

美国网络军事战略探析

李恒阳

内容提要 网络军事战略是美国军事战略的重要组成部分,服务于美国国家安全战略。该战略为美军在网络空间有效开展行动、保卫国家利益提供了指导方针。鉴于互联网和其他军事行动领域的紧密联系,网络空间军事化已经是大势所趋。为此,美军不断加强网络战和网络威慑能力建设,进攻性倾向越来越明显。通过加强与盟友及伙伴国的合作打造网络军事同盟,美国力图引领未来网络空间秩序的发展方向。然而,美国的网络军事战略面临一系列挑战。网络空间的结构性特点使得美国难以实现该领域的绝对安全,美军构建和维护网络空间优势地位进而谋求网络军事霸权的构想将很难实现。

关键词 地区与国别政治 美国 网络安全 军事战略 “斯诺登事件”

随着全球互联网技术的迅速发展,虚拟世界的网络武器开发、网络军队部署和相互攻击从未间断。在某些情况下,数字技术的应用速度要快于人们对其安全含义的理解并克服潜在危险。^① 作为信息时代的奠基人和领跑者,美国希望利用其在网络空间的既有优势建立新的军事霸权。由于互联网具有快速通信和信息共享等特点,美国军方不仅要利用其强化部队的军事训练、情报搜集、人员流动和资源

* 李恒阳:中国社会科学院美国研究所助理研究员。(邮编:100720)

** 感谢《国际政治研究》编辑部和匿名评审专家提出的宝贵修改意见,文中的不足和疏漏概由作者负责。

① US Intelligence Community, “Worldwide Threat Assessment,” March 12, 2013, p. 1, <http://www.intelligence.senate.gov/130312/clapper.pdf>, 2014-01-10.

调配,而且要实现现在网络空间内指挥和控制军事行动。21 世纪以来,美国政府和国防部出台了一系列战略文件来指导美军在网络行动。然而,美军对网络空间的严重依赖与网络安全的天生脆弱性形成鲜明对比。如何有效在数字空间开展行动,美军面临诸多的挑战。

关于美国网络军事战略,国外学者(主要是美国学者)进行了广泛探讨,其关注点主要集中在网络战和网络威慑问题上。关于网络战的预防及可能性,有学者认为,网络武器并不会减少战争的毁伤性。若不对其进行适当控制,会使冲突扩大化,美国应该采取措施来规避网络战而不是参与其中。^①有学者认为,控制一国关键基础设施的网络系统在应对网络攻击时非常脆弱。除非国家提高网络防御能力,否则网络战是注定要发生的。^②也有学者提出相反观点,认为网络战过去没有发生过,现在和将来也不会发生。人们普遍谈论的网络攻击充其量不过是破坏、间谍或颠覆行为的升级版,远未达到战争的程度。^③

关于网络威慑,有学者认为这种威慑是脆弱的,只能暂时起作用。因为网络武器不同于核武器,建设足够的网络攻击能力不仅无法阻止对手使用网络武器,反而促进小国在危急中发动不成比例的进攻。^④有学者持相反观点,认为尽管威慑战略在网络空间的实施会遇到困难,但这些困难可以被克服。在实践中,大部分网络威慑战略的目标能够实现。^⑤此外,有学者认为,强大的网络防御虽不能完全阻止网络渗透和利用,但可以缓解网络攻击的影响,从而起到一定的威慑作用。^⑥

美国学者对网络战和网络威慑进行了深入研究,但对与盟国合作及网络情报能力建设方面探讨较少。2013 年“斯诺登事件”暴露出美国军方在网络安全上的一些问题。根据美国政府发布的官方文件及有关智库的研究成果,本文试图在论述美国网络军事战略历史演进的基础上,对美国军事战略的目标、要点及面临的挑战进行探讨。

① Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, New York: Ecco Press, 2010, pp. 121-131.

② Gary McGraw, “Cyber War Is Inevitable (Unless We Build Security In) ,” *The Journal of Strategic Studies*, Vol. 36, No. 1, 2013, pp. 109-119.

③ Thomas Rid, “Cyber War Will Not Take Place ,” *The Journal of Strategic Studies*, Vol. 35, No. 1, February 2012, pp. 5-32.

④ Ross M. Rustici, “Cyberweapons: Leveling the International Playing Field ,” *Parameters*, Vol. 41, Issue 3, Autumn 2011, pp. 40-41.

⑤ Will Goodman, “Cyber Deterrence: Tougher in Theory Than in Practice?” *Strategic Studies Quarterly*, Fall 2010, pp. 128-129.

⑥ Jonathan Solomon, “Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?” *Strategic Studies Quarterly*, Spring 2011, p. 23.

一、网络军事战略的出台背景和历史沿革

美国网络军事战略的形成是一个循序渐进的过程。冷战后,随着互联网在全球的普及率不断增高,网络攻击和网络间谍等问题愈发严重。为了维护美国的安全利益和经济利益,美国政府开始制定在数字空间的战略方针。新世纪以来,白宫和国防部相继出台了一系列与网络军事行为有关的文件,为美军在数字时代如何行动指明了方向。

(一) 网络军事战略的出台背景

计算机网络对美国政府和军队开展行动已经变得必不可少。国防部在全球几十个国家的几百个装置中运行超过 1.5 万个网络和 700 万个计算机设备。^① 由于互联网在设计之初首先考虑的是开放性和信息传输的畅通性,安全措施和身份管理并不是关注重点,这使得互联网在面对攻击时有着与生俱来的脆弱性。黑客攻击很难被溯源,尤其是在攻击发生时。作为全球现代化水平领先的美国部队,其指挥、部署和通信更是严重依赖网络来进行,这就为其他国家、恐怖组织、黑客等实施网络攻击和网络利用(Cyber Exploitation)提供了机会。

十几年来,美国政府和军队的网络持续受到攻击。一些成功的网络入侵行为盗走了大量敏感数据,不仅造成了巨大的经济损失,而且削弱了美军的技术优势和创新优势。被美国情报部门称为“月光迷宫”(Moonlight Maze)的网络盗窃行动从 1998 年起连续两年潜入美国国防部、航空航天局、能源部、私立大学及试验室,盗走了上万份军事材料,包括军事地图、美军部署、军事硬件设计和海军密码等。基础设施保护公司首席执行官詹姆斯·亚当斯(James Adams)在国会作证时说,“被偷的数据价值几千万甚至上亿美元”。^② 2008 年,国防部的秘密计算机网络遭到入侵,病毒扩散到中央司令部网站的秘密和非秘密系统中,把数据传输到外国控制的服务器上。^③ 2009 年 12 月,伊拉克武装分子用价值 26 美元的软件拦截了美军“捕食者”无人机的视频画面,并逃避和监视美军的行动。^④ 2011 年 9

^① US Department of Defense, “Strategy for Operating in Cyberspace,” July 2011, p. 1, <http://www.defense.gov/news/d20110714cyber.pdf>, 2014-01-10.

^② James Adams, “Testimony of James Adams, Chief Executive Officer Infrastructure Defense Inc.,” Hearing before Committee on Governmental Affairs, U. S. Senate, March 2, 2000.

^③ William J. Lynn III, “Defending a New Domain: The Pentagon’s Cyberstrategy,” *Foreign Affairs*, Vol. 89, No. 5, September/October 2010, p. 97.

^④ Siobhan Gorman, Yochi J. Dreazen and August Cole, “Insurgents Hack U. S. Drones,” Dec. 17, 2009, <http://online.wsj.com/news/articles/SB126102247889095011>, 2014-01-10.

