B.17
美国对华网络安全战略走向分析

石培培*

摘　要： 随着网络空间在国家安全战略层面地位的提升，网络攻击背后的国家力量日趋明显，网络安全战略是美国国家安全战略的重要组成部分，随着中美两国在网络信息技术领域的互动交流越发频繁，美国对华网络安全战略也在不断地调整：由战略防御向战略攻击转变；在攻击模式上开始由原来的“硬入侵”向“软入侵”转变；进一步重视社交网络的战略价值；在组织架构上，强化了网络安全相关部门联合作战的能力。

关键词： 网络安全战略　网络攻击　社交网络

网络安全战略是美国国家安全战略的重要组成部分，受到美国政府的重视，2017 年深受“通俄门”困扰的美国总统特朗普也不例外，大选过程跌宕起伏，从竞选初期至今，关于俄罗斯网络干预美国总统大选的争论持续不断。12 月，《美国国家安全战略报告》进一步强调了美国政府将根据安全需要对网络攻击方采取行动，公开将中国作为网络安全战略性防御对象。

随着中美网络技术信息不断发展与互动，两国网络安全问题，尤其是涉及国防军事、专利技术等网络信息问题的各种争论和指责不断增多，美国对华网络安全战略也在不断调整变化。

* 石培培，中国社会科学院美国研究所研究人员，主要研究领域为美国政治。

一　网络安全问题历史背景

早期的网络安全冲突主要表现形式是人为更改设备控制系统，从而对工业或者对军事基础设施造成物理性破坏。而后网络病毒的出现使得网络技术成为攻击武器，不受物理设备和地理边界的限制，带来更大威慑力和破坏性。业界公认的第一个专门攻击物理世界基础设施的蠕虫病毒是震网病毒。震网病毒是首个针对工业控制系统的蠕虫病毒，[①] 它无需通过互联网就可以实现感染传播，具备极强的复制和传播能力，一旦病毒确认感染，对目标设备的损坏是不可逆的。基于网络病毒强大的破坏性和威慑力，美国政府将网络病毒提升至网络安全战略武器的地位，这将对未来国家间战略模式产生巨大的冲击和影响。

网络安全冲突模式也渐渐地由人为更改设备系统的模式转为以远程操控的攻击模式为主。历史上首次国家间网络攻击案例发生在 1982 年，美国通过远程操作改变管理天然气输送管道的计算机软件程序，对苏联实施网络安全攻击，直接导致苏联国内的天然气管道爆炸。[②] 1997 年，美国在五角大楼进行了首次国家网络安全实战演习，通过演习发现利用互联网上公开的网络信息技术和软件，就可以对国内的工业基础设施和信息系统实施有效的网络攻击。[③] 之后美国网络安全工作的重心也逐渐开始从军事攻击转向注重国内基础设施战略防御建设，以避免高度依赖网络信息技术的发展趋势而遭受数字化“珍珠港偷袭式”的网络攻击。庞大的数据资源逐渐成为经济和政治资源的重要组成部分，各国对网络安全问题的关注焦点也由如何进行网络攻

① 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.

② 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.

③ Steven Hildreth, “Cyber Warfare,” CRS Report for Congress, Jun. 2001, https://fas.org/irp/crs/RL30735.pdf.

击转向对数据信息资源加强控制。同年美国正式界定了网络空间的概念,[①]正式将网络空间信息资源与国家领土、领空资源列为同等重要的国家资源。

二　网络安全战略由防御转向攻击

虽然近年来美国民主和共和两党“极化”严重，对国内外不同议题存在较大争议和分歧，然而不同党派在对待国家网络安全战略上的态度都保持了较高的一致性，始终将国家安全利益放在首位。2017 年上任的总统特朗普多次强调要废除包括医保在内的多项奥巴马任期的法律、行政令等，但在国家网络安全方面，特朗普政府对奥巴马任期的网络安全战略有所继承和发展。特朗普在竞选初期便多次表示美国在应对网络威胁方面远远做得不够，强调网络安全的重要性。

