国"网络间谍活动",美国应该通过深思熟虑的欺骗来减少信息的价值,加强反间谍活动,与台湾等

国际伙伴增进合作,通过有效的威慑来强加成本等[3]。

二　美国对中国网络战能力的应对策略

通过以上对中国网络战能力的几份评估报告的分析可以看出,美国智库强调中国的计算机网络行动战略水平和开发利用能力在不断提高,针对美国的计算机网络行动不断增加,对美国国家安全构成重大威胁,建议美国政府予以积极应对。据此,美国政府应对中国网络行动和开发利用能力发展的策略主要集中在以下三个方面。

(一)加强对华网络情报活动

根据2013年6月6日爱德华·斯诺登向《华盛顿邮报》和《卫报》披露的美国国家安全局的"棱镜"项目(PRISM),美国国家安全局与谷歌、苹果、微软、脸谱、推特等9家互联网公司自2007年就已经开始合作,对全球范围内互联网数据流进行实时动态监听。斯诺登公布的资料显示,"棱镜"项目主要监控10类信息,包括电邮、即时消息、视频、照片、存储数据、语音聊天、文件传输、视频会议、登录时间和社交网络资料的细节等[5]。随后,美国外交政策网站2013年6月10日发文披露称,一系列机密信息显示,美国国家安全局设有一个名为"定制入口组织办公室"(the Office of Tailored Access Operations,或TAO)的秘密机构,在过去15年时间里,TAO已成功渗透进入中国计算机及电信系统,获得了有关中国国内所发生的"最好的、最可靠的情报"。据称TAO是美国国家安全局信息情报理事会最大、最重要的组成部分,有超过1000名军队及民间的计算机黑客、情报分析家、目标定位专家、计算机硬件及软件设计师、电气工程师等,黑客们每周7日、每日24小时轮班[6]。2014年3月23日,根据《纽约时报》曝光的机密文件,华为是美国国家安全局代号"狙击巨人(Shotgiant)"项目的目标,NSA从2007年开始就侵入深圳华为公司的服务器,以查看其是否与中国政府有联系,同时监控华为高管的通信,并收集华为产品的信息[7]。

(二)增强亚太地区网络防御合作

1947年,美国与英国、加拿大、澳大利亚和新西兰五国达成一项名为"UKUSA"的秘密安全协定,组成后来著名的代号为"梯队"系统(ECHELON)的全球电子情报监听网络(信号情报收集和分析网络,SIGINT),其中澳大利亚负责中国南部和印度地区,新西兰负责西太平洋,加拿大负责苏联的北极地区,英国则主要负责苏联的乌拉尔山以西地区、非洲和欧洲,而美国自己的监控能力覆盖中国北部、亚洲、苏联亚洲部分和拉美[8]。后来美国相继在德国、日本和韩国建立军事基地,监控活动也随之扩大。可见,在亚太地区美国早已同其盟友对中国实行全方位监控。2004年,美国对台军售10套卫星监听截收系统,用于监听大陆的卫星通讯信号和截收卫星通讯中的声音、图像和数字信号,使美国在亚洲建成继韩国之后第二个拥有"梯队"系统的中枢网点[9],进一步增强了美国对中国的网络情报活动能力。

2010年5月,美国国防部宣布成立网络司令部(Cyber Command),隶属于美国战略司令部,以网络防御战作为主要任务。2011年7月,美国国防部发布首份"网络空间行动战略",把网络空间列为与陆、海、空、太空并列的行动领域,使网络政策和安全防御一体化,加强网络威慑或击败敌手的能力,并提出主动防御以及加强与盟友合作[2]。2011年9月14-16日,美澳两国定期部长级磋商,据称在会晤时双方将网络空间防御纳入《澳新美安全条约》[10]。2013年7月22日,"梯队"系统澳、加、新、英、美五国国家安全最高官员在美国加利福尼亚州举行会议,集中讨论关键基础设施的网络安全、打击暴力极端主义以及有关数据交换的倡议[11],从而进一步增强亚太地区网络防御合作。