月,一个计算机病毒把能记录按键历史的恶意软件安装到美国空军无人机在地面控制站的网络系统中,使内华达州克里奇空军基地的秘密和公开网络都被感染。^①2011 年 7 月,美国国防部副部长林恩在国防大学讲话时承认,“过去十年,国防承包商大量的数据被外国网络入侵者拿走……涉及的文件从坦克、飞机、潜艇的小部件说明书,到机载航空电子设备、监视技术、卫星通信系统和网络安全协议等敏感系统的数据”。^②

美国政府和军方认识到,保护网络空间的利益是保障经济发展和国家安全的重要手段。在 21 世纪,美国要想维持其在陆地、海洋、天空和太空的军事优势,强化在数字空间的行动能力是先决条件。美国军方认为,网络攻击将成为未来国家和地区冲突的重要组成部分,网络空间作为战斗领域的趋势越来越明显。美国在网络空间的军事能力将成为美国维护全球霸权地位的有力保障。为此,美国白宫和国防部陆续发布了网络安全的相关战略文件,以适应互联网不断变化的趋势。这些战略文本为美军在信息时代提供了行动指南。

(二) 网络军事战略的演进

鉴于网络安全问题对国家安全的影响日益凸现,新世纪以来,美国政府和国防部陆续发布了一批有关网络军事行动的文件。这些文件涉及美军网络行动的目标、手段、战略重点和发展方向等方面,有利于国防部在数字空间的行动规范化和系统化。2003 年 2 月,小布什政府发布了由国土安全部酝酿完成的《保障网络空间安全的国家战略》,^③这是美国在网络空间开展行动的基础性文件。文件强调美国在网络空间的三个战略目标:阻止对美国关键基础设施的网络攻击;减少遭到网络攻击时的国家脆弱性;尽量减少损失并迅速从网络攻击中恢复。为此,美国政府要在五个方面重点开展工作:建立国家网络空间安全反应系统;减少网络空间的威胁和脆弱性;增加国家网络安全意识和培训;保卫政府网络空间安全;增加国家和国际网络空间合作。文件要求在全国范围推进网络安全,不仅政府的系统,而且私营机构的关键基础设施也要受到重视。该战略强调美国经济和国家安全对信息技术和信息基础设施的严重依赖性。文件为 21 世纪美国在网络空间开展行动打下了基础,其中一些观点在后来的网络安全文件中被反复提及。尽管该

① James Andrew Lewis, “Significant Cyber Incidents since 2006,” Dec. 19, 2013, <http://csis.org/publication/cyber-events-2006>, 2014-01-10.

② William J. Lynn III, “Remarks on the Department of Defense Cyber Strategy,” Speech at the National Defense University, Washington, D. C., July 14, 2011, <http://www.defense.gov/speeches/speech.aspx?speechid=1593>, 2014-01-10.

③ The White House, “The National Strategy to Secure Cyberspace,” Washington, D. C., February 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, 2014-01-10.

文件不是专门针对国防部的,但其内容对美军制定相关的网络军事行动有重要的指导意义。

2004年,美国参谋长联席会发布《美国国家军事战略》,第一次将网络空间作为一个与陆、海、空和太空并列的战斗领域。文件强调军事行动的三个重点:打击恐怖主义,增加联合作战,促进作战部队转型以应对未来全球挑战。该文件认为,网络攻击将产生灾难性的后果,这种攻击可以视为大规模杀伤性武器的攻击。^①由于当时美国深陷阿富汗战争和伊拉克战争,《美国国家军事战略》对网络攻击论述得不多,但它把网络空间作为一个战斗领域,与陆、海、空和太空并列还是第一次。^②

2006年,参谋长联席会发布《网络空间的国家军事战略》(NMS-CO),专门讨论网络安全问题。^③该文件指出网络空间的特点、存在的威胁和脆弱性,并提出一个确保美国在网络空间的军事优势的战略框架,包括六种手段和四个战略重点。《网络空间的国家军事战略》是对2003年《保障网络空间安全的国家战略》的发展和细化,也为2011年出台《网络空间行动战略》打下了基础。2006年的《网络空间的国家军事战略》的公开版本尽管隐去了许多相关内容,但从剩余部分依然能看出军方的忧虑,体现了较强的忧患意识,对美国在网络空间的威胁和脆弱性进行了较多论述。该文件提出,国家网络空间军事战略的目标是确保美军在网络空间的优势地位。文件把网络空间的行动与国防部在军事、情报和商业领域的行为整合起来。

2008年1月,小布什总统签署54号国家安全总统令和23号国土安全总统令(NSPD-54/HSPD-23),提出《全面的国家网络安全倡议》(CNCI)。^④该倡议涉及多个政府部门,包括国土安全部、管理和预算办公室及国家安全局等,希望通过提升政府的网络能力来抵御未来的入侵。^⑤2008年,倡议的最早签署和听证会都是不

① Chairman of the Joint Chiefs of Staff, "The National Military Strategy of the United States of America," Washington, D. C., Joint Chiefs of Staff, 2004, p. 1, <http://www.defense.gov/news/mar2005/d20050318nms.pdf>, 2014-01-10.

② Ibid., p. 18.

③ Chairman of the Joint Chiefs of Staff, "The National Military Strategy for Cyberspace Operations," Washington, D. C., Joint Chiefs of Staff, December 2006, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf, 2014-01-10.

④ George W. Bush Administration, "National Security Presidential Directives [NSPD]," <http://www.fas.org/irp/offdocs/nspd/index.html>, 2014-01-10.

⑤ The Department of Homeland Security, "Computer Network Security & Privacy Protection," February 19, 2010, http://www.dhs.gov/xlibrary/assets/privacy/privacy_cybersecurity_white_paper.pdf, 2014-01-10.

公开的。^① 2010 年 3 月 ,奥巴马政府公布了这一倡议的部分内容。^② 《全面的国家网络安全倡议》提出了网络安全要达到三个目标。第一 ,建立“国防前线” ,通过共享状态来抵御现存的威胁 ,通过减少脆弱性来阻止未来的入侵;第二 ,通过改善反情报能力和关键信息技术供应链来抵御全方位的威胁;第三 ,扩展网络教育 ,加强跨联邦政府的研发 ,制定并发展威慑敌对或恶意行为的战略。^③

倡议明确提出反情报计划 ,希望利用该计划来侦查、威慑和减少外国支持的网络情报威胁。反情报工作要和其他网络行为整合在一起。倡议还提出了威慑问题 ,希望通过提高预警能力、明确私营机构和国际伙伴的责任 ,以及对国家或非国家行为体的适度反应 ,建立威慑效应。该文件对威慑的论述比较笼统。

在小布什政府后期 ,美国政府对网络安全重视度逐渐提高。2007 年 8 月 ,小布什建立了第 44 届总统网络安全委员会 ,以检查国家网络安全战略需要改善的地方。2008 年 12 月 ,该委员会提交报告认为 ,美国网络安全保护不力是新一届美国政府所面临的最紧迫的国家安全问题之一。^④ 以此报告为基础 ,2009 年 2 月奥巴马任命梅利萨·哈撒韦(Melissa Hathaway) 领导的评估小组对美国的网络安全状况进行评估。

2009 年 5 月 29 日 ,奥巴马政府公布了《网络空间政策评估: 保障可信和强健的信息和通信基础设施》报告。报告对此前涉及的国家网络安全战略进行了广泛评估 ,其中包括《全面的国家网络安全倡议》。报告提出了保障美国数字基础设施安全的五个建议: 加强对网络安全的顶层领导; 构建数字化国家的竞争力; 通过合作共同承担网络安全责任; 建立有效的信息共享和应急反应机制; 鼓励创新。^⑤ 美国政府问责办公室的官员曾建议 ,美国要有网络安全的国家战略来清晰地表达战略目标 and 战略重点。^⑥ 该报告是奥巴马政府推进网络安全政策的基础 ,后来出台

① The Department of Homeland Security, “Hearing on NSPD-54/HSPD-23 and the Comprehensive National Cyber Security Initiative,” March 4, 2008, <http://www.hsgac.senate.gov/hearings/nspd-54/hspd-23-and-the-comprehensive-national-cyber-security-initiative>, 2014-01-10.

