

美国网络安全战略变化趋势及问题研究

石培培 刘玉书

摘 要：美国方面认为未来十年的网络安全问题的首要挑战将来自中国和俄罗斯，并将视中国为主要对手。在攻击模式上开始由原来的“硬入侵”向“软入侵”转变。其中病毒工具的开发将上升到了战略武器的地位，并将进一步重视社交网络的网络价值。同时，美国在网络安全方面高度重视反介入/区域拒止（A2/AD）战略。在组织架构上，强化了网络安全相关部门联合作战的能力。同时，最近五年来美国在网络安全战略方面加强了亚太地区针对性监控，建立了网络安全问题联动机制。另一方面，美国在网络安全方面也存在自身基础设施运营和政府体制方面的问题，并需要加强对美国网络安全国际战略和公私合作模式相关方面的研究。

关键词：网络安全；网络空间；网络病毒

作者简介：石培培，中国社会科学院美国研究所，中国社会科学院全球战略智库特约研究员、博士；

刘玉书，美国佐治亚理工学院人工智能博士。

随着网络安全问题重要性的日益显现，中美之间涉及网络安全问题的冲突也日益增多。网络安全问题不同于其他国家冲突，网络安全冲突持续存在，并无战争与和平之分，只存在爆发和潜伏两种状态。因此，对美国网络安全战略变化的实时跟踪，是有效进行网络防御，捍卫我国网络空间

本研究是2017年笔者在美为期7个月的调研成果，针对网络战问题先后走访了美国乔治华盛顿大学、乔治城大学、乔治梅森大学、加州大学伯克利分校、哥伦比亚大学、埃默里大学等大学的相关教授，并与美国国际战略研究中心、美国和平研究基金会、大西洋理事会、兰德公司、美国外交委员会等智库和部分IT公司技术人员进行了交流。

特别感谢：对《战略决策研究》匿名评审专家所提宝贵修改意见表示诚挚的感谢。

主权的重要工作。笔者利用今年在美访学机会,对此问题进行了为期7个月的调研。通过对美国智库、大学和网络科技公司等十余家单位的走访,我们发现美国网络安全战略存在较大转变,具体如下。

一、网络安全问题历史背景及未来十年的挑战

(一) 网络安全问题历史简要回顾

历史上首次国家之间的网络安全攻击是1982年由美国对苏联发起的。当时美国间谍通过更改苏联购买的用于控制天然气管道输送管道的计算机软件,从而导致了苏联的天然气管道爆炸。^①早期的网络安全冲突主要是通过人为更改设备控制系统,从而进行工业或者军事设施的物理性破坏。到1988年,康奈尔大学学生罗伯特·塔潘·莫里斯开发了全球第一个蠕虫病毒,导致美国当时88000台通过网络互联的电脑中超过10%停止运转。^②至此,网络安全问题开始由人为直接攻击模式为主转向主要依赖远程控制攻击模式。

1997年美国五角大楼进行了首次网络安全实战演习,发现通过当年互联网上公开可用的网络攻击技术和软件,即可对当时美国的工业基础设施和信息系统进行有效攻击。^③1997年以后,美国网络安全重心开始从军事攻击向国内基础设施战略防御倾斜,以避免数字经济占比日益增加的发展趋势遭受数字化“珍珠港偷袭”的打击。2003年,计算机、摄像录音设备和其他数字系统创造的数字信息总量超过了人类历史上创造的信息的总和。^④网络安全问题由以攻击为主转向数据驱动的信息资源控制,

① Gus W. Weiss, Duping the Soviets, Jun., 2008. <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.html> (访问时间:2017年2月13日)。

② Charles Schmidt and Tom Darby, The What, Why, and How of the 1988 Internet Worm, Nov., 1988. <https://snowplow.org/tom/worm/worm.html> (访问时间:2017年1月22日)。

③ Steven Hildreth, Cyberwarfare, CRS Report for Congress, Jun., 2001. <https://fas.org/irp/crs/RL30735.pdf>

④ Robert O'Harrow Jr. and Greg Linch, Timeline: Key events in cyber history, The Washington Post, Jun., 2012. <http://www.washingtonpost.com/wp-srv/special/investigative/zeroday/cyber-history-timeline/> (访问时间:2016年12月22日)。

大数据开始成为重要的经济和政治资源。同年美国正式界定了网络空间的概念，^⑤将网络空间信息资源列入国家领土资源同等重要的地位。2003年至今，美国与我国在网络问题上的冲突不断，其中涉及国防军事、专利技术等网络信息问题的各种争论和构陷不断增多。其对华网络安全博弈战略战术在此过程中也在不断演化调整并逐步形成了体系。

（二）美国防部认为未来十年美国网络安全问题的首要挑战来自中国和俄罗斯

2017年2月，美国国防部和美国国防科学委员会联合发布《美国网络威慑核心能力建设》报告。^⑥该报告认为美国的网络安全存在三个主要挑战，一是中俄等网络大国已经具备了随时可以通过网络对美国基础设施进行致命打击的能力，并且这种网络攻击的可能性在逐渐增加。美方认为，中俄的网络力量已经使美国处在了战略不利的位置。虽然美国对本土基础设施的网络保护能力在不断进步，但至少在下一个十年，美国的网络防护力量将远远弱于中俄等网络大国的攻击能力。而更致命的是美国军方自身对网络依赖严重，因此构成了制约战斗力的重要隐患。二是区域性力量（如伊朗、朝鲜）对美发动网络安全冲突的趋势增加，甚至可能通过购买和开发恶意网络工具对美国基础设施造成灾难性攻击。三是美国将面临各类非政府组织和个人黑客的持续性网络攻击。

为应对未来十年的网络挑战，美国防部认为需要从三个方面进行准备。一是细化应对不同网络攻击的对抗措施。随着技术的发展，网络攻击的模式越来越多样化，很难找到通用的方式方法去应对所有的网络攻击，因此要提高网络对抗的针对性。二是要提高在大规模网络攻击前提下，美国网军力量、核打击和非核打击力量的防御能力。特别是在遭受打击的前提下快速恢复和形成战斗力的能力。表1为美国防部对美国网络安全冲突防御的基本要求。其核心的要求就是战斗力的快速恢复。三是要强化各种网络基础能力，如增强网络稳定性、带宽快速恢复能力、以及增加网络基础设施安全防护等。

^⑤ The National Strategy to Secure Cyberspace, Feb., 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (访问时间:2017年4月22日)。

^⑥ Task Force on Cyber Deterrence, Department of Defense, Feb., 2017. http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf (访问时间:2017年4月22日)。

表1 美国防部对美国网络安全冲突防御的基本要求^⑦

美国重点防范的潜在网络对抗国家/组织					
攻击内容	俄罗斯	中国	朝鲜	伊朗	ISIS/其他恐怖组织
对美国关键基础设施发动网络攻击	如果网络大国发动类似攻击，将无法躲避。只能加强自身基础设施的建设，如进一步加强电网的稳定性建设等，重点是 被攻击后的快速恢复能力		美国不能容忍任何小国对美国基础设施的网络攻击和挑衅		
对美国核心战斗系统的网络攻击	美国必须全力确保核心战斗系统单元的信息安全。即使在经受远程打击和核打击的情况，也要能保持核心战斗系统的作战力		美国不会容忍任何小国通过网络攻击对其战斗核心战斗部队进行冒犯		美国必须阻止任何类似恐怖组织的网络攻击
对美国其他非核心军事设施的攻击	美国不可能躲避网络大国对美国非核心军事设施及其日常运营的侵扰。此类网络冲突将会成为常规工作的一部分		美国不会容忍任何小国对美国非核心军事相关设施运营网络的侵扰		
各类黑客对美的攻击行动	美国必须在知识产权保护方面阻止黑客的窃取行为。同时也要加强阻止各类黑客通过信息控制对美国事务干涉的行为。如俄罗斯黑客对2016年总统大选的操纵				