(三)确立美国主导的国际网络空间秩序

2011年5月16日,美国白宫发布的"网络空间国际战略"高调表示,美国国际网络空间政策强调"对基本自由、个人隐私和信息自由流动的核心承诺",以此为基础提出支持基本自由、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、稳妥处置网络安全等十大网络空间行为规范。为此,美国将综合运用外交、国防和发展三项措施,主要在外交上加强伙伴关系;在国防上采取劝阻及威慑策略;发展上寻求建设技术能力、网络空间能力和政策关系以获得繁荣与安全。为实现这一愿景,美国政府将在七个领域开展活动:(1)经济,推动建立国际标准和创新型的开放市场;(2)保护网络,加强网络安全性、可靠性和恢复能力;(3)执法,拓展合作与加强法治;(4)军事,准备应对21世纪的安全挑战;(5)互联网管治,推动有效和包容性的管治结构;(6)国际发展,提高能力,确保安全,促进繁荣;(7)互联网自由,确保基本自由和隐私安全[1]。从这份"网络空间国际战略"可以看出,美国政府强调"安全"、"繁荣"、"价值观"和"主导权"四个战略目标,其本质是通过一系列战略部署和行动策略,利用其网络技术优势,确立美国主导的国际网络空间秩序[12]。

三　美国对华网络空间安全政策的几个缺陷

第一,美国对华网络空间安全政策充满意识形态偏见和冷战思维。近年来,随着中国国家实力的增长和中国在国际格局中地位的提升,美国对华政策变得更加务实。对华定位为利益攸关者,但从美国多方对中国网络行动能力和开发利用能力的评估报告及其对策建议来看,由于美国情报部门监控到一些对美国政府网络的"黑客"行为和网络间谍活动 IP 地址来源于中国,一些美国官员和分析人士就想当然地认为是中国政府和军队在背后主导和参与了这些攻击行为。例如早在 2010 年美国媒体曾仅依据一个发布病毒邮件的 IP 地址,就宣称山东蓝翔技术学校和上海交大信息安全工程学院是政府背景的中国黑客"大本营",但事实上该 IP 地址来自学生寝室的一台感染木马病毒的电脑。稍有常识便知,网络攻击者总是尽可能地隐藏其真实地址和身份,仅凭 IP 地址的通联关系就确定攻击源来自中国是令人毫无信服的依据的,因此美国对华网络空间安全政策充满着意识形态偏见和冷战思维,美国对于中国防御性军事战略的怀疑和对中国崛起意图的不信任渗透在评估报告之中。但与美苏争霸的冷战时代所不同的是,后冷战时期的冷战思维表现出内在的矛盾,美国不可能像对苏联一样遏制中国,而是采取遏制与合作的双重态度。在 2013 年 6 月 8 日的"习奥会"上,两国元首同意共建"中美新型大国关系",即"不冲突不对抗、相互尊重、合作共赢"[13],这一共识具有历史性意义,也为中美网络安全合作奠定了基础。

第二,美国对华网络空间安全认知误差较大,与中国缺乏战略互信。从美国方面披露的各种报告,如曼迪亚特公司和国防部的报告,都多次讨论所谓的中国对美国的"网络间谍活动"和中国对美国"无间断网络攻击威胁",过分夸大中国的网络战能力。2013 年 2 月 19 日,美国网络安全公司曼迪亚特(Mandiant)发布了一份长达 76 页的安全研究报告,一方面详细阐述了中国人民解放军总参谋部的机构设置与智能,另一方面阐述该公司的重要发现与证据,称其用 6 年时间追踪了针对 141 家美国公司或组织的 1905 次持续入侵行动,其中追踪到 97%的 IP 地址来自上海,而且发现被追踪的入侵使用的是简体中文计算机操作系统,认定此类黑客行动一定得到中国政府的支持,中国人民解放军与这些黑客存在密切联系[3]。2013 年 5 月 6 日,美国国防部公布向国会提交的"2013 年度涉华军事与安全发展报告",声称:"美国政府计算机系统正在遭到中国政府和军队的直接入侵",意即中国正在利用"网络间谍活动"搜集美国外交、经济和国防工业基础等方面情报,并可能很容易利用同样的手段给美国通信网络毁灭性打击[14]。可见,美国对中国的认知误差较大,中美两国在网络安全问题上缺乏战略互信。值得注意的是,在 2013 年 6 月 8 日"习奥会"上,中美两国元首就网络安全问题达成共识,对构建网络安全战略互信具有建设性意义。中方指出,"中国政府高度重视网络安全问题,反对任何形式的黑客和网络攻击行为。中国也是网络攻击行为的受害者,是网络安全的坚定维护者。在网络安全问题上,中美面临共同挑战。网络安全不应成为中美互疑和摩擦的源头,而应成为两国合作的新亮点。双方同意通过已设立的两国网络工作组,加强对话、协调与合作,并通过联合国这一主渠道,推动建立公正、民主、透明的互联网国际管理机制,构建和平、安全、开放、合作的网络空间"[15]。中国政府的态度和立场为中美双方在网络安全上建立战略互信奠定了基础。