② Jaikumar Vijayan, “Obama Administration Partially Lifts Secrecy on Classified Cybersecurity Project,” March 2, 2010, http://www.computerworld.com/s/article/9164818/Obama_administration_partially_lifts_secrecy_on_classified_cybersecurity_project, 2014-01-10.

③ The White House, “The Comprehensive National Cybersecurity Initiative (CNCI),” Washington, D. C., March 2, 2010, <http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>, 2014-01-10.

④ Center for Strategic and International Studies, “Securing Cyberspace for the 44th Presidency, a Report of the CSIS Commission on Cybersecurity for the 44th Presidency,” Washington, D. C., December 2008.

⑤ US White House, “Cyberspace Policy Review,” May 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, 2014-01-10.

⑥ David Powner, “National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation’s Posture,” GAO-09-432T, Washington, D. C., Government Accountability Office, March 10, 2009, <http://www.gao.gov/assets/130/121813.html>, 2014-01-10.

的《网络空间国际战略》和《网络空间行动战略》体现了该报告的宗旨和原则。尽管该报告没有专门论及美军在网络安全方面的问题,但它提出的建议对2011年国防部《网络空间行动战略》具有指导性意义。《网络空间行动战略》是该评估报告思想在军事领域的落实。

2011年5月,白宫颁布了《网络空间国际战略》。^①该文件提出美国在网络空间的核心原则是“基本自由、保护隐私和信息自由流动”,美国国防的目标是和别国一道鼓励负责任行为,反对破坏网络和系统的行为者,劝阻和威慑恶意行为者,有权以适当方式保卫这些关键的国家资产。文件从外交、国防和发展等三个方面论述了美国在未来网络空间的作用,并提出七项政策重点。关于网络军事行为,该文件提出了三个重点。首先,美军对安全的网络环境的依赖性日益增加;其次,建设和加强现有军事同盟以应对未来的网络空间威胁,通过发展在网络空间的集体自卫手段来支撑盟友间的集体威慑能力;再次,扩展与盟国及伙伴国的合作来强化集体安全。美国 and “志同道合”国家的合作将有利于减少集体风险、增强利益攸关者的主动性,从而威慑网络空间的恶意行为。《网络空间国际战略》主要涉及美国外交方面的问题,强调确保网络空间的国际合作。军事问题在该战略文本中篇幅不长,但为两个月后国防部出台的《网络空间行动战略》确立了指导方针,后者是《网络空间国际战略》在军事领域的发展和完善。

2011年7月,国防部公布了《网络空间行动战略》的公开版本。由于该战略绝大部分内容涉及军事机密,国防部仅公开了合计13页的小部分内容。该战略的重点是通过规划美军在互联网领域的军事行动以确保美国的军事优势和维护战略资产安全。《网络空间行动战略》意义重大,它体现了美国政府对网络空间在国家安全领域内重要性的认知。正如国防部副部长林恩所说,“网络空间的威胁促使国防部编写一份新的网络安全战略……其革命性的创新可以提高美国国家安全和经济安全”。^②《网络空间行动战略》提出了五项战略措施:把网络空间视为与陆、海、空和太空同样重要的行动领域;运用新理念来保护国防部的网络和系统;加强与其他政府部门及私营机构的合作;加强与盟国及国际伙伴的合作;加强人才培养和技术创新,等等。这些措施有的和前面提到的一些战略文本有重合,例如,加强与其他政府部门和私营机构合作,加强与盟友合作,培养后备队伍和注重研发等。然而,由于网络时代的快速进步,这些措施的内涵往往有了新的变化。《网络空间行

① The White House, “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,” Washington, D. C., May 2011, p. 12, http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf. 2014-01-10.

② William J. Lynn III, “Defending a New Domain: The Pentagon’s Cyberstrategy,” Washington, D. C., U. S. Department of Defense, https://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx, 2014-01-10.

动战略》的五项措施为国防部在网络空间有效开展行动、保卫国家利益、达到国家安全目标提供了指导方针。这五项措施即彼此独立又相互联系,体现了美军经过多年实践在网络空间战略思想的新境界。该战略发布后,有评论认为其“为国防部军事、情报和商业行动指出了新的前进方向”。^①

纵观 21 世纪以来美国网络军事战略的发展脉络,可以看出三个特点。首先,与军事有关的网络安全战略的公开版本往往有所删减。这说明了与网络空间有关的军事行为还是很敏感的,美军网络战略及思想需要严格保密;其次,与国际盟友和国内私营企业合作一直是美国网络军事战略的重点。这体现了网络空间参与方多元化的特点,也反映了美国无法依靠自己的力量实现对网络的绝对控制。由于美国的多数网络基础设施掌握在私企手中,网络部队的行动对这些企业有很大依赖性;再次,相关网络军事战略文件很少谈及主动攻击。由于规划网络攻击容易引起网络空间军备竞赛,并在国际社会树立负面形象,所以美军要回避这一主题。然而,网络进攻能力是应付网络战的必备能力,美军研发进攻性网络武器是不可避免的。

二、网络军事战略的主要内容

美国的网络军事战略是一个综合性战略,其核心是提高部队的网络战能力,从而在未来数字空间的对抗中获得优势。此外,该战略还包含加强网络威慑能力、情报能力及与盟友和国际伙伴的合作等方面。美国国防部希望通过全面发展自己在网络空间的行动能力,构建攻防兼备的网络战体系。

(一) 提高网络战能力

网络战是指两个或更多政治行为体间的冲突,其特点是故意、有成本地使用网络来攻击对手的关键民用或军用基础设施,目的是迫使对手做出政治上的让步、削弱对手的自卫能力或常规武器报复能力,也可能是为了特定战略目标来塑造对手。^② 尽管网络战发生在虚拟世界里,但在物理世界要产生影响,^③例如,使对手的指挥系统瘫痪或造成人员伤亡等。为了提高网络战的能力,美军在领导机构的设立、研发资助、技术支持、队伍建设等方面采取了一系列的举措。

^① Department of Defense, "DOD Announces First Strategy for Operating in Cyberspace," Washington, D. C., July 14, 2011, <http://www.defense.gov/releases/release.aspx?releaseid=14651>, 2014-01-10.

^② Thomas Rid, "Cyber War Will Not Take Place," *The Journal of Strategic Studies*, Vol. 35, No. 1, February 2012, p. 7.

^③ Gary McGraw, "Cyber War Is Inevitable (Unless We Build Security In)," p. 112.

首先是网络司令部的成立。美国军方认识到,由于网络空间和军事行动领域的紧密结合,把军事行为扩大到网络空间已经是大势所趋。陆、海、空和太空等传统领域都要通过网络进行连接,网络冲突会成为未来战争的一个重要组成部分。美国国防部努力提升本国在网络空间的行动能力是着眼长远的。“为了应对网络空间的复杂挑战和巨大机遇,国防部将进行有效的组织、训练和装备。”^①2010年初,美国国防部成立了网络司令部,负责协调美军不同军种内部的网络指挥部门。此前,美军的网络管理权力分散,缺乏统一指挥。这次重组把美国网络司令部和国家安全局(NSA)安置在同一地点办公并且由一个人领导,从而可以最大限度地利用资源并提高决策效率。国家安全局既保障网络司令部的网络安全,又向其提供情报支持。^②此外,美军不同军种在网络空间的行动和信息也可以直接联系在一起。

其次,美国一直在增加投资推动网络部队的建设。通过网络系统和遥控平台可以改变未来战争的作战方式,网军既可以独立对敌作战,又可以配合其他军种开展行动。为了提高网军的战斗力,五角大楼不仅扩编网络部队,而且投资开发高端网络武器。2013年5月,美国国防部与数据策略公司签署了约2580万美元的合同,并与雷神公司签署了约975万美元的合同。^③这些公司负责开发用于网络战的设备和软件。鉴于此前国防部已经开发过大量用于网络战的设备和病毒软件,未来的网络武器将更注重性能的提升,某些新式网络武器甚至可以帮助美军在敌军军事系统未接入互联网的情况下对该系统实施攻击。在美国国防预算持续削减的背景下,国防部加大在网络部队和网络武器方面的投资表明了美军对网络空间军事化的重视。

再次,为了保证美军在网络空间的自由行动,打造更加有弹性和安全的计算机系统就非常重要。提高自我修复和入侵忍耐能力对维护有弹性的网络意义重大。恢复能力是互联网原本的主要设计目标。^④自我修复能力是一个更高级的能力,它可以使网络自动侦查到错误并修改周围的连接路线,从而只受到很少的影响。^⑤同样,入侵耐受性也是一项高级技术,其目标是即使面对入侵,也要保持关键系统

① US Department of Defense, “Strategy for Operating in Cyberspace,” p. 5.