二、美国网络安全战略的变化趋势

网络安全攻击方式是多样化的。即可以是破坏设备、也可以是扰乱信息服务，攻击方式可以是远程入侵，也可以是通过目标系统内部人员进行破坏。美国防部认为，网络安全攻击不仅是针对已经上线和开始运营的系统，从系统供应链的视角看，系统开发、测试、运营、更新等系统全周期都具备可攻击性。^⑧ 就对华网络安全攻击而言，美国事实上已远超过了技术攻击的局限性，网络攻击作为一种战略选择，是对华总体战略部署的一

⑦ Defense Science Board.Task Force on Cyber Deterrence , Department of Defense. Feb, 2017. http://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf(访问时间:2017年4月2日).

⑧ Defense Science Board , Task Force on Cyber Supply Chain , Nov. 2016. <https://www.hsdl.org/?abstract&did=799509>. (访问时间:2017年6月22日).

环,随着美国对华战略的调整而在不断变化。具体如下:

(一) 由战略防御为主向战略攻击转变,将中国视为首要竞争对手

2003年2月,美国白宫在当年的《国家网络空间安全战略》中首次正式界定了“网络空间(cyberspace)”的概念。^⑨2009年,美国国防部公布了《四年目标与任务评估》,将网络攻击与网络安全冲突定位为美国军方作战的核心能力,2010年美国正式启用了网军司令部,开始整合国内多方力量,形成网络攻击合力。^⑩到2015年4月23日,美国五角大楼在当年《美国国防部网络战略》发布会^⑪中明确强调,要提高美国军方在网络空间的攻击和进攻能力。并且,该报告首次提出要把网络作战作为重要的战术攻击能力要求。这表明美国网络安全战略正式公开从战略防御转向战略进攻。

白宫在2015年发布的《国家安全战略报告》中指出:“美国作为互联网的发源地,我们有特殊的责任去领导已经存在的网络世界。”报告同时公开将中国作为网络安全战略性防御对象:“美国的繁荣与安全越来越依赖稳定的互联网,我们的经济、安防与医疗卫生依靠我们的信息基础设施进行连接,但却成为了来自恶意政府、犯罪集团和个体挑衅者的攻击目标……在网络安全方面,我们需要采取必要的行动来保护我们的各行各业,建设能有效阻挡来自私人部门或者中国对商业机密等进行窃取的网络防御体系。”^⑫

对中国的竞争性还表现在,美国方面坚信随着中国网络能力的不断增加,会对美国关键基础设施、国家安全和经济构成严重威胁。近年来,在舆论上的指责也在不断加大。最近几年美国方面不断编造各项罪名转嫁国内网络安全问题。如2013年,《纽约时报》公开指责中国“61398部队”对美国信息安全构成了威胁。美国国防部公开指出,“中国已经具备了必要时对美国基础设施及关键部门实施网络安全冲突系统打击的能

⑨ The National Strategy to Secure Cyberspace, Feb., 2003. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (访问时间:2017年3月22日)。

⑩ 李恒阳:《美国网络军事战略探析》,载《国际政治研究》2015年第1期,第113~134页。

⑪ 该报告于4月17日签署,4月23日发布。https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (访问时间:2017年4月22日)。

⑫ National Security Strategy, Feb.2015. <http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf> (访问时间:2017年3月10日)。

力。”^⑬除此之外,美国最近几年不断制造“F35资料失窃”,美国各类公司核心技术失窃等噱头,以莫须有的罪名直指中国。各类智库以及利益相关公司此起彼伏,游说国会与联邦政府,不遗余力争取网络相关事项的经费和政策支持。

(二) 网络安全攻击转向“软入侵”

和平时期的硬入侵容易激发攻击对象的强烈反抗,甚至会进一步提升对方网络安全能力,难以达成目标。对比近年来美国的各种网络攻击行为,笔者发现,对华网络攻击有两种入侵类型:一类是“硬入侵”,另一类是“软入侵”。硬入侵是针对国家“硬实力”,如基础设施、网络底层设备以及重要工业建设的破坏。直接对攻击对象国造成重大的经济损失、社会瘫痪等。另一种是“软入侵”,是相对于硬入侵的物理性攻击而言的,指的是针对一个国家文化、政治价值观、外交政策等涉及影响力、组织力、国家形象和意识形态等“软实力”的攻击。

以美国对中国网络安全攻击为例,笔者通过走访美国智库专家发现,总体来看,美国认为中国网络安全目标可以分为两类:一类是以遏制军队战斗力相关联实物为目标的“硬入侵”;另一类是瓦解政府组织和领导力意识形态体系的“软入侵”。

在抑制军队战斗力的关联实物目标方面,美国认为中国军方使用的信息和通讯技术越多,面对网络攻击时就越脆弱。^⑭美国国防部认为,随着中国经济的转型,对信息技术就愈加倚重,中国之前军方依靠的相对物理隔离的地下和海底光缆,以及基于本土的路由服务器构成的与外界相对绝缘的环境正在难以避免的打破;中国2015年提出的“打赢信息化局部战争”的战略是中国军方信息化防护策略向地方社会及经济实体连接加速的表现,是在加速建立“网络国界和国防线。”^⑮

2017年3月15日,在美国国际战略研究中心主办的“2017年网络冲

^⑬ Office of the Secretary of Defense, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016. April, 2016. <http://www.defense.gov/Portals/1/Documents/pubs/2016%20China%20Military%20Power%20Report.pdf> (访问时间:2017年2月22日)。

^⑭ M. Taylor Fravel. China's New Military Strategy: "Winning Informationized Local Wars." China Brief. June 2015. http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=44072&cHash=c403ff4a87712ec43d2a11cf576f3ec1#. V1BLDPkrK70 (访问时间:2017年3月21日)。

^⑮ 同上注。

突研讨会（Cyber Disrupt 2017）”^{①⑥}上，笔者就中美网络冲突相关问题当面提问美国前国防部政策研究局副局长詹姆斯·米勒，他认为就美国军方而言，2017年及以后一段时间的关注重点是对中国战区及军改后中国新调整部署的网军的实际战力评估。^{①⑦}此外美国国防部对中国应对现代战争的4CI系统（4CI：指挥、控制、通讯、计算机与情报集成信息指挥系统）的快速反应，数据共享及决策等方面的实战能力高度关注，并强调了对中国军队高可靠性通讯及指挥自动化打击的重要性。^{①⑧}