特朗普承诺将会把网络安全作为国家安全第一重要的议题，并要大力加强美国网络防御和攻击能力。2017 年 1 月 28 日，白宫发布了《2 号国家安全总统备忘录》（National Security Presidential Memorandum－2），就国家安全委员会、国土安全委员会成员组成、议事程序、组织框架等内容重新进行了调整。2 月在公布的内阁成员名单里，特朗普将国家情报局局长和中央情报局局长列在其中。[②] 5 月，就网络安全问题签署了 13800 号行政令，强调从增强联邦政府计算机网络安全、加大信息基础设施建设以及制定空间行为规范三个方面加强美国网络安全建设[③]。在行政令签署后的白宫新闻发布会上，负责网络安全事务的国土安全顾问汤姆·博塞特（Tom Bossert）表示将以 13800 号行政令为蓝本，从强化计算机信息安全、基础设施和网络行为规

① “The National Strategy to Secure Cyberspace,” Feb. 2003, https://www.us－cert.gov/sites/default/files/publications/cyberspace_ strategy.pdf.

② “President Donald J. Trump Announces His Cabinet,” https://www.whitehouse.gov/presidential－actions/president－donald－j－trump－announces－cabinet/.

③ Executive Order 13800 of May 11, 2017, “Strengthening the Cyber Security of Federal Networks and Critical Infrastructure,” https://www.gpo.gov/fdsys/pkg/FR－2017－05－16/pdf/2017－10004.pdf.

范三个方面制定美国新的网络安全战略，同时还强调美国受到俄罗斯、中国、伊朗等国家的网络攻击，美国不能允许此类事件再次发生。[①] 9 月 30 日，特朗普宣布 2017 年 10 月为国家网络安全意识月（NCSAM），号召全民重视网络安全。

特朗普当选总统后很快组建了网络安全团队。任命纽约前市长鲁迪·朱利安尼（Rudy Giuliani）作为网络安全顾问，专门解决信息安全问题；原先在通用汽车公司担任财务总监的克里斯·里德尔（Chris Liddell）作为美国创新办公室工作核心成员，主要负责联邦政府计算机信息现代化；[②] 里德·科迪什（Reed Cordish）任政府技术计划项目的总统助理，同时也是创新办公室核心成员之一。10 月，特朗普提名柯尔斯顿·尼尔森（Kirstjen Nielsen）任国土安全部长，柯尔斯顿成为美国第六位国土安全部部长，也是特朗普上台以来第三位国土安全部部长。柯尔斯顿擅长网络安全事务、紧急事件处理，她在参议院听证会上曾表示将会把网络安全战略视为国家安全战略的重中之重。[③] 从网络安全团队组成来看，团队核心成员大多为商业背景出身，缺乏政治经验。这从客观上也反映了特朗普政府重视私营部门在网络安全工作中的重要性，而重视政府与私营部门的合作也是奥巴马总统政府网络安全工作的重点之一。

2017 年《美国国家安全战略报告》中指出："美国是互联网的发源地，它应该反映美国的价值观，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，"如何面对网络信息时代所面临的挑战和机遇，将决定美国未来的繁荣和安全。历史上，我们

① "Press Briefing by Principal Deputy Press Secretary Sarah Sanders and Homeland Security Advisor Tom Bosser," May 11, 2017, https://www.whitehouse.gov/briefings-statements/press-briefing-principal-deputy-press-secretary-sarah-sanders-homeland-security-advisor-tom-bossert-051117/.

② "What Jared's Office Actually Does," *The Agenda*, July 2017, https://www.politico.com/agenda/story/2017/07/01/jared-kushner-office-american-innovation-000470.

③ "Senate Confirms Kirstjen Nielsen to Head Homeland Security," CBS, December 5, 2015, https://www.cbsnews.com/news/senate-confirms-kirstjen-nielsen-to-head-homeland-security/.

通过掌控领土、领空、太空和海域来保护美国国土安全。当今，网络空间给其他国家以及组织在不跨越边界的情形下，提供了危害美国政治、经济和安全利益的可乘之机，低成本且难以确认攻击者的网络攻击手段却足以对美国关键的基础设施、企业造成严重性破坏，破坏美国军事、金融、电网和通讯等设施，削弱联邦政府的网络建设能力、给美国人民日常生活带来巨大的安全威胁”。[①] 报告指出美国受到的网络恶意破坏主要是一些国家或其他组织通过敲诈、散布虚假信息实施网络攻击，这种攻击行为严重损害美国民主国家的信仰和信心，很多国家利用网络作为扩大专制统治影响的工具。报告将中国和俄罗斯、伊朗与朝鲜以及恐怖主义视为威胁美国国家利益、挑战美国在世界影响力的主要对象。