② Office of the Under Secretary of Defense, “Overview-FY 2014 Defense Budget,” http://comptroller.defense.gov/defbudget/fy2014/FY2014_Budget_Request_Overview_Book.pdf, 2014-04-10.

③ U. S. Department of Defense, “Contracts,” May 31, 2013, <http://www.defense.gov/contracts/contract.aspx?contractid=5053>, 2014-04-10.

④ David Clark, “The Design Philosophy of the DARPA Internet Protocols,” *Computer Communication Review*, Vol. 18, No. 4, August 1988, pp. 106-114.

⑤ C. Green, “Protocols for a Self-Healing Network,” paper presented at IEEE Military Communications Conference (MILCOM '95), November 6, 1995, pp. 252-256.

功能正常运行。^① 对于大规模的互联网,恢复能力的技术还不成熟。考虑到国防部运行 1.5 万个网络,涉及 700 万个设备,成功实施高级技术(自我修复、入侵耐受)是个巨大的挑战。要执行这些技术,需要更换设备、软件和互联网协议。2014 财年,国防部建议网络行动方面的预算为 47 亿美元,^②比上一财年增长 21%。网络领域的增加投资将有利于国防部提高数字对抗能力。

最后,加强网络队伍建设。通过加强网络部队建设,美国的网络战能力在不断提高。2010 年网络司令部成立之初,里面的网军只有几百人。到 2013 年初,司令部的在编人数已接近一千人。2014 年 3 月 28 日,美国国防部长哈格尔宣布到 2016 年将网络司令部在编人数扩至 6000 人。^③ 为了充实网络战后备军并保持网络人才优势,美国国防部每年都从全美各大院校招募大量计算机、数学、语言学等专业的优秀毕业生。近年来,国家安全局在“网络行动计划”(COP)下设立了“国家优秀学术中心”(CAE)项目。该项目通过在一些特定大学开设与网络攻防技术有关的课程,普及有关网络战的知识。据报道,国家优秀学术中心开设的课程除了普通的计算机编程、网络维护外,还包括编写计算机病毒、入侵网络、破解密码、数据挖掘等。2012 年 5 月,国家安全局宣布四所大学获准参加“国家优秀学术中心”项目,分别是达科他州立大学、海军研究生院、东北大学和塔尔萨大学。^④ 2013 年 9 月,国家安全局宣布又有四所大学参与这项计划,它们是空军技术研究院、奥本大学、卡内基梅隆大学和密西西比州立大学。^⑤ 鉴于美国在国际网络空间的已有优势,以及防范未来不断增加的网络攻击和黑客行为,如何不断创新是美国维持这种优势地位的关键。国防部通过与总统执行办公室合作,设立动态的规划来吸引人才,具体措施包括:简化录用程序、人才“无害流动”、开发预备役和国民警卫队的网络能力、继续教育等。^⑥

① Yves Deswarte and David Powell, “Internet Security: an Intrusion-Tolerance Approach,” *Proceedings of the IEEE*, Vol. 94, No. 2, February 2006, pp. 432-441.

② Department of Defense, “Summary of the DoD Fiscal Year 2014 Budget Proposal,” April, 2013, <http://www.defense.gov/news/2014budget.pdf>, 2014-04-10.

③ Jim Garamone, “Hagel Thanks Alexander, Cyber Community for Defense Efforts,” Washington, D. C., March 28, 2014, <http://www.defense.gov/news/newsarticle.aspx?id=121928>, 2014-04-10.

④ National Security Agency, “NSA Announces New Program to Prime College Students for Careers in Cyber Ops,” May 21, 2012, http://www.nsa.gov/public_info/press_room/2012/new_college_cyber_ops_program.shtml, 2014-04-10.

⑤ National Security Agency, “Central Security Service, NSA Announces Four New Schools for Cyber Initiative,” September 4, 2013, http://www.nsa.gov/public_info/press_room/2013/new_cyber_schools.shtml, 2014-04-10.

⑥ US Department of Defense, “Strategy for Operating in Cyberspace,” p. 10.

(二) 加强网络威慑能力

美国军队对网络空间的高度依赖加之互联网在安全上的天生脆弱性,刺激了潜在对手对美国军方发动数字攻击。为了应对网络空间的攻击和破坏,保护自己在网络空间的安全与利益,美国对网络威慑手段越来越重视。威慑主要分为据止性威慑和惩罚性威慑。据止性威慑通过展示有效防御能力,减少攻击者的期望,使其认为进攻成功的概率很小。惩罚性威慑是对敌手的核心利益拥有可信赖的威胁,迫使其认识到发动攻击会得不偿失。鉴于美军在网络空间的技术、资源及人才优势,美国政府更倾向利用惩罚性威慑来捍卫自己在网络空间的利益。

美国希望利用网络威慑扩大化来给潜在攻击者施加更大的压力。这种扩大化表现在反击手段和参与方的扩大上。反击手段的扩大主要指利用网络以外的手段来反击网络攻击;参与方的扩大主要指对一国的网络攻击可能会招致其他国家的报复。2011年6月,时任美国国防部长罗伯特·盖茨在新加坡举行的香格里拉会议上表示,如果敌方的网络攻击构成了战争行为,美国会动用武力进行反击。^①《网络空间国际战略》提出,网络使国家间联系更紧密,所以对一国的网攻可能会影响到其他国家。美国把网络威慑扩展到与盟友的军事合作中。根据美国与澳大利亚、日本等国签署的网络合作条约,参约国一方网络如遭破坏,它可以借用盟友的网络空间发起攻击。集体威慑的建立避免了美国在网络防御上的单打独斗,减轻了美国在人员、资源等方面的压力。为了加强在网络空间的集体威慑能力,美国与盟国及伙伴国进行了一系列网络军事演习。始于2006年的“网络风暴”演习到2013年已经举行了四次,参加国也从四个增加到11个。2011年12月,以美国为首的北约成员国和六个伙伴国举行了代号为“2011网络联盟”的演习,表明北约在网络空间军事化的背景下提高了数字攻防能力的考虑。通过这些军演,美国国防部检验了网络武器的实战效果,提高了与盟友在信息共享、态势感知程度和决策过程等方面的磨合。网络军演扩大了美国军事同盟的内涵,对网络空间的潜在对手形成了威慑。

除了加强对外网络威慑,美国国防部还通过完善内部管理以威慑来自内部的攻击。为了维护美军内部的网络安全,国防部在四个方面开展工作。首先,实施网络防护行动来提高网络安全;其次,通过加强对工作人员的沟通、问责和内部监督,解决内部威胁;再次,执行积极的网络防御来应对外部威胁;最后,开发新的防御行动概念和计算体系。国防部表示,现在的防御是积极防御,不同于以前的被动防

^① Jim Garamone, “Gates Answers Questions for Security Conference Delegates,” Singapore, June 4, 2011, <http://www.defense.gov/news/newsarticle.aspx?id=64193>, 2014-04-10.