另外，美国方面认为，如果只考虑对解放军进行网络攻击，不考虑瓦解中国政府组织的领导力和意识形态体系，即使解放军遭受了重创也能在强大领导体系下迅速恢复起来。因此针对中国政府领导力和中国意识形态体系的网络攻击比对解放军的网络攻击更有战略价值。美国信息安全专家利比克认为，中国高度统一的政治体系本身就是高价值的战略攻击目标，而且中国的长期稳定需要依赖民族主义和持续的经济增长。因此只要中国经济增长率出现波动，就可以看作是进行意识形态领域网络攻击，破坏中国政府领导力的战略机会。^{①⑨}他认为，经济波动会导致失业，通过网络对中国的年轻人进行渗透，本身能产生巨大的网络攻击作用，其实施成本相对较低，但战略意义甚至高于直接与解放军进行网络对抗。美国考虑的 attack 有三个方面，一是揭露和曝光中国政府领导者相关的个人信息和财产信息；二是针对防火墙进行攻击，让普通中国用户能自由穿越防火墙；三是对涉及信息审查的中国组织、关键公司及技术支持部门进行攻击和破坏。^{②⑩}在和平时期，“软入侵”将会成为越来越重要的网络安全攻击模式。

^{①⑥} CSIS. Cyber disrupt 2017. Mar. 2017. <https://www.csis.org/events/cyber-disrupt-2017>. (访问时间:2017年3月21日)。

^{①⑦} Adam Segal, “Is China a Paper Tiger in Cyberspace?” Asia Unbound, Feb. 2012. <http://blogs.cfr.org/asia/2012/02/08/is-china-a-paper-tiger-in-cyberspace/> (访问时间:2017年1月18日)。

^{①⑧} Office of the Secretary of Defense. Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2016. Apr. 2016. <https://www.defense.gov/Portals/1/Documents/pubs/2016%20China%20Military%20Power%20Report.pdf> (访问时间:2017年1月18日)。

^{①⑨} Libicki M. Pulling Punches in Cyberspace. In: Proceedings of a Workshop on Deterring Cyber-attacks, 2010. p. 123-147.

^{②⑩} Sanger, D. US Decides to Retaliate Against China’s Hacking. New York Times, July 2015. <http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html> (访问时间:2017年5月1日)。

(三) 将病毒工具研发提升到了战略武器的地位

网络病毒的威慑力和破坏性已引起了全球各国的高度重视。网络安全冲突成败的关键取决于病毒工具的先进程度。以“震网”病毒为例，“震网”病毒是首个针对工业控制系统的蠕虫病毒，^{②①}利用西门子控制系统（SIMATIC WinCC/Step7）存在的漏洞感染数据采集与监控系统（SCADA），^{②②}能向可编程逻辑控制器（PLCs）写入代码并将代码隐藏。^{②③}“震网”病毒无需通过互联网就可以实现感染传播，只要目标计算机使用微软系统，“震网”便会伪装 RealTek 与 JMicron 两大公司的数字签名，顺利绕过安全检测，自动找寻及攻击工业控制系统软件，以控制设施冷却系统或涡轮机运作，甚至让设备失控自毁，而工作人员却毫不知情。因此“震网”成为公认的第一个专门攻击物理世界基础设施的蠕虫病毒。

表2为著名网络安全公司赛门特克提供的“震网”病毒的演进版本。赛门特克公司发现，“震网”病毒作为自动感染病毒，并没有预留人为控制后门。例如，一旦该病毒进入伊朗铀分离工厂所在城市纳坦兹，其攻击就无法再阻止。虽然纳坦兹的网络存在物理隔绝和防火墙阻断。但因为纳坦兹的设备要升级和通信，因此仍然存在漏洞。“震网”病毒的感染是从伊朗的基础设施供应厂家开始的，例如电气公司和管道公司。通过感染伊朗这些公司，再通过这些公司网络到达纳坦兹，因为“震网”病毒自身的复制和传播能力，并具备精确识别是否已经到达攻击目标的能力。一旦“震网”病毒确认已经成功感染目标设施，那么对该设施的破坏就成了不可逆的行为。这种病毒一旦在网络上释放，就没有回头或者人为制止的余地。当前美国已将计算机病毒开发提升到了战略武器的重要地位，这很有可能会对未来战争模式产生巨大的影响。

②① Robert McMillan. Siemens: Stuxnet worm hit industrial systems. Computerworld. Sep., 2010. <https://www.computerworld.com/article/2515570/network-security/siemens--stuxnet-worm-hit-industrial-systems.html> (访问时间:2017年4月26日)。

②② Associated Press, Iran's Nuclear Agency Trying to Stop Computer Worm. Independent. Sep. 2010. <http://www.independent.co.uk/news/world/middle-east/irans-nuclear-agency-trying-to-stop-computer-worm-2089447.html> (访问时间:2017年4月11日)。

②③ Gregg Keizer, Is Stuxnet the 'best' malware ever? . Computerworld. Sep., 2010. <https://www.computerworld.com/article/2515757/malware-vulnerabilities/is-stuxnet-the-best-malware-ever-.html> (访问时间:2017年4月19日)。

表2 “震网”病毒进化过程^{②4}

时间	版本	说明
2005.11.3	0.500	注册远程控制服务器
2007.11.15	0.500	提交（通过）公共网络检测
2009.6.4	0.500	感染停止日期
2009.7.22	1.001	代码补丁更新记录
2010.3.1	1.100	代码补丁更新记录
2010.4.14	1.101	代码补丁更新记录
2012.6.24	1.x	感染停止日期

（四）强化社交网络在网络安全问题中的作用

通过对美国国际战略研究中心以及美国和平基金会等相关研究人员的大量走访，我们发现美国未来五年的网络安全重心依然是社交网络体系。主要体现在以下两个方面：

1. 人是整个安全系统中最脆弱的连接点

从互联网茉莉花革命到2013年美国波士顿马拉松恐怖袭击的快速侦破，美国对社交网络的重视程度是逐步提高的，并在对外网络攻击、策反以及对内反恐，政治互动等各领域都发挥了重要的作用。美国乔治城大学信息安全学教授罗伯特·曼德尔在接受访谈时表示：“人是整个安全系统中最脆弱的环节。人本身具有天生的不稳定性。而基于人的社交网络，特别现在线上与线下生活逐步融合的情况下，在情报搜集、网络攻击方面将发挥着最为核心的作用。”美国国防部高级研究计划局信息创新办公室主任约翰·普雷斯伯里指出，“震网”病毒的关键传播，其实是依靠了以色列在伊朗的社交关系网络。^{②5}按照罗伯特·曼德尔教授的观点，其中人在信息安全系统和网络攻击中的脆弱性，主要体现在以下几个方面：

一是再安全的信息系统也无法保证使用者的可靠性。例如U盘的不规范使用，无线网络环境下手机网络与办公网络的互联，不规范电脑操作等都可能带来病毒的释放或者木马的侵染。在熟悉攻击对象社交网络的情况

^{②4} Symantec Security Response, Stuxnet 0.5: How It Evolved, Feb. 2013. <https://www.symantec.com/connect/blogs/stuxnet-05-how-it-evolved> (访问时间:2017年4月13日)。

^{②5} CSIS. Cyber disrupt 2017. Mar. 2017.<https://www.csis.org/events/cyber-disrupt-2017> (访问时间:2017年3月21日)。