美国网络安全战略的发展也经历了由被动防御到积极进攻的演变过程：克林顿总统政府时期重视网络防御内以基础设施保护为主的信息安全战略，小布什总统时期采取网络攻防结合战略，奥巴马总统时期则是全球网络威慑战略，并在组织管理体系、法律法规体系、技术体系和执行体系四个方面形成了全民的综合保障系统。[②] 2003 年，在《美国国家网络空间安全战略》报告中第一次对“网络空间”（cyberspace）的概念进行了界定。[③] 2005 年在《美国国防战略报告》中，美国明确将网络空间提升到国际公共领域的高度，将其列为与陆海空及太空同等重要的五大公域的范畴之一。[④] 2009 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。[⑤] 2013 年美国国家情报局主任詹姆斯·克拉柏（James Clapper）公开声明网络威胁是美国国家安全的第一

① “National Security Strategy,” Dec. 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

② 程群：《美国网络安全战略分析》，《太平洋学报》2010 年第 7 期。

③ The National Strategy to Secure Cyberspace, Feb. 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

④ The National Defense Strategy of the United States of America, March 2005, p. 13.

⑤ 李恒阳：《美国网络军事战略探析》，《国际政治研究》2015 年第 1 期。

威胁。[①] 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[②]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，该报告首次提出要提升网络作战的战术攻击能力，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。美国经济顾问委员会在2018年2月发布的《恶意网络攻击对美国经济的损害》报告中估算，2016年美国受到的网络黑客攻击直接导致了570亿至1090亿美元的经济损失。[③]

美国方面认为随着中国网络技术水平不断提升，其网络攻击能力会对美国政治、经济、军事等领域造成严重危害。近年来，美国在网络安全领域对中国的舆论指责也在不断加大。美国公开以国家安全为由限制中国互联网通讯企业进入美国电信市场，近年来，以华为、中兴为代表的中国通信公司在美国电信市场上屡屡受挫，受到百般阻挠。2018年2月13日参议院情报委员会听证会上，包括CIA、FBI、NSA等在内的六家美国情报部门的负责人表示不信任华为及中兴公司的通信产品，同时呼吁美国民众不要购买来自中国公司的产品，美国企业不要与中国华为、中兴公司合作，指责华为、中兴对美国通信网络市场造成干扰。[④] 除此之外，美国方面不断编造各项罪名将其国内网络安全诱因转嫁给中国。近几年不断制造“F35战机资料失窃”、各类大型公司核心技术失窃等噱头，以莫须有的罪名直指中国政府。2013年《纽约时报》刊发文章公开指责中国“61398部队”对美国国家安全构

① James R. Clapper, “Statement for the Record Worldwide Threat Assessment of the U.S. Intelligence Community, Senate Select Committee on Intelligence,” February 9, 2016, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.

② 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。

③ “The Cost of Malicious Cyber Activity to the U.S. Economy,” The Council of Economic Advisers, Feb. 2018, https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

④ “Six Top US Intelligence Chiefs Caution Against Buying Huawei Phones,” CNBC news, Feb. 13, 2018, https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html.

成直接威胁。2014 年 5 月 19 日，美国司法部起诉五名中国军官通过网络窃密。2016 年，美国国防部在向国会提交的报告中指出“中国已经具备了对美国基础设施以及核心部门实施系统网络攻击的能力”。[①] 同时，美国各类智库以及利益相关公司不遗余力地对国会与联邦政府就网络安全问题争取经费和政策支持的游说活动，加大研究力度。

三　由硬入侵转向软入侵的攻击模式

在美国国际战略研究中心（CSIS）主办的“2017 年网络冲突研讨会”（Cyber Disrupt 2017）[②] 上，奥巴马总统时期的国防部官员詹姆斯·米勒（James Miller）表示，2017 年及未来，美国军方的关注重点会是对中国战区及军改后新调整部署的网军实际战力进行评估，强调对中国军方通讯及指挥自动化攻击的重要战略价值。[③] 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、通信、计算机与情报集成信息指挥系统）的快速反应能力、数据共享及决策等方面的实战能力高度关注。[④]

随着计算机信息技术的进步，通过网络技术实施攻击变得越来越普遍，网络攻击的形式也随着技术的不断更新而变化。美国国防部认为，网络攻击的对象不仅可以针对已经上线和开始运营的系统，在系统的开发、测试、运

① 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.