御。积极防御意味着网络被实时监督,以便发现、侦查、分析和减少威胁与脆弱性。此种防御可以理解为实时入侵侦查和阻止,其目标是在恶意行为影响网络 and 系统前进行阻止。^① 美国在入侵侦查方面进行了大量研究。由于对手的创新和随机应变,实时侦查是个有争论的问题。美国国防部的战略没有阐述执行积极防御的具体步骤,以及技术的提供者是谁。一般来说,入侵侦查可以通过基于签名的“误用侦查”或者基于行为的“反常侦查”来实现。^② “误用侦查”对已知的进攻会起作用,但会忽略新的攻击(因为没有现存的签名)。另外,“反常侦查”会侦查到未知的新进攻,因为其在统计上偏离正常行为。然而,入侵侦查在实践中很难完美。现存的入侵侦查系统可以实时监督网络,但是检测的精度及因此产生的防护仍然不确定。

(三) 加强情报能力建设

随着国际环境的变化,未来大国的竞争一定程度上取决于情报收集能力和解码能力。为了在互联网中高效率地获取信息并进行分析,美国军方十分重视与其他政府部门和私营机构的合作。“国防部的关键功能和行动依赖于商业资产,包括互联网供应商和全球供应链,国防部对这些行业没有直接的控制力,所以不能有效地降低风险。”^③

在政府部门中,国土安全部是国防部的合作重点。2010 年 10 月,国防部与国土安全部签署备忘录,目的是通过相互提供人员、设备来共同提高网络安全能力,使两个部门在网络空间的行动协调一致。^④ 该备忘录提出,派遣一位国土安全部的主任常驻国家安全局,作为网络安全的项目主管,并要求国防部和国土安全部的分析师联合支持国家网络安全和通信集成中心(NCCIC)。该备忘录把美国互联网的军事和民事管理部门联系在一起,为政府部门间协作打下了基础,体现了一定的战略前瞻性。

美国国家安全局通过法律手段、秘密监控和行政措施,使得美国的一些互联网和电信企业成为情报合作的伙伴。国家安全局通过在这些企业的服务器中增设过滤器、在软件中预留后门,以及拥有破解加密信息的密钥来掌控网络空间流动的信息。根据斯诺登提供的材料,微软公司与国家安全局进行了广泛合作。每次修改

① US Department of Defense, “Strategy for Operating in Cyberspace,” pp. 6-7.

② Ryan Trost, *Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century*, Upper Saddle River, NJ: Addison Wesley, 2009.

③ US Department of Defense, “Strategy for Operating in Cyberspace,” p. 8.

④ Department of Homeland Security and the Department of Defense, “Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity,” October 13, 2010, <http://info.publicintelligence.net/DOD-DHS-MoA.pdf>, 2014-04-10.

加密技术及相关软件技术的时候,微软都会及时给予国家安全局权限,使其能访问公司最新用户数据。^① 微软公司帮助国家安全局绕开其 Outlook 网站门户加密网络聊天功能所使用的加密技术,从而保证国家安全局能在加密前进入 Outlook 邮件,查阅包括 Hotmail 在内的邮件。微软公司下属的 Skype 也同美国政府和军方合作,帮助其收集视频及音频资料。联邦调查局(FBI)也和微软公司进行了密切合作。例如,微软允许联邦调查局进入其云端 Sky Drive 服务系统获取资料,这种云储存服务系统内拥有数以百万计的用户资料。微软公司还和联邦调查局合作研究在 Outlook 网站内如何允许用户设置电子邮件别名的问题。美国军方通过加强与科研机构的合作来促进自身网络行动能力的提高。2013 年 8 月,美国国家安全局宣布和北卡罗来纳州立大学准备合作建设分析科学实验室(LAS)。^② 该实验室主要通过汇集来自政府、学界和企业界的先进理念来对大数据进行分析。安全局的研究主任将担任领导来组织实验室的项目。美国国防部希望通过合作来解决外国信号情报和信息安全方面的挑战,从而使美国在情报处理领域更有优势。

(四) 加强与盟国及国际伙伴的合作

美国军方希望通过和其他国家合作,实现在网络空间的集体自卫和集体威慑,促进所谓“开放、可互操作、安全和可信赖的”国际网络空间标准。国际合作的手段包括信息分享和情况交流。信息分享涉及网络事件、恶意代码的威胁特征、正在出现的行为者和威胁的相关信息。情况交流包括各自网络空间能力建设、教育培训、好的实践经验交流等。^③ 国防部强调在网络空间集体自卫的优势,不仅涉及关系密切的盟国,而且涉及“更多的伙伴国”和“志同道合的国家”。国防部将与盟国和伙伴国密切合作来开发共同的预警能力、参与网络行动能力建设并进行联合训练。通过接触,美国和这些国家可以在网络取证、能力开发、参与演习和公私伙伴关系等问题上沟通意见。这样,在网络军事化的背景下,美国不仅可以减轻经济上的负担,而且可以避免在数字空间孤军作战的不利局面,并树立自己在该军事领域的领袖地位。此外,通过分担责任可以发挥不同国家的核心优势,同时帮助那些网络能力较差的伙伴国提高行动能力,强化网络空间的集体安全。

美国军方与盟友网络合作的典范是所谓的“五只眼”(Five Eyes)安排。这“五只眼”主要指五个国家的军事情报机构,包括美国、英国、加拿大、澳大利亚和新西

^① James Risen, “Report Indicates More Extensive Cooperation by Microsoft on Surveillance,” July 12, 2013, <http://cn.nytimes.com/usa/20130712/c12nsa/en-us/>, 2014-04-10.

^② National Security Agency and Central Security Service, “NSA Creates Partnership with North Carolina State University,” August 15, 2013, http://www.nsa.gov/public_info/press_room/2013/nc_state_partnership.shtml, 2014-04-10.

^③ US Department of Defense, “Strategy for Operating in Cyberspace,” pp. 9-10.

兰。多年来,这几个国家共同承担对网络的监控,分享信息并交流经验。“五只眼”安排是美国对外进行信息情报合作的基础,美国在资源、设备及技术水平等方面要领先于其他四国。此外,美国国防部还与其他国家开展有限的合作,包括称为“九只眼”“十四只眼”等非正式合作项目。除了以上项目,美国与北约成员国的 26 个国家情报机构间的合作机构奈斯赛(Nasici)也进行了广泛的合作。

美国和英国的网络安全合作关系的密切度超过其他盟国。美国国防部通过“棱镜”项目可以监控一系列美国互联网公司的数据,而英国的情报机构也有权进入这个项目的电脑网络。这样的信息共享会让英国相关机构免受本国法律对电子监控行为的制约。根据斯诺登泄露的材料,英国情报部门对数以百万计的光纤通信线路进行窃听,并与美国情报部门分享大量电子邮件及网络交流信息。这一计划被称为“时光”(Tempora)项目,其行动包括在从北美跨大西洋到达英国海岸的光缆上安装拦截探测器。英国政府通信总部(GCHQ)可以将这些线路上的通信内容储存 3 天,并将记录谁在何时与谁联系的所谓“元数据”(Metadata)储存 30 天。^①从数量上讲,英国方面收集的元数据甚至比美国国家安全局收集的还多。在元数据储存这段时间里,英国的情报官员和美国国防部的分析员可以在储存的数据中搜寻任何值得注意的信息。

在亚洲,美国和日本的网络安全合作进展较快。2013 年 5 月,美日之间举行了第一届网络安全对话。对话强调美日两国在国际网络空间有共同的战略目标,两国对于负责任的国家行为标准意见基本一致。两国强调要和私营机构紧密合作以解决网络空间的安全挑战。2013 年 10 月 3 日,美国和日本签署协议,同意加强在网络空间的军事合作。合作范围包括情报、监控、侦查、制订计划、使用设备、扩展威慑、信息安全、培训和军事演习。^②美日两国就网络防御政策工作组(CDP-WG)的职权范围达成一致。该工作组将提升两国网络防御的合作,以及两国军队在网络空间的互动。^③

① Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, “GCHQ Taps Fibre-optic Cables for Secret Access to World’s Communications,” *The Guardian*, Friday June 21, 2013, <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>, 2014-04-10.