下，很容易实现通过人为附着达到攻击对方所在工作网络的目标。

二是特权使用者带来的问题难以预测。一个组织体系中对信息系统使用特权越大的人，其带来的系统性风险也会越大。在实际的保密组织体系中，为了确保信息的可控性，基本上大部分核心信息都掌握在少部分人手里。这对于攻击方而言，找到关键的人，就意味着找到了突破信息系统的钥匙。而定位目标对象，依托社交网络技术，可以实现精准定位。

三是信息系统安全性、可用性和功能性三个系统要素存在结构性矛盾。三个要素不可能同时兼具，如果强调安全性，那么功能性和可用性就会受到影响。美国外交关系委员会数字与网络空间项目研究员亚当·塞格尔认为，随着中国经济转型和信息化程度的提高，其系统漏洞和弱点就会越大，对中国的网络攻击的战略意义会越加明显。^{②6} 这种观点在美国具有代表性。

2. 基于社交网络发动攻击可以直接左右一个国家的政局

一个比较典型的例子，2009年的南非选举中曾出现了利用社交网络监测选票舆情，同时通过操纵相应地区食物稀缺性来控制选举。^{②7} 当选举操纵者通过社交网络发现一个地区的人倾向于投票给不是他们想要的“正确”领袖的时候，那么就会在该地区制造食物短缺。并且，会进一步剥夺他们的工作机会，将这些工作机会转让给那些支持他们需要的“正确”领袖的人。根据南非媒体报道，这个改变选民投票意愿的过程并不需要很长时间。在缺乏食物和工作机会的情况下，人们很快就会妥协。社交网络所反映的巨大人际网络潜力，使得各国对其信息情报和网络安全冲突价值的兴趣与日俱增。

（五）反介入/区域拒止（A2/AD）战略受到高度重视

“反介入/区域拒止（简称反介入战略）”是美国对中国等国反强敌干预战略的一种解读，中国官方并没有这种提法。所谓“反介入”，是指通过打造反舰弹道导弹、反舰巡航导弹、高性能战斗机、先进水雷、静音潜艇、

^{②6} Segal A. US Offensive Cyber Operations in a China-US Military Confrontation. June 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836203（访问时间：2017年3月19日）。

^{②7} South Africa: Food Used as Election Weapon, Say Monitors. Apr. 2009. <https://www.social-engineer.org/wiki/archives/Governments/Governments-FoodElectionWeapon.html>（访问时间：2017年3月21日）。

反卫星武器、网络武器等系统迫使敌方军队不得不在远离本国主权区域武器的有效射程之外活动，从而丧失对本国近海危机的介入能力。2003年，美国战略与预算评估中心的安德鲁·克雷宾涅维奇等人在其《应对反介入和区域拒止挑战》的报告中正式提出该概念。随后，它迅速被美国观察家和决策者所接受，高频率的出现在美国政府、军方及智库的文件或报告之中。^②

“反介入/区域拒止”作战体系主要由两大核心系统组成，一是情报、监视与侦察系统（ISR），二是具备快速反应和联动的能力打击系统。近两年来，反介入/区域拒止战略在美国网络安全方面，受到了高度重视。

反介入战略在网络攻击方面有两层意思，一是战术层面的反介入，主要指的是对主权网络空间的反介入。例如通过精准的网络攻击，摧毁卫星图像侦察、破坏敌方导弹系统、海军及空军导航系等。据美国国际战略研究中心信息安全专家伊森·索恩透露，在战术层面，还有意识形态拒止的意思，例如屏蔽恐怖分子信息等，但这并不会被提及，而是由各种民营企业自己把握。二是战略层面的反介入，战略层面上，网络攻击的反介入讨论比较少，但事实上却受到了很大的重视。网络攻击层面的反介入战略指的是具备完全掌控本国网络以及可以完全防止别国对本国网络设施进行攻击的能力。根据我们与美国主要智库研究人员交流发现，从2012年开始，美国就已经将网络攻击的反介入战略列为了重点。

经过与网络反介入战略专家，美国梅里马克大学政治学与信息安全副教授艾莉森·罗素的沟通，她认为美国的网络攻击反介入战略主要体现在几个方面：一是在网络物理层方面，主要涉及海底光缆通讯安全、EMP（电子脉冲炸弹）威胁等。二是逻辑层面的安全，包括全球13个DNS根服务器集群以及美国国内网络系统稳定等。艾莉森·罗素认为，美国最有效的网络反介入战略是随时具备击溃敌方反介入的网络攻击能力。她以中国为例，进行了说明。她说中国与美国以及东亚各国数十条海底光缆相连，美国不可能完全切断与中国的网络光缆连接。并且中国还有自己成熟的、独立覆盖全球的卫星网络，并备有无人机地空路由系统，如果发生网

^② 胡波，“美国人眼中的中国‘反介入’威胁及其应对”，《中国海权策：外交、海洋经济及海上力量》，网址：<http://blog.ifeng.com/article/33534490.html>（访问时间：2017年4月22日）。

络安全冲突,美国不可能通过物理阻隔的方法来对中国的网络攻击进行反介入,而只能采取以攻代守的方式,通过网络攻击和网络安全冲突击溃中国的网络体系,从而实现自保。这也是美国网军相关方面,对中国的网络反介入能力和相关情况高度重视的原因。

(六) 网络安全相关部门组织架构设计更加侧重多部门联合作战能力

美国原中央情报局局长迈克尔·海登在接受媒体采访时透露,2010年“震网”病毒攻击爆发后,美国有些部门其实也遭到了误伤;同时也透露了美国对外网络作战缺乏统一协调的问题。因此在当年成立了美国网军司令部。^②从组织结构看,美国网络安全冲突组织有战斗部和战斗支援部两个部分组成。作战部由美国网军司令部统一协调,支援部由美国战斗支援局下属的国防信息系统局以及国家安全局等九个职能局联合组成。

1. 美军网军司令部

2010年10月1日成立了美国网军司令部,该司令部收编了美国第二陆军(美国远征军),并整合了预备役部队、各军种网络作战部队、合作企业、相关科研机构,形成了美国网络作战的整体力量。^③美国网军司令部是全球首个统一规划管理美国各军种的网络司令部,是美国战略司令部下的一个次级联合司令部,^④与美国国家安全局相邻,都在马里兰州米德堡。该司令部下属机构如图1^⑤所示,其组织结构涵盖网络作战各个方面。美国网络司令部的核心使命是整合已有资源、协调各单位进行立体式

^② General Michael Hayden discusses the Stuxnet Virus on 60 Minutes. <https://www.youtube.com/watch?v=8HK3XPXBbNk>

<https://www.youtube.com/watch?v=0FEr0DFwvcY> (访问时间:2017年6月19日)。

^③ The Relationship of U. S. Army Cyber Command and Second Army. <http://www.arcyber.army.mil/Pages/History.aspx> (访问时间:2017年6月19日)。

^④ 2017年8月中旬,特朗普宣布将提升网军司令部的地位。但根据美国国防部相关网页的官方说明,以及作者本人直接致电美国网军司令部问询(美国网军司令部电话:402-294-4130),截至2017年10月12日,美国网军司令部依然是美国战略司令部下的一个次级联合司令部。相关网址:https://www.washingtonpost.com/news/checkpoint/wp/2017/08/18/president-trump-announces-move-to-elevate-cyber-command/?utm_term=.89418d32a0d9