② CSIS, “Cyber Disrupt 2017,” Mar. 2017, https://www.csis.org/events/cyber-disrupt-2017.

③ 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/.

④ 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.

营、更新等每个不同阶段都具备可攻击的战略价值。[①] 同时，网络攻击方式是多样化的，可以是通过破坏设备干扰信息服务，也可以通过远程入侵操作，还可以是通过目标系统内部人员进行内部程序的破坏。

总的来说，网络攻击方式主要有两类：一类是“硬入侵”，另一类是“软入侵”。硬入侵是针对国家，如基础设施、网络底层设备以及重要工业建设等硬实力的破坏，会对攻击目标国造成重大的经济损失、导致社会服务系统瘫痪等。软入侵是相对于硬入侵的物理性攻击而言的，主要指的是针对国家的文化、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。就近年来美国的网络攻击行为来看，美国对华实施的网络攻击主要有两种入侵类型：一类是以同遏制军队战斗力相关的基础设施等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。

在对军队战斗力的硬入侵方面，美国认为中国军方使用的信息和通信技术越多，对网络信息技术越依赖，面对网络攻击时就越脆弱。[②] 中国军方之前主要依靠的是物理隔离的地下和海底光缆和设施，整体环境是由本土的路由服务器所构成的，而这种相对绝缘的趋势正在不可避免地被全球网络技术信息化的发展所打破；2015 年中国提出“打赢信息化局部战争”的战略，加速了“网络国界和国防线”的建设，也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。[③]

美国方面认为，如果只考虑对中国军方进行网络硬入侵攻击模式，即使遭受网络攻击重创，中国军方也能在强大领导体系下迅速恢复。所以，针对中国政府领导力和意识形态体系的网络软入侵攻击比对军方的网络硬入侵攻击更有战略价值。美国信息安全专家马丁·利比克（Martin Libicki）表示，

---

① Defense Science Board, “Task Force on Cyber Supply Chain,” Nov. 2016, https://www.hsdl.org/?abstract&did=799509.

② 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.

③ 同上。

中国高度统一的政治体系本身就是具有高价值的战略攻击目标。中国经济增长出现波动的时候，就可以将其看作对中国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。[①] 他认为，经济波动影响社会就业问题，通过网络信息传播对中国的年轻人进行网络意识形态渗透，攻击成本较低，但其战略意义甚至大于与军方直接进行网络对抗的意义。据材料分析，美国对中国政府领导力和意识形态系统的网络软入侵主要从三个方面入手：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，通过网络信息的传播进行意识形态的渗透；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。[②]

四　社交网络是网络安全系统的重心

近期，美国媒体称英国剑桥数据分析公司（Cambridge Analytica）利用社交网络平台 Facebook 上的 5000 万用户数据来分析选民心理，从而影响他们在 2016 美国总统竞选中的投票选择。[③] 根据剑桥公司的前员工克里斯托弗·威利（Christopher Wylie）的爆料，2014 年剑桥公司投资一个项目，即通过对 Facebook 用户进行在线心理测试对其进行性格分析以了解选民心理，之后根据分析结果，通过 Facebook 和电子邮件发放不同的政治竞选广告，从而影响其投票行为。特朗普前首席战略顾问史蒂夫·班农（Steve Bannon）当时任剑桥公司董事，负责这个项目的执行和策划。克里斯托弗

① Libicki M. Pulling Punches in Cyberspace, in Proceedings of a Workshop on Deterring Cyberattacks, 2010, pp. 123 – 47.

② D. Sanger, "U. S. 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.

③ Mark Thompson and Brian Stelter, "Facebook's data crisis deepens as questions mount," *CNNtech news*, March 20, 2018, http://money.cnn.com/2018/03/20/technology/facebook – data – scandal – deepens/index.html.