② Karen Parrish, “U. S. , Japan Agree to Expand Security , Defense Cooperation ,” American Forces Press Service , Tokyo , Oct. 3 , 2013 , <http://www.defense.gov/news/newsarticle.aspx?id=120902> , 2014-04-10.

③ Joint Statement of the Security Consultative Committee—Toward a More Robust Alliance and Greater Shared Responsibilities , Issued by Secretary of State John Kerry , Secretary of Defense Chuck Hagel , Japanese Minister for Foreign Affairs Fumio Kishida , and Japanese Minister of Defense Itsunori Onodera , Tokyo , Japan , Oct. 3 , 2013 , p. 4.

三、对美军网络战略的评估

网络军事战略是美国军事战略的重要组成部分,服务于联合部队的全频谱作战模式。在未来战争中,美军在网络空间的行动贯穿于决策、进程和反馈的全过程。网络情报收集可以获取高质量的决策信息;战争进程中信息和数据传输系统将陆、海、空、太空连接在一起,可以高速传递作战指令、数据和情报;战争结束后,通过对互联网数字信息的处理可以有效分析军事效果,完善系统以促进联合作战的效率和机制。此外,网络空间存在着一些不确定因素,影响美军开展行动。这些因素主要包括传统的、非正规的、灾难性的、破坏性的、自然的和意外的等六类威胁。为此,提高识别恶意代码和非授权功能的水平对美国网军意义重大。

美国网络军事战略的目标是确保美军在网络这一新兴的军事领域内开展行动的自由,在战时力争获取并保持网络对抗优势,同时置敌人于不利境地;在平时保持网络威慑能力,使潜在对手不敢轻易发动攻击。从长远看,美军希望通过转型建设提升部队信息化水平,削减对手在网络空间的不对称优势,从而保证美国国内网络基础设施的安全,维护经济发展和国家安全利益。为了达到这样的目标,美国不但开发了大量进攻性网络武器,而且加强了基于未来架构的、即插即用的网络防御系统。美军在强化自身网络部队的同时也注重与传统盟友在数字空间的合作。国防部的这些手段和措施将在一定程度上保障美军网络战目标的实现。未来,随着美军网络行动能力的提高,网络军事战略的目标也可能调整。

美国军方在网络空间领域有着传统的优势。美国健全的网络基础设施、成熟的技术手段、大量的计算机人才储备和相关知识的普及为国防部网络能力建设打下了基础。通过与科研机构、私营企业的合作,国防部努力把先进的技术转化成网络产品,服务于未来的网络行动。利用网络空间的信息共享和快速通信来支持军事行动,美军可以大幅度提高在陆、海、空和太空等战斗领域的行动效率。美军对国防部信息网络的依赖具体表现为通过该网美军指挥和控制部队、情报、物流并开发和应用武器技术。^①

互联网的脆弱性是对美国网军的重大挑战。美国军方遍布全球的网络给对手提供了利用和攻击的广阔空间。“使美国成为领先者的技术同样也会帮助那些试图搞破坏的人。”^②广泛散布的黑客工具使得个人或小组有能力对美国发动攻

^① Department of Defense, “2010 Quadrennial Defense Review, February 2010,” http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf, 2014-04-10.

^② The White House, “2010 National Security Strategy, May 2010,” http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf, 2014-04-10.

击,从而威胁其国家安全和经济安全。这种不对称的威胁一定程度上刺激了恶意行为的产生。网络罪犯或黑客可以通过控制大量被感染的主机形成僵尸网络,其目标可能是经济利益、知识产权或者破坏军方的关键系统。国防部的网络产品供应链也是脆弱的。国防部使用的多数信息技术产品是在海外生产和组装的。无论软件还是硬件,其在设计、生产、服务、分配等方面都存在安全隐患,有可能被修改或盗用。此外,如果有内部人员泄露了美军的网络秘密,其对国家安全的影响也非同小可。

在奥巴马第二任期内,美国网络军事战略表现出更强的进攻性。相比克林顿政府的“全面防御”和小布什政府的“攻防结合”网络安全战略,奥巴马政府有意提升美军的网络威慑能力和主动攻击能力。美国表示要对某些网络攻击采取物理武器打击的办法予以还击。网络部队中负责对敌人发动攻击的成员数量首次超过负责防御的成员数量。2013 年,美国网络司令部计划新增 40 支网络小队,其中有 13 支的重点是进攻,其他 27 支的重点是培训和监控。2013 年 3 月,美军网络司令部司令基思·亚历山大表示,“如果美国在网络空间遭受攻击,被称为国家任务团队的 13 支网络小队会发动反击”。^①此外,到 2016 财年,国防部计划再配备 25 个支持小队和 68 个保护小队。^②

随着全球互联网参与者规模的增大,美国认识到单凭一己之力难以维护网络空间安全。为此,加强在网络空间的国际合作成为近几年来美国的关注重点。美国通过倡导维护不同国家在网络空间的共同利益来引起国际社会关注。在此基础上,美国积极促进与盟友及伙伴国的网络交流、网络集体自卫,并构建网络空间行为标准,把美国的战略主张灌输给这些国家。通过打造网络军事同盟,美国不仅可以借助别国力量更从容地掌控网络空间事务,而且有利于塑造和巩固自己网络霸主的地位,从而引领未来网络空间秩序的发展方向。网络空间的国际合作是美军未来应付网络战及开展各项行动的重要基础。

综合来看,美国希望全面占领网络高地,利用其资源、技术、人才、标准制定等优势,确立并维护美国的网络霸权。在网络世界里,美国不但要有“防守之盾”,更要有“进攻之矛”,再结合美国在陆、海、空、太空等领域的优势,从而在网络空间实现绝对的主导权。

① US Government Printing Office, “Information Technology and Cyber Operations: Modernization and Policy Issues to Support the Future Force,” Hearing Before the Subcommittee on Intelligence, Emerging Threats and Capabilities of the Committee on Armed Services House of Representatives, March 13, 2013, p. 15, <http://www.gpo.gov/fdsys/pkg/CHRG-413hhrg80187/pdf/CHRG-413hhrg80187.pdf>, 2014-04-10.

② Department of Defense, “Defense Budget Priorities and Choices: Fiscal Year 2014,” April 2013, p. 14, <http://www.defense.gov/pubs/DefenseBudgetPrioritiesChoicesFiscalYear2014.pdf>, 2014-04-10.

四、网络军事战略面临的挑战

美军制定了较为完善的网络行动战略,不断增加的预算有利于网络部队的建设和软硬件的升级。然而,这并不意味着美国网络军事战略的执行会一帆风顺。国防部在推进该战略的过程中将遇到一系列挑战。

(一) 国内合作面临困难

目前在美国,不同政府部门之间关于保护网络空间的责任还不清晰。总体来说,国防部负责管理军事网络,包括应对网络袭击和发动网络战;国土安全部负责管理民用网络和政府网络,与民生相关的绝大多数网络基础设施由其监督,防止网络犯罪是其重要职责。从技术上讲,最好的网络防御能力在国防部。由于美国在官方文件里没有明确规定哪个部门是网络安全的领导机构,所以容易造成管理混乱的问题。对于一个针对民用网络发起的进攻,国防部有义务提供防御。但由于民用网络归国土安全部管理,国防部如何提供帮助成为问题。2009年《网络空间政策评估》就提出过联邦政府很多部门都担负有网络安全的责任,但存在职权重叠的现象,难以协调一致地去处理相互矛盾的问题。^①只有搞清楚“联邦政府内与网络安全相关的各部门的权利、角色和责任”,^②不同政府部门之间才能够密切合作,对网络基础设施的保护才能效率更高。

与此同时,由于利益冲突,政府与私营机构的合作存在困难。美国政府问责办公室提出要在私营公司和政府部门间努力发展新的信息共享机制。^③然而,在分享以网络为基础的威胁信息方面,私营企业利益攸关方的期待并没有被联邦政府满足。^④一般来说,为了按照政府的规定参与合作,私营公司要增加支出成本。就网络安全来说,企业认为它们对网络更熟悉,对威胁的反应也更快。相比而言,政府的规定往往滞后,而且要消耗企业更多的资源。目前,美国政府主要是希望企业自愿加入与国家的合作,但企业更需要的是激励措施。对公司来说,信息共享是个

① US White House, Cyber Space Policy Review, May 2009, p. 3.