<http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-us-cybercom/>

^⑤ 根据美国网军司令部资料绘制,网址:<http://www.arcyber.army.mil/Pages/USCyberCommand.aspx> (访问时间:2017年4月19日)。

网络防御与攻击,对网络空间上的攻击者和破坏者进行精准有效打击。该司令部的成立是美国网络威慑从防守转向进攻的重要标志。

2. 美国国防部战斗支援局下属相关机构

战斗支援局下属9个职能局,其中与网络安全冲突直接相关的是美国国防信息系统局和美国国家安全局。

美国国防信息系统局(DISA),隶属于美国国防部战斗支援局(图2^③),职能是为白宫、军方及联合作战司令部提供信息技术支持。该局前身是1960年成立的国防通讯局,1991年更名为国防信息系统局,主要工作集中在硬件通讯的基础设施的整合。该局核心任务是确保作战指挥与控制系统的稳定运行。该局涉及信息作战的部门有三个:国防频谱管理部(DSO),主要负责通讯频谱管理。战区网络作战中心,整合各安全中心、网络攻击部队、通讯卫星支持等有效整合。国防部信息网络联合部队总部(JFHQ-DODIN),主要履行指挥职责。

美国国家安全局负责监听的包括电台广播、通讯、互联网,尤其是军事和外交的秘密通讯,是世界上单独雇佣最多数学博士和电脑专家的组织。美国国家安全局继承了第二次世界大战中成功破译敌方密码的工作(美国军情八处)。此外美国国家安全局有自己的芯片工厂和研究基地,并且和私营研究机构和设备生产商保持着广泛的联系。^④

综合图1和图2可以看出,战斗支援局和网军司令部均是横向组织结构。即其所属的职能局和作战部队均纵向率属于其他相关职能部门,接受不同职能上级单位的垂直管理。同时也接受战斗支援局和网军司令部的横向领导。这种条块结合,以作战为导向的双重领导体系,能有效突破各部门单位之间的隔阂,迅速形成战斗力。这对要求快速反应和长期保持信息高度共享的网络作战而言是非常有效的设计。

^③ 根据美国国防部资料绘制,网址:<http://dcmo.defense.gov/Portals/47/Documents/OSD%20DA-FA%20Organization.pdf>

<https://www.defense.gov/About/Military-Departments/Unified-Combatant-Commands/>(访问时间:2017年4月19日)。