第三,美国试图主导国际网络空间秩序,确保网络空间霸权地位。基于美国在网络安全领域的能力建设、制度设计和战略制定无疑有着显著的优势,美国政府试图在国际领域主导网络空间秩序,确保其网络空间霸权地位。2006 年 12 月,美国国防部发布的"网络空间作战国家军事战略"强调:"美国必须拥有网络空间优势,通过一体化的网络防御、侦查和攻击,确保美国的行动自由并阻挠敌方的行动自由。"[16]2011 年 5 月 16 日,奥巴马政府发布"网络空间国际战略"报告,强调"规则"和"秩序"的重要性,声称"通过规范寻求稳定",表示"美国将致力于就可接受的行为达成共识,与那些认为这些规则对于各国自身利益和各国共同利益至关重要的国家结成伙伴关系"[1]。该报告是美国在新形势下针对网络空间规则和秩序建立的重要政策宣示。值得注意的是,它在试图为网络空间确立行为规则的同时,强调"要保留自卫的权利、自由行动的权利,发展和保持网络空间控制能力以及应对潜在危险的应变能力、防护能力、恢复能力和反击能力"等[1]。显然,"网络空间国际战略"的实质是要确立美国在网络空间秩序方面的主导地位,以及保持美国在网络空间的绝对优势。对此,中国应该积极防御,建立健全国家网络安全政策决策体制机制,加速形成我国国家网络安全战略,将中国对网络安全的定义、涵盖的主要领域、遭遇的挑战与威胁、政府应对措施等问题形成官方的文件,从而建立起新型大国对网络安全的新

认识。

四　美国对华网络空间安全战略的评价与启示

从2013年开始至今,美国对中国频繁发起网络安全攻势,给中国带来了巨大的压力和挑战。在这种情势下,中国更要认清美国网络安全战略的实质,坚持和平发展战略,建设好符合中国自身利益的国家网络安全战略。

其一,美国在网络安全问题上对中国抱有的"冷战思维"具有误导性,对中美关系与世界和平造成危害。冷战思维"过分强调国家间意识形态或价值观念的对立,具有'非敌即友'和必须确定一个头号敌手的观念,把前苏联当作评判其他社会主义国家行为的参照物",冷战思维是导致"中国威胁论"的重要因素[17]61-62。由于美国对中国仍然抱有冷战思维,美国政府和智库对中国的网络战能力作出了不确切的评估,过分夸大中国的网络战能力,错误地认为中国政府和军队正在"入侵"美国政府计算机系统,将中国视为"网络世界最具威胁性的国家"[6]。虽然后冷战时期的冷战思维表现出内在的矛盾,美国对中国采取遏制与合作的双重态度,但美国政府和智库的冷战思维仍然具有很强的误导性,不但影响新时期美国的对华政策,对中美关系产生消极影响,也会使世界和平与和谐遭受危害。

其二,中美建立网络安全战略互信在实践中具有必要性和可行性。中美关系是世界上最重要的双边关系之一,对世界经济和政治正产生越来越重要的影响。但是,由于意识形态和国家利益等方面的差异,中美两国在政治、军事、战略安全等方面都存在很深的猜忌和互疑,影响着双边关系向更深层次发展,影响亚太地区乃至整个世界的和平与发展。在网络安全领域,中美两国必须增加信息透明度,及时通过各种对话机制进行真诚沟通以增进战略互信。一方面,增进战略互信能够提高双方信任,减缓紧张情绪,加强国际网络空间的和平与安全,有助于约束双方在网络空间潜在的入侵或破坏行为。另一方面,增进战略互信也是中美两个大国自信和负责任的表现,对共同构建网络空间行为规范具有积极作用,也将促进国际网络空间的安全与稳定。目前,中美两国在网络空间安全领域增进战略互信已有良好的前提:一是中美关系日益机制化,双方在各层次、各领域都建立了对话与合作机制,特别是最高层次的"中美战略与经济对话";二是2013年6月"习奥会"两国元首就网络安全问题达成共识,并将通过两国网络工作组加强沟通与合作,为中美建立网络安全战略互信奠定了基础。