称，2014 年通过对 Facebook 用户数据分析，他们得出美国保守白人选民中有很高的民粹主义情绪。他认为当时这些数据的分析结论被班农后来用于帮助特朗普竞选，成为特朗普成功当选的关键因素。①

从 2011 年突尼斯的“茉莉花革命”到 2013 年美国波士顿马拉松恐怖袭击案件，社交网络在对外网络攻击、信息情报、对内反恐及政治选举等领域发挥了重要的作用，各国政府对社交网络的战略价值也越来越重视。利用社交网络影响政治选举的一个比较典型的例子是 2009 年发生在南非的利用社交网络影响政治选举的结果。② 当背后操纵者通过社交网络数据统计发现一个地区的民众倾向于投票给其他候选人时，操纵者就会在该地区制造食物短缺的情况。同时，操纵者会进一步剥夺选民的工作机会，从而将工作机会转让给那些支持他们的人。根据当地媒体的报道，在同时缺乏食物和工作的形势下，原来投票给其他候选人的选民很快就妥协从而改变投票，而这个改变投票意愿的过程周期并不是很长。

美国政府当局越来越重视社交网络的安全战略价值。美国国防部下属的国防高级研究项目局信息技术创新办公室主任约翰·劳恩贝瑞（John Launchbury）指出，震网病毒传播的关键，主要是通过以色列在伊朗的社交关系网络渠道。③ 美国乔治城大学教授罗伯特·曼德尔（Robert Mandel）表示：“人具有天生的不稳定性，作为社交网络的主体，人是安全系统中最脆弱的联系因素。社交网络的推广和使用，特别是在线上与线下生活逐步融合的情况下，在情报搜集、网络安全方面发挥着越来越核心的作用”④。按照罗伯特教授的观点，在信息安全系统和网络攻击中，社交网络中的主体的脆

① “Christopher Wylie：The Whistleblower in the Cambridge Analytical Scandal，” *The Straits Times*，March 20，2018，http：//www. straitstimes. com/world/united - states/christopher - wylie - the - whistleblower - in - the - cambridge - analytica - scandal.

② “South Africa：Food Used as Election Weapon，” *Say Monitors*，Apr. 2009，https：//www. social - engineer. org/wiki/archives/Governments/Governments - FoodElectionWeapon. html.

③ CSIS，“Cyber Disrupt 2017，” Mar. 2017，https：//www. csis. org/events/cyber - disrupt - 2017.

④ *Optimizing Cyber Deterrence*：*A Comprehensive Strategy for Preventing Foreign Cyberattacks*，Georgetown University Press，2017.

弱性主要体现在以下几个方面。

一是再安全的信息系统也需要特定使用者，而使用主体的不稳定性也就无法保证安全的可靠性。例如，公共无线网络环境下办公通信设备与手机网络的链接、信息存储设备的不规范使用以及电脑使用中的不规范操作等都可能导致网络病毒的释放或者木马的侵染。尤其是在熟悉攻击对象社交网络的情况下，攻击者很容易确认并攻击对方所在工作网络的目标。

二是特权使用者带来潜在的网络安全风险问题。在一个组织体系信息系统里往往使用特权越大的主体，其自身所带来的系统性风险也会越大。在实际的保密组织体系中，为了确保信息的安全和可控性，只有少部分人掌握核心信息。所以对于核心信息的网络攻击，关键是找到掌握信息的那少部分人，而随着技术的更新和社交网络广泛的使用，攻击者能够实现精准定位找到目标主体。

信息系统主要有安全性、可用性和功能性这三个基本要素。而这三个要素相互矛盾，如果强调信息的安全性，那么其功能性和可用性就会受到影响，反之亦然。美国外交关系委员会研究员亚当·塞格尔（Adam Segal）表示随着中国信息化技术的发展和更新，其信息系统漏洞和弱点也就越大，对中国的网络攻击的战略意义也就会越加明显。[①]

五　多部门联合作战的组织架构

美国网军司令部是第一个国家层面的统一指挥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，2017 年 8 月，特朗普总统宣布为提升美国网络行动力，将网军司令部升级，[②] 升级后的网军司令部将与美

① A. Segal，“U. S. Offensive Cyber Operations in a China-US Military Confrontation，” June 2016，https：//papers. ssrn. com/sol3/papers. cfm? abstract_ id = 2836203.

② “Statement by President Donald J. Trump on the Elevation of Cyber Command，” https：//www. whitehouse. gov/briefings - statements/statement - president - donald - j - trump - elevation - cyber - command/.