^④ NSA.gov. <https://www.nsa.gov/about/faqs/>(访问时间:2017年4月19日)。

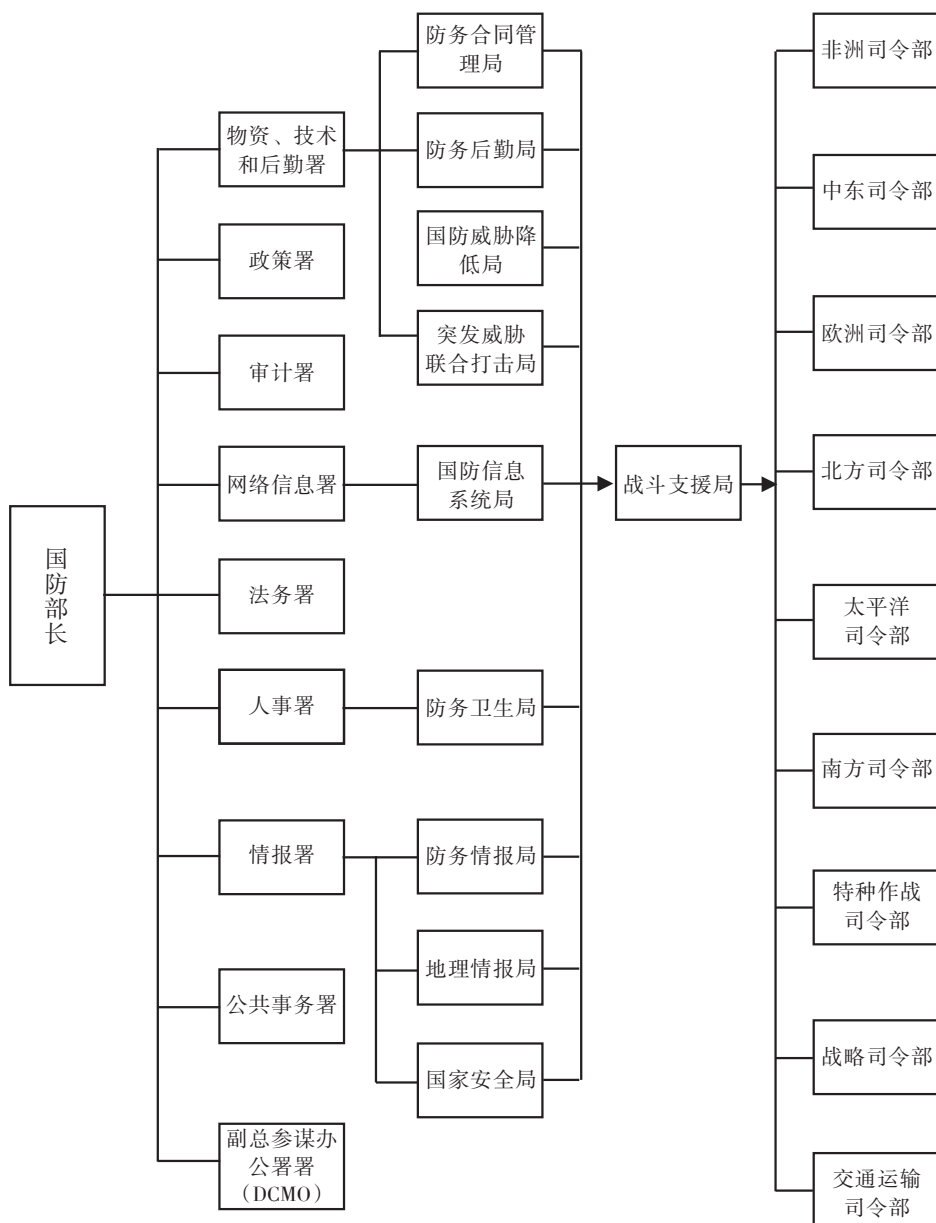


图1 美国网络安全冲突战斗支援体系组织架构

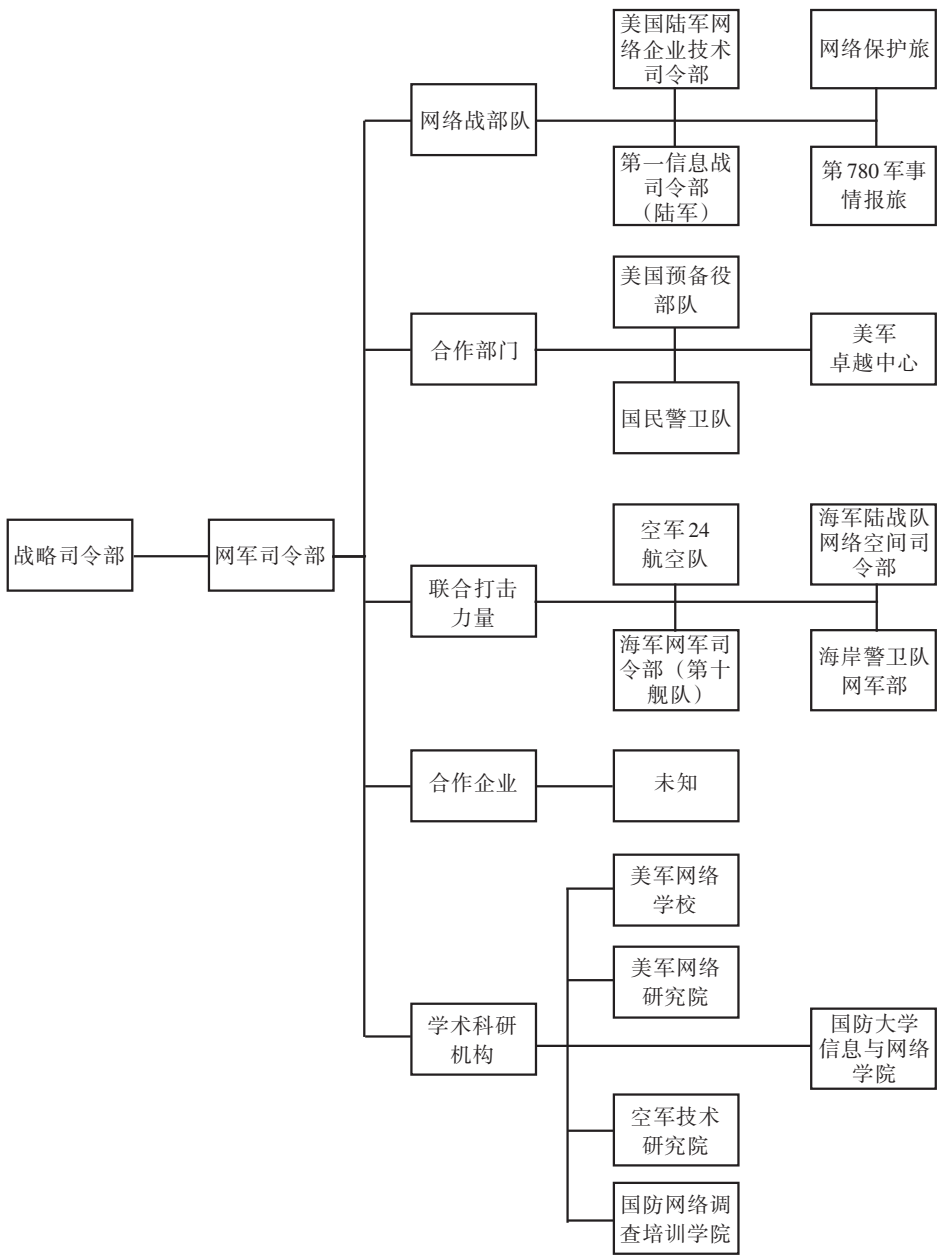


图2 美国网络安全冲突战斗作战体系组织架构

三、近五年来美国网络安全战略的重要部署

(一) 加强与印度、日本等地区的网络安全合作

一是积极推动与印度合作,加强区域性、针对性监控,建立网络安全问题联动机制。美国军方要求网络进攻能够“一招制敌”,即一开始就必须造成敌方大面积瘫痪等重大损失,使其丧失还击能力。2013年7月,印度颁布了国家网络安全法,并提出了未来5年要发展50万名网络专家的计划。同年,印度还设立了国家信息基础设施保护中心并开始与美国开始逐步展开深度合作。^⑤2016年美国与印度达成了网络合作战略合作框架协议,^⑥其中关键点是开展网络信息的深度共享和网络信息安全的联防。二是推动美日网络安全合作,除印度外,2016年在兰德公司,美日双方召开了一次非常重要的网络合作会议,并达成了战略合作意向。^⑦该会议报告中提及中国的内容达40余次,主要讨论如何对中国开展联合防御问题。合作内容涉及到了包含途经日本的海底网络光缆管理、网络安全互信和联防、下一代网络开发等内容。特别需要注意的是,该会议提出了建立美国、日本和澳大利亚网络合作三边关系的共识。美日、美印以及未来可能进一步加强的美澳之间的网络合作,对未来中美两国的网络竞争存在的影响需要进一步研究。

(二) 建立主动抑制潜在网络威胁体系

即发动防御性攻击行动,在攻击者发动攻击之前将其进行有效抑制,并尽可能提高网络攻击者的攻击成本。2015年,时任美国总统奥巴马于当年4月1日签发网络攻击制裁总统令,授权美国政府部门对通过网络威

^⑤ Curtis L. The Cyber Bridge to Improved India-U.S. Cooperation, The Heritage Foundation. Oct, 2014. <http://www.heritage.org/asia/commentary/the-cyber-bridge-improved-india-us-cooperation> (访问时间:2017年5月9日)。

^⑥ Framework for the U.S.-India Cyber Relationship. The White House, June 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/06/07/fact-sheet-framework-us-india-cyber-relationship> (访问时间:2017年7月1日)。

^⑦ Rand Corporation. Strengthening Strategic Cooperation. US-Japan Alliance Conference.2016. https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF351/RAND_CF351.pdf (访问时间:2017年6月20日)。

胁美国利益的组织或个人进行制裁。根据2015年美国国防部发布的《美国国防部网络战略》，美国网络司令部的直属队伍由之前计划的140支变为133支。总数减少的同时，新增了13支“国家核心任务队伍”和27支“网络安全冲突攻击队伍（表2）”。并且进一步灵活化了用人机制，时任美国国防部部长卡特亲自前往硅谷招募人才。

表2 美国到2018年要建成133支网络部队^⑧

军队名称	队伍数量	队伍职责
国家任务军	13	维护美国国家核心利益，对抗严重网络攻击
网络防御军	68	主要负责美国国防部所属网络防御
网络攻击军	27	执行网络攻击命令，执行网络威慑和持续性网络威慑及攻击
技术支援军	25	为国家任务和战斗任务提供分析、计划和技术支持

四、美国网络安全自身存在的问题

在网络安全方面，美国方面主要存在两个问题，一是网络基础设施运营体系相对脆弱；二是美国政府体制存在掣肘。

（一）美国网络基础设施运营存在诸多问题

1. 网络基础设施漏洞多

随着信息技术的飞速发展，网络基础设施的开放化、高可用性是不可避免的趋势。然而这对美国的信息基础设施也带来了不可估量的问题。^⑨根据美国国际战略研究中心的研究，目前美国的网络基础设施依然存在诸多问题，并坚持认为这让中国等其他国家获取了大量的机会，能及时掌握美国最新专利技术。研究表明美国内部在网络方面也存在很多问题。例如职责不明，将部门自身问题归结为网络基础设施问题等。这涉及到美国各部门之间的利益冲突。^⑩

^⑧ The Department of Defense, Cyber Strategy. https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/ (访问时间:2017年6月18日)。

^⑨ Lord M. and Sharp T. America's Cyber Future: Security and Prosperity in the Information Age. Washington, DC: Center for a New American Security, 2011. 1:20-24.

^⑩ Lewis J A, Langevin J R, McCaul M. Securing cyberspace for the 44th presidency. Center for Strategic and International Studies, 2008, 8.