其三,中国相关部门和行业应该借鉴美国国家网络安全战略并积极应对。首先,重视顶层设计,实现有序管理。以中国国家安全委员会为领导核心,统筹国家安全部、解放军总参二部三部、总政联络部、外交部等部门,建立比较健全的国家网络安全政策决策体制,尽快形成中国国家网络安全战略,取得国际网络安全的话语权。另外,可以参照美国创建网络战司令部,对网络安全威胁实施动态监控和主动防御,进行网络攻防对抗演习,提高网络战防御水平。其次,加强科技研发,尽快实现技术自主。我国网络信息领域的核心技术对外依存度较高,重要信息系统安全存在很多隐患。因此,必须加大对核心电子器件、高端通用芯片及基础软件产品(简称"核高基")的研发和投入,中国互联网络信息中心、各大网络信息研究所、高等院校、网络运营商、信息与通信解决方案供应商等相关机构与行业也应该在加强网络安全和防御方面加大科研投入和技术更新。最后,注重网络信息技术人才的培养和利用。利用高等院校和科研机构等多种途径,培养出更多高水平的网络安全工程师队伍;通过政府和企业的资金支持,网罗海内外网络安全领域高技术人才;通过政策扶持和资金援助,加强我国网络安全公司和"白帽"团队(如中国著名的"白帽"团队Keen Team)的建设和发展。

参考文献:

[1]The White House. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World[EB/OL].[2014-03-09]. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[2]Department of Defense. Strategy for Operating in Cyberspace July 2011[EB/OL].[2014-03-09]. http://www.defense.gov/news/d20110714cyber.pdf.

[3]National Security Archive Electronic Briefing Book No. 424[EB/OL].[2014-03-09]. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/.

[4]USCC 2012 Annual Report[EB/OL].[2012-11-09]. http://origin.www.uscc.gov/sites/default/files/annual_reports/2012-Report-to-Congress.pdf.

[5]PRISM. From Wikipedia[EB/OL].[2014-03-09].http://en.wikipedia.org/wiki/PRISM_%28surveillance_program%29.
[6]Inside the NSA's Ultra-Secret China Hacking Group:Deep within the National Security Agency, an elite, rarely discussed team of hackers and spies is targeting America's enemies abroad[EB/OL].[2013-06-10]. http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group.
[7]美监听计划 Shotgiant 曝光 中国业界强烈谴责[EB/OL].[2014-03-23]. http://www.chinanews.com/gj/2014/03-23/5983191.shtml.
[8]ECHELON From Wikipedia[EB/OL].[2014-03-09]. http://en.wikipedia.org/wiki/ECHELON.
[9]台湾军方加入美国监听网络 截收大陆卫星信号[EB/OL].[2004-01-05]. http://news.qq.com/a/20040105/000160.htm.
[10]网络空间成新战场 美国澳大利亚拟结网络战同盟[2011-09-16]. http://www.chinadaily.com.cn/hqsj/shbt/2011-09-16/content_3795921.html.
[11]美国、澳大利亚、加拿大、新西兰和英国要求安全合作达到新水平[EB/OL].[2013-07-25]. http://iipdigital.usembassy.gov/st/chinese/article/2013/07/20130725279491.html#axzz2vxhVtahN.
[12]刘勃然.21 世纪初美国网络安全战略探析[D].长春:吉林大学,2013.
[13]杨洁篪谈习奥会晤成果系中美高层交往之创举[EB/OL].[2013-06-09]. http://news.youth.cn/gn/201306/t20130609_3345337_1.htm.
[14]Department of Defense. Military and Security Developments Involving the People's Republic of China 2013[EB/OL].[2013-05-06].http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf.
[15]杨洁篪谈习奥会晤成果系中美高层交往之创举[EB/OL].[2013-06-09]. http://news.youth.cn/gn/201306/t20130609_3345337_2.htm.
[16]National Military Strategy for Cyberspace Operations December 2006[EB/OL].[2014-03-09]. http://www.carlisle.army.mil/DIME/documents/National%20Military%20Strategy%20for%20Cyberspace%20Operations.pdf.
[17]张小明. 何谓"冷战思维"[J].世界经济与政治,1997,(4).

The United States' Assessment and Countermeasures to China's Cyberwarfare Capabilities

WANG Jing
(College of Humanities, Shenzhen Polytechnic, Shenzhen, Guangdong 518055, China)

Abstract:In recent years, based on the consideration of national interests and ideology, the United States is increasingly concerning about China's cyberwarfare capabilities. Based on an assessment of China's cyberwarfare capabilities, the United States believes that China is likely to use the increasing ability of information technology to launch cyber warfare to the United States, so it must not only strengthen network defense and look for partners, but also build international network space order, integrate make policy and security defense network as well as to strengthen network ability to deter or beat the enemy. The U.S. cyber security policy toward China is full of ideological bias and cold war thinking in that it lacks strategic mutual trust with China on network security and tries to dominate the network space order to ensure network space supremacy.

Key words:China's cyberwarfare capabilities; the United States; assessment and countermeasures

[责任编辑:张 卉]