国中央司令部、战略司令部等主要作战司令部并列，成为美军第十个联合作战司令部。[①] 特朗普称网络司令部的升级展示了美国抵御网络威胁的决心以及坚定了网络安全盟友和美国一起对抗网络攻击的信心。

迈克尔·海登（Michael Hayden）曾任克林顿总统时期、小布什总统时期的国家安全局局长，后任中央情报局局长，他在接受媒体采访时表示，2010 年震网病毒攻击爆发后，美国政府有些部门其实也遭到了误伤，这也反映了在对外网络作战中，美国内部各政府部门之间存在无法相互协调配合的问题。为了避免同样问题的发生，2010 年 10 月 1 日，美国成立了网军司令部。[②] 美国网军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，形成了美国网络安全作战的整体力量。[③] 网军司令部核心任务是协调各部门进行立体式网络防御与网络攻击，整合资源，对网络空间上的攻击破坏者进行精准有效的防御和攻击。网军司令部与美国国家安全局都在马里兰州的米德堡。该司令部的下属机构（见图 1）涵盖网络作战的各个方面。

从整体的结构来看，美国网络安全冲突组织架构由作战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指挥，战斗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。

美国国防部战斗支援局下面有九个职能部门，其中涉及网络安全冲突问题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），隶属于战斗支援局（见图 2），主要工作职能是为白宫、军方及联

---

① 但根据美国国防部相关网页的官方说明及材料，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 - uscybercom/。

② “General Michael Hayden Discusses the Stuxnet Virus on 60 Minutes，” https：//www. youtube. com/watch？ v = 8HK3XPXBbNk， https：//www. youtube. com/watch？ v = 0FEr 0DFwvcY.

③ “The Relationship of U. S. Army Cyber Command and Second Army，” http：//www. arcyber. army. mil/Pages/History. aspx.

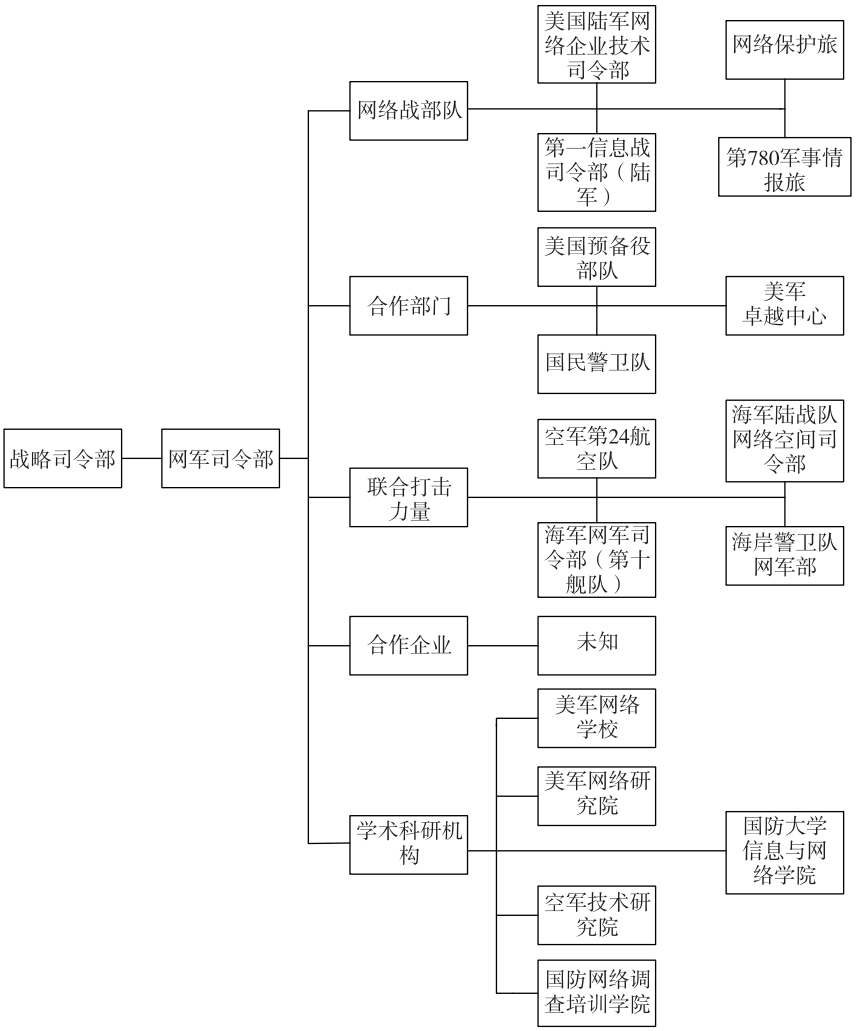

图 1　美国网军司令部组织架构

资料来源：根据美国国防部、网军司令部资料绘制。Defense Agencies and DoD Field Activities，http：//dcmo. defense. gov/Portals/47/Documents/OSD% 20DAFA% 20Organization. pdf，https：//www. defense. gov/About/Military - Departments/Unified - Combatant - Commands/，https：//www. nsa. gov/about/，http：//www. arcyber. army. mil/Organization/About - Army - Cyber/。