2. 防御速度跟不上网络攻击武器/工具发展速度

一款优秀的网络攻击武器具备向对方发动了攻击而对方依然不自知的特点,网络武器的廉价、隐蔽性、高可用性以及极强的破坏性引起了各方的重视。包含美国在内的诸多国家已经成立了专门的实验室来研究网络攻击武器。^{④①} 由于网络武器的广泛用途和高附加值,各类黑客和开发者前赴后继,且形成了全球性的广泛市场。在一些网络病毒论坛上,以低于100美元的价格就可以买到能造成极大影响的攻击工具。^{④②} 各类攻击者从多样化的病毒获取渠道获益,极大的降低了网络攻击的准入瓶颈。由于缺乏国际约束规则和联合惩罚机制,使得攻击行为和网络攻击工具的泛滥难以控制,从而破坏者和攻击者始终保持着优势的主动权。

3. 僵化、静态和过于谨慎的攻击策略体系

美国国际战略研究中心信息安全专家路易斯用二战时期法国的马奇诺防线来形容现在的美国的网络防御机制,认为目前美国的整体网络防御机制僵化、防御模式静态、反击策略受到的限制太多。^{④③} 当前美国的网络安全模式,依然是触发机制为主。即不出问题,即视为安全。这种模式容易导致作为信息安全的公共部门的懒政,不会主动去进行防御更新。^{④④}

4. 美国社会对网络的物理和心理依赖程度日益增加,受攻击目标越来越多

整个美国社会对网络的依赖程度日益增加,过去十年中,全球新增网民超过20亿。2015年,美国互联网经济在经济总量占比中,从3%增加到了13%。美国军方对互联网的依赖更为明显。^{④⑤} 美国军方由1.5万个子网

④① Hunt C, Chesser N. Deterrence 2.0: Deterring Violent Non-State Actors in Cyberspace. Workshop Proceedings, Arlington, VA: US Strategic Command Global Innovation and Strategy Center. 2008. p.141

④② Political denial-of-service attacks on the rise, Homeland Security News Wire, Mar., 2009. <http://www.homelandsecuritynewswire.com/political-denial-service-attacks-rise> (访问时间:2017年4月20日)。

④③ Lewis J A. Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage. Center for Strategic and International Studies, 2014.p.4.

④④ Kenneth Geers. Strategic cyber security, June 2011. https://ccdcoc.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF (访问时间:2017年6月12日)。

④⑤ US Department of Defense. The DoD Cyber Strategy. Washington, DC: US Government Printing Office, Mar.2015. https://www.defense.gov/Portals/1/features/2015/0415_cyber_strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (访问时间:2017年4月22日)。

络系统和超过 700 万台跨域数百个国家和基地的计算机设备构成,涉及的设施运维、指挥调度、实时情报和远程控制等人员超过 90 万。^{④⑥}美军的数字化系统是他的核心战斗力,也是最致命的弱点。^{④⑦}由此美国各军种都非常重视自身网络加速的安全性,并独立发展自己的网军力量。同样危险的是,人们对网络的心理依赖。网络已经成为了网络生活的组成部分。特别是社交网络,将政治家、高管、各类专业人员和普通民众以多元化、多层次的模式进行了多向连结,这其实是为敌对国家提供了前所未有的开放情报源。

(二) 美国政府体制方面存在掣肘

1. 僵化的官僚体制及人事管理制约网络能力发展

美国官方网络能力发展首要障碍是,在民主体系下庞大的官僚体系,陈旧的数字治理结构以及因此而形成的利益链条,再加上根深蒂固的对维护部门利益的态度,对美国政府网络能力发展构成了顽固的阻碍。政府部门相关网络及数字技术部门的终身公务雇员成了阻碍技术更新的直接障碍。^{④⑧}除了核心位置被不思进取的老雇员占据外,联邦政府体系的薪资待遇、发展机会、自由度也很难吸引年轻有为的技术人员加入。另外,一旦系统出现安全问题,也很难找到责任担当人,因为很少能搞清楚系统问题到底出在什么地方。^{④⑨}

乔治梅森大学杰里米·梅耶副教授在接受我们采访时指出,希拉里·克林顿私自架设邮件服务器的一个重要原因是整个联邦政府的邮件系统非常落后,基本上还是 20 年前的样子。收发邮件极慢,严重影响工作效率,不堪忍受。政府体系的慢节奏与网络安全需要的快速迭代形成了天然

^{④⑥} Lynn W J. Defending a new domain. Foreign Affairs, Sep. 2010. <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain> (访问时间:2017 年 4 月 24 日)。

^{④⑦} Havely J. When states go to cyber-war. BBC News Online, Feb. 2000. <http://news.bbc.co.uk/2/hi/science/nature/642867.stm> (访问时间:2017 年 3 月 24 日)。

^{④⑧} Baker S A, Waterman S, Ivanov G. In the crossfire: Critical infrastructure in the age of cyber war. McAfee, Incorporated, 2009. p.33.

^{④⑨} Timberg, Craig, and Lisa Rein. "Senate cybersecurity report finds agencies often fail to take basic preventive measures." The Washington Post, Feb.2014, https://www.washingtonpost.com/business/technology/senate-cybersecurity-report-finds-agencies-often-fail-to-take-basic-preventive-measures/2014/02/03/493390c2-8ab6-11e3-833c-33098f9e5267_story.html?utm_term=.8a30a662fb82 (访问时间:2017 年 3 月 24 日)。

的矛盾。

美国埃默里大学信息安全学教授林恩公开发表文章批评美国当局在信息安全问题上的官僚主义：“政府官员们都不愿意冒风险去试验新的网络安全模式。如果不出事，甚至不愿意去变动本部门的任何设施及相关管理环节。这使得政府网络系统具有天然的被动性。不出事即不变的传统政府管理模式，与需要应对未来挑战的高灵活性、主动防御的网络安全模式之间存在着较大的冲突。并且，这种体制性问题将长期存在。在今后很长的时间之内，也看不到改变的可能性。”^{⑤0}

2. 决策层官员与技术官僚之间存在沟通断层

美国存在比较普遍的决策层官员不懂网络空间及网络技术领域业务的情况。因为决策层政务官员年龄等问题，对高速发展的网络世界知识有限。^{⑤1}即使是中层领导者，也并不愿意花大量的时间去了解飞速发展的相关技术细节问题。^{⑤2}基础网络的管理者们经常抱怨缺乏好的电脑设备用来研究外来入侵者，同时还面临者各种严苛的条条框框的约束，使得他们难以施展拳脚。^{⑤3}与此同时，一线技术人员和管理决策者之间存在很大的隔阂。这主要体现在网络安全战略制定者们对一线技术人员所面临的各种挑战了解不足，而一线技术人员的声音又无法及时传达到管理层。^{⑤4}这种分裂导致建设性的建议无法及时转换为网络的防御和攻击能力。

国土安全局基础设施保护局的一位官员透露，网络恐怖主义攻击能力急剧增长的重要原因是，极端组织的领导层越来越多精通信息技术和年轻的领导者，他们具备了呆在卧室里就能随时对一国主权和国家重要设施安全造成威胁的能力，虽然美国一直在加大相关打击力度，但由于技术的爆

^{⑤0} Lynn W J. Defending a new domain. Foreign Affairs, Sep. 2010. <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain> (访问时间:2017年4月24日)。

^{⑤1} Kenneth Geers. Strategic cyber security, June 2011. https://ccdcoc.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF (访问时间:2017年6月12日)。

^{⑤2} Carl Hunt, Chesser N. Deterrence 2.0: Deterring Violent Non-State Actors in Cyberspace. Workshop Proceedings, Arlington, VA: US Strategic Command Global Innovation and Strategy Center. 2008. p.18.