② Peter Fox, “Domestic Cybersecurity Requires Clearer Federal Roles and Responsibilities,” March 2012, http://www.americanbar.org/content/dam/aba/publications/law_practice_today/domestic-cyber-security-requires-clearer-federal-roles-and-responsibilities.authcheckdam.pdf, 2014-04-10.

③ David A. Powner, “Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed,” GAO-40-628, Washington, D. C.: Government Accountability Office, July 15, 2010. <http://www.gao.gov/assets/310/307222.pdf>, 2014-04-10.

④ Gregory C. Wilshusen, “Cybersecurity: Continued Attention Needed to Protect Our Nation’s Critical Infrastructure,” GAO-11-865T, Washington, D. C.: Government Accountability Office, July 26, 2011. <http://www.gao.gov/assets/130/126702.pdf>, 2014-04-10.

复杂的经济问题,有优点也有缺点。^①

此外,美国企业界对依靠联邦政府来监督互联网和预警攻击一直存在疑虑,这使得 2013 年底火眼(Fire Eye)公司收购曼迪安特(Mandiant)公司引起了广泛关注。^②作为网络安全软件供应商,火眼公司开发出独特的探测攻击行为的技术,而曼迪安特公司则能根除把软件植入企业电脑系统的攻击者。两者的结合可以使用户不必等到恶意软件已经进行破坏的时候才被发现和阻止。互联网企业希望通过自身的技术创新提高网络的抗攻击性,它们对美国政府和军方提供的安全保护软件并不放心。

(二) 集体威慑难以实现

美国的网络军事战略除了集体自卫外,还在国际合作中提出了集体威慑问题。美国考虑遵循北约模式,与盟国和伙伴国达成在网络空间开展军事合作的战略条约。如果此类条约规定共享情报或早期预警,应该是容易做到的。但如果利用集体威慑来实现自己在网络空间的利益,似乎要面对更大的挑战。按照传统的军事观点,增加人员和武器数量可以对未来敌手的攻击产生有效威慑。遵循核威慑逻辑,对手应该相信美国盟友拥有一定规模的、对手无法承担的报复和摧毁能力。^③然而,网络环境完全不同于核环境,核武器可以被跟踪并计算弹道运行轨迹,而网络武器的攻击源头很难查找。为了效率,网络威慑必须克服一些现实障碍。^④

如何识别出真正的网络攻击源是参与集体自卫国家的首要任务。在网络世界里,发动攻击的国家或非国家行为体可以轻易地隐藏自己的身份。即使某一个人或团体被怀疑发动了网络攻击,也很难找到充分的证据来证实。从技术上讲,互联网有着与生俱来的脆弱性——安全性较差。互联网在设计上不是要验证信息包源头的 IP 地址、追踪信息包或者其运行轨迹的记录。即使某个信息包被追踪到一个 IP 地址,这个地址也可能是假的。黑客会通过匿名代理或盗窃的账户作为中介发动攻击。而且,很多攻击是通过恶意软件发起的,恶意软件的投放者很难被发现。虽然对恶意软件代码可以进行反汇编处理,但也很难找到攻击者。即使目标国最

① Esther Gal-Or and Anindya Ghose, "The Economic Incentives for Sharing Security Information," *Information Systems Research*, Vol. 16, No. 2, June 2005, pp. 186-208.

② Nicole Perlroth and David E. Sanger, "FireEye Computer Security Firm Acquires Mandiant," January 2, 2014, http://www.nytimes.com/2014/01/03/technology/fireeye-computer-security-firm-acquires-mandiant.html?hpw&rrref=technology&_r=0, 2014-04-10.

③ Matthew Crosston, "World Gone Cyber MAD," *Strategic Studies Quarterly*, Spring 2011, pp. 100-116.

④ David Elliott, "Deterring Strategic Cyberattack," *IEEE Security and Privacy*, Vol. 9, No. 5, September/October 2011, pp. 36-40.

后成功地准确识别出攻击源,溯源过程将是很费时间的。这种反应的滞后严重降低了发动网络反攻威胁的可信度。

进行集体威慑,需要向对手展示己方强大的报复能力。尽管有报道称美国开发出强大的网络武器,但其效果如何并没有定论。网络武器是“一次性”使用的武器,一旦展示,其密码、漏洞等就会很快展示在网络上。^①这样,作为网络武器的软件就会被敌国进行相反的操作。可以说,展示网络武器或网络攻击能力不能产生威慑效果,除非真正使用它们。而且,展示美国的网络攻击能力会引发全球网络军备竞赛。此外,根据美国国防部的相关规定,美国向盟友和伙伴提供的网络武器主要是防御性的,进攻性的武器需要总统特批。这就使美国与其合作国之间产生技术缺口,从而损害集体威慑的力度。

如何让对手感知集体威慑力量是美国的一个难题。目前,美国还没有和任何盟国签署正式文件,承诺在对方遭受网络攻击时给予帮助。对网络威慑一个普遍的误解是:一国发出公开、明确的声明,对其网络或其他领域的攻击将导致常规打击或核报复,这样就能对网络攻击建立可信赖的威慑。^②美国有很多这样的观点,要求政府公开发出明确的警告,对任何攻击美国军事和民用目标的行为用军事打击做出反应——无论是常规打击、核打击还是网络攻击。^③其实,这种声明并不会让对手感受到威慑。首先,由于担心“确保相互摧毁”而使核威慑有效,^④但这并不能影响网络空间的低水平冲突。一般来说,为了避免核战争或常规战争,网络攻击者会控制网络战的强度。尤其当进攻者的战略目标很有限的时候,会尽量避免冲突升级;其次,只有参与集体威慑的国家能够对不同水平的网络冲突发动成比例的反击,威慑才有作用。这就要求这些国家要么拥有不同层次击败对手的能力,要么敢于把冲突扩展到其他领域(例如,用常规军事力量反击网络攻击)。目前看,美国的盟国不一定都拥有各层次的网络战能力。而且,如果攻击者认为美国不愿对网络攻击发动跨领域的反击,其常规威慑和核威慑都可能是无效的;^⑤再次,由于多数网络攻击不会造成人员伤亡或仅造成很少的伤亡,而且现存国际法对在网络空间适用武力的规定也不明确,一些攻击者认为即使发动攻击也不会受惩罚。相

① Eric Talbot Jensen, “Cyber Deterrence,” *Emory International Law Review*, Vol. 26, Issue 2, May 29, 2012, p. 788.

② Amit Sharma, “Cyber Wars: A Paradigm Shift from Means to Ends,” *Strategic Analysis*, Vol. 34, No. 1, 2010, p. 69.

③ Baker Stewart, Shaun Waterman and George Ivanov, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, Santa Clara, CA: McAfee, 2010, p. 30.

④ Eric Sterner, “Retaliatory Deterrence in Cyberspace,” *Strategic Studies Quarterly*, Spring 2011, pp. 62–80.