^{⑤3} Nathan Thornburgh. The invasion of the Chinese cyberspies. Time, Aug. 2005. <http://content.time.com/time/magazine/article/0,9171,1098961,00.html> (访问时间:2017年7月12日)。

^{⑤4} Colin Gray. Making Strategic Sense of Cyber Power: Why The Sky is Not Falling, April 2013. <https://ssi.armywarcollege.edu/pdffiles/PUB1147.pdf> (访问时间:2017年5月12日)。

炸性发展, 依然难以做到及时制止和有效预防。^⑤

3. 政府与民营公司合作存在诸多问题

为加强美国整体的网络安全能力, 政府需要与民营公司合作。但从公开的信息看, 政府与民营公司合作也存在诸多方面的问题: 一方面政府层面对民营公司的不信任。政府方面认为与民营公司共享网络安全信息会导致机密泄露;^⑥ 另一方面私营公司也不愿意与政府进行公开的过多合作。因为这会暴露公司自身存在的弱点, 也会影响公司自身的独立形象。美国网络安全联盟协会主席莱里·克林顿指出, 如果要求公司公开他们公司的网络安全状况, 会让公司感觉自己因为安全问题而被点名了。^⑦ 而且, 公司也会担心政府部门滥用自己的数据。这种政府与私营公司相互不信任的状况导致了美国网络安全防御方面的分裂。根据2011年的一项调查, 73%的美国公司有被黑的经历, 而且88%的公司在咖啡上的花费超过了他们在网络安全方面的投入。^⑧

针对美国公私部门在信息安全领域合作的问题, 2012年奥巴马政府当局曾提交了一个议案, 要求允许私营公司可以共享国家网络安全核心数据信息, 并允许私营公司为国家核心基础设施提供网络安全保护。但该议案在2014年正式被国会否决, 否决原因是无法防止俄罗斯渗透。^⑨ 但我们通过调研发现, 2016年以来美国就如何就网络安全相关领域与民营公司开展合作有了新的动向, 相关情况有待进一步研究。

^⑤ Nando Times. U.S. Official Warns of Future Attacks on Vital Computer Systems, Nov. 2001. <http://www.nando.net/technology/story/172635p-1669909c.html> (访问时间: 2017年5月2日, 此链接需通过 archive.org 打开)。

^⑥ Thomas Rid. Cyberwar and Peace: Hacking can reduce real-world violence. Foreign Affairs. Nov. 2013. <https://www.foreignaffairs.com/articles/2013-10-15/cyberwar-and-peace> (访问时间: 2017年6月12日)。

^⑦ Amitai Etzioni. Cybersecurity in the private sector. In Science and Technology, Fall 2011. <http://issues.org/28-1/etzioni-2/> (访问时间: 2017年5月3日)。

^⑧ HelpNet Security, 73% of Organizations Hacked, Feb. 2011. <https://www.helpnetsecurity.com/2011/02/08/73-of-organizations-hacked-in-the-last-2-years/> (访问时间: 2017年4月26日)。

^⑨ Homeland Security News Wire “Russia may launch crippling cyberattacks on U.S. in retaliation for Ukraine sanctions”, May 2014, <http://www.homelandsecuritynewswire.com/dr20140502-russia-may-launch-crippling-cyberattacks-on-u-s-in-retaliation-for-ukraine-sanctions> (访问时间: 2017年5月26日)。

五、结语

网络安全问题是全民问题，赢在技术、赢在变化。经过在美国为期7个月的调研，我们对美国网络安全战略的变化调整进行了分析研究，发现随着网络冲突的不断加剧，美国的网络安全战略事实上已经远超过了网络安全防御的局限性，网络安全战略作为中美博弈的一环，随着美国对华战略的调整而在不断变化。在战略上已转向攻击为主，并进行了对华网络攻击的重要部署。美国方面认为未来十年的网络安全问题的首要挑战将来自中国和俄罗斯，并将视中国为主要对手。在攻击模式上开始由原来的“硬入侵”向“软入侵”转变。其中病毒工具的开发上升到了战略武器的地位，并将进一步重视社交网络的网络价值。同时，美国在网络安全方面高度重视反介入/区域拒止（A2/AD）战略。在组织架构上，逐步将网络防御和网络作战分离，并强化了网络安全相关部门联合作战的能力。我们同时也注意到，最近五年来美国在网络安全战略方面有一些重要的部署，例如加强与印度、日本等地区的网络安全合作，加强区域性、针对性监控，建立网络安全问题联动机制，建立主动抑制潜在网络威胁体系等。但另一方面，我们发现美国在网络安全方面也存在自身基础设施运营和政府体制方面的问题。

值得注意的是，2016年开始，美、日、澳等国开始推动网络安全三边合作，并且美印网络安全合作也在不断加强。此类网络安全国际合作对中国的影响有待进一步研究。与此同时，美国政府与民营公司之间就网络安全相关事项的合作模式存在较大的转变，了解美国政府与民营公司网络安全问题合作模式和合作关系，对及时把握美国网络安全战略动态变化有着重要意义，需要进一步细化跟踪。

Research on the Trends of U.S. Cyber Security Strategy

Shi Peipei, Liu Yushu

Abstract: According to the survey in the U.S., it is found that the U.S. authority believes that China and Russia will become the main challenges in the situation of cybersecurity. And the U.S. will take China as the main competitor in the field of cybersecurity. It is also found that the U.S. cybersecurity strategies have changed immensely, from “hard attack” to “soft attack”. The computer virus attacking tools have been employed as strategic weapons, and the social network is increasingly becoming important. Besides, the U.S. authorities pay much attention to the utilization of cyber A2/AD strategy, and display great efforts on the joint operation efficiency of multi-departments. Meanwhile, they have strengthened the cybersecurity cooperation in the Asia-Pacific region. But, the issue of public information infrastructure management and the limitation of government bureaucracy institutions have become obstacles to the U.S. cybersecurity. The further research will need to pay due attention to the U.S. international cybersecurity cooperation and the cooperation in public-private agencies.

Key words: cyber security; cyber space; cyber virus

About the Authors: Shi Peipei, Institute of American Studies, CASS; Liu Yushu, Georgia Institute of Technology, the United States of America.

British Intervention in Hong Kong Affairs and Its Impact on the Sino-British Relations

Chen Hanxi, Liu Shiqi

Abstract: This article is to explore the objectives and policy instruments of the British policy towards Hong Kong, and the impact of this policy on the Sino-British relations. Since 1997, the political goal of UK has been supporting the democratization process in Hong Kong. In recent years, the UK has adopted certain approaches to intervene in Hong Kong's political affairs such as human rights, local general elections, and the so-called “Central occupation movement”, which has brought some negative impact on the Sino-British relations. As to the issue of “Hong Kong independence”, the UK has tried to take the same stance with