⑤ James Lewis, “Cross-Domain Deterrence and Credible Threats,” CSIS, July 2010, http://csis.org/files/publication/100701_Cross_Domain_Deterrence.pdf, 2014-04-10.

比发动攻击的低成本,网络攻击的期望收益还是很高的。

(三) “斯诺登事件”的影响

爱德华·斯诺登是前美国国防部承包商雇员。2013 年 6 月以后,他陆续向英国《卫报》和美国《华盛顿邮报》等媒体披露了美国政府对国内外进行的互联网和电话监控情况。

“斯诺登事件”影响了美国与盟友的关系。根据斯诺登披露的材料,美国过去一直对法国、德国、日本等国驻美国使馆进行监控,甚至德国总理默克尔的电话都被监听。尽管后来奥巴马向这些盟国进行了解释,但事件造成的不信任感给这些国家投下了阴影。此外,一些盟友内部的保护公民隐私权组织认为美国与别国的合作有可能损害合作国公民的权利,要求政府检讨此类合作。例如,英国情报部门“政府通信总部”一直与美国国家安全局进行合作,共同监视英国国内外多条高流量光纤线路。在网络上被获取的数据包被两国情报部门分享,双方的情报人员还就一些具体问题交流经验、对话磋商。消息一经披露,引起英国民众的质疑,认为本国政府在破坏公民的隐私权。英国政府不应该为了与美国的合作而损害本国人民的利益。在美国国内,有人怀疑碍于法律和法规的规定,国家安全局不能收集有关美国人的某些信息,但这些信息有可能最后通过英国政府通信总部获取。美国与盟友的合作不仅侵犯了对方公民的利益,也侵犯了本国公民的利益。

“斯诺登事件”增加了美国情报机构获取信息的难度。2014 年 1 月,奥巴马在总统政策指令中提出,美国必须保持和发展稳定的、技术先进的情报能力来保护本国及盟国的安全……解决现在或未来的挑战。^① 过去十年里,国家安全局为了加强信息搜集能力,投入数十亿美元发起了一项秘密行动。该行动通过数码扰频技术,绕过或破解了互联网络空间的不少加密措施,对美国和其他国家的电子邮件、网络搜索、网络聊天和电话通信进行监控。斯诺登泄露了相关机密后,一些恐怖分子试图采取新的联络方式,这导致情报机构截获通信的水平呈下降趋势。对于新的通信方式,情报部门要花很长一段时间才能突入进去展开监控,而如果在这期间发生了问题,情报部门是没法控制的。一些恐怖组织发布了更新的加密软件,让用户可以对即时通信和手机通话进行加密。这些新软件给国家安全局的代码破译人员带来了较大的麻烦。2013 年 7 月 18 日,网军司令基斯·亚历山大上将(Gen. Keith Alexander)在阿斯彭安全论坛上说,“(‘斯诺登事件’)让我们的工作变得更

^① The White House, “Presidential Policy Directive—Signals Intelligence Activities,” January 17, 2014, <http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>, 2014-04-10.

困难……政府将严格限制能在国家情报机构和国防部系统中转移数据的系统管理员的人数”。^①

互联网供应商和电信公司等私企在与政府的合作中更加谨慎。根据斯诺登提供的材料,美国国家安全局和联邦调查局把数据线直接接入微软、雅虎、谷歌等九家美国互联网公司的中心服务器,通过拦截邮件和音视频资料来收集情报。为了维护公司的形象和保护商业利益,这些公司反复否认自己曾同意政府进行广泛的数据收集活动。例如,微软公司表示其不会让任何政府部门大范围或直接进入微软云端(SkyDrive)、Outlook、Skype或其他微软产品及服务。雅虎公司还要求外国情报监视法庭(FISA)允许它公开2008年一项质询的记录。质询内容是要求雅虎公司向情报机构提供用户数据的法律是否违宪。2013年12月,哥伦比亚特区联邦地区一名法官裁决,美国国家安全局应该停止收集公民的信息,收集活动有可能违反了宪法。^② 鉴于保护公民权利组织的抗议和公司的长远发展,互联网企业在与政府的合作中会更加谨慎。如何在政府要求和维护客户利益间寻找平衡是企业面临的主要挑战。此外,政府对互联网供应商的监管还可能潜在地破坏美国在开放性互联网络空间的领导地位。^③

结 论

作为美国军事行动的神经中枢,互联网在整合美军在陆、海、空、太空开展行动方面起着越来越重要的作用。美军对数字空间的严重依赖和该空间天生的脆弱性使得国防部认识到维护网络安全的重要意义。在过去的十几年里,美国政府和国防部陆续出台了一系列关于网络空间的战略文件,用以指导美军在该领域的行动。2011年7月的《网络空间行动战略》在总结过去战略文件的基础上,比较系统地提出了未来美军在网络空间的行动框架。该战略提出的五个政策重点成为美军构建和维护网络空间优势地位的指导方针。

美国的网络军事战略将面临一系列挑战。军方与国内其他政府部门及企业合作存在困难,国防部与其他政府部门关于保护网络空间的责任还不清晰,国防部

^① National Security Agency, "Clear and Present Danger: Cyber-Crime; Cyber-Espionage; Cyber-Terror and Cyber-War," Aspen Security Forum, Aspen, Colorado, July 18, 2013. http://www.nsa.gov/public_info/_files/speeches_testimonies/GEN_A_Aspen_Security_Forum_Transcript_18_Jul_2013.pdf, 2014-04-10.

^② Andrea Peterson, "New Ruling Threatens the Legal Foundation of the NSA's Phone Records Program," December 16, 2013, <http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/16/new-ruling-threatens-the-legal-foundation-of-the-nasas-phone-records-program/>, 2014-04-10.

^③ Marvin Ammori and Keira Poellet, "Security Versus Freedom on the Internet: Cybersecurity and Net Neutrality," *SAIS Review*, Vol. 30, No. 2, Summer-Fall 2010, pp. 51-63.

与私营机构的信息共享可能侵犯公民的隐私权 ,国防部与私营机构的合作还存在利益冲突 ,集体威慑面临现实的障碍。识别出真正的网络攻击源难度较大。如何向对手展示己方的强大报复能力并让对手感知集体威慑力量是有难度的。“斯诺登事件”给美国带来了负面影响 ,该事件不仅增加了美国情报机构获取信息的难度 ,而且影响了美国与盟友的关系。“斯诺登事件”使互联网供应商和电信公司等私企在与政府的合作中更加谨慎。

在网络空间 ,国际电信联盟只有名义上的管辖权。这一领域缺乏法律规范和政治框架 ,在受保护的行为及禁止、限制的行为方面也没有共识。^① 美国希望通过强化自身网络攻防能力 ,有效抵御和打击网络攻击和网络利用行为 ,从而维护网络基础设施安全 ,促进经济繁荣并保障国家安全利益。美国不仅要受益于信息时代的不断创新 ,而且要打压敢于挑战自己的对手。尽管美国在资源、技术、人才、标准制定、盟国合作等方面有优势 ,但网络空间的结构特点使得美国难以实现在该领域的绝对安全。在电子对抗日趋强烈的背景下 ,美国力图建立和维护自己网络超级大国的地位 ,全面控制网络的信息流动、设备更新、技术进步 ,从而实现网络霸权。未来超级大国的竞争将主要体现在数字空间 ,美国要在军事上抢占这块高地。然而 ,世界其他国家和国际行为体出于保护经济利益和维护自身安全的考虑 ,并不希望美国在网络空间一家独大 ,会以实际行动进行掣肘。美国在网络空间建立军事霸权的前景渺茫 ,其前进过程必将坎坷艰辛。

^① Richard N. Haass , *Foreign Policy Begins at Home: The Case for Putting American's House in Order* , New York: Basic Books , 2013 , p. 56.