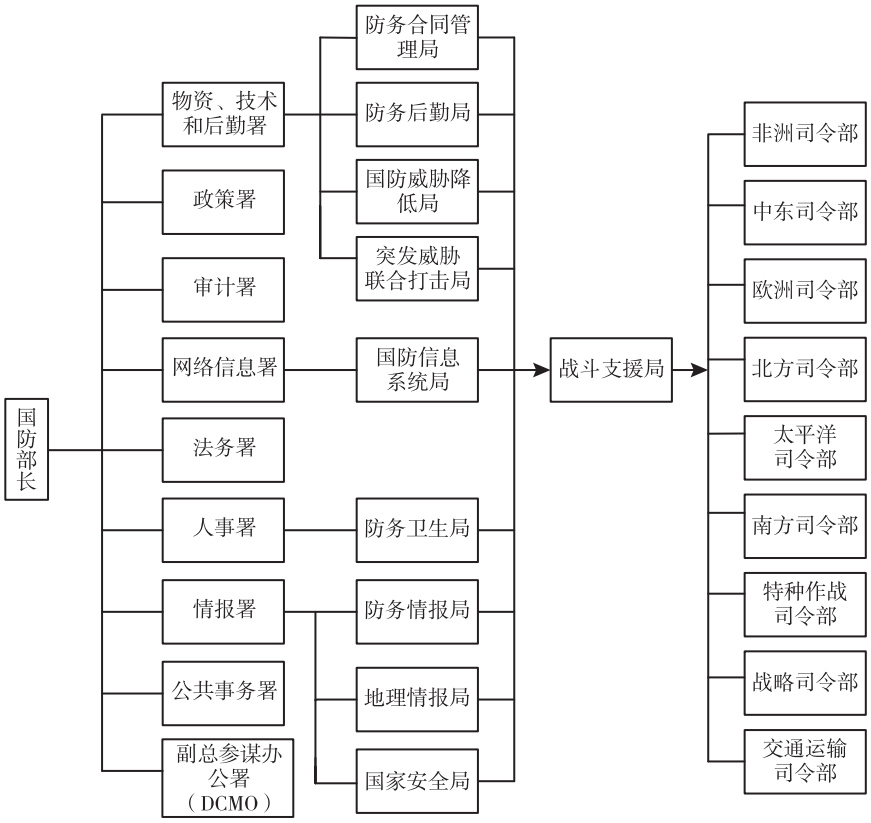

图 2　美国网络安全支援体系组织架构

合作战司令部提供信息技术支持。该局前身是 1960 年成立的美国国防通讯局，主要工作集中在硬件通讯的基础设施的整合方面，1991 年更名为国防信息系统局。该部分的核心任务是确保作战指挥与控制系统的稳定运行。该局通过三个部门分工配合实施信息作战：国防频谱管理部（DSO），负责通讯频谱管理；战区网络作战中心，负责各个安全中心、网络攻击部队、通信卫星支持等信息的有效整合；国防部信息网络联合部队总部（JFHQ-DODIN），履行指挥职责。美国国家安全局，是全球雇佣最多数学专业人才和电脑技术专家的机构，具有自己独立的芯片工厂和研究基地，对包括电台

广播、互联网，尤其是军事和外交的秘密通信进行监听。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），与私营研究机构、设备生产商保持着广泛的联系。①

从图 1 和图 2 的美国网络安全作战和支援体系组织架构可以看出，负责网络安全的战斗支援局和网军司令部都是横向组织结构。它们所辖的职能局和作战部队在纵向上都隶属于其他相关职能部门，受到上级不同职能单位的垂直领导，同时也接受战斗支援局和网军司令部的横向指挥。这种以作战为导向的双重领导体系，能够有效突破各部门单位之间的隔阂，迅速形成高效战斗力。这种架构设计对要求快速反应和长期保持信息高度共享的网络作战来说，是非常有效的。

奥巴马政府任期建立网军司令部，联邦调查局牵头负责网络安全事件的调查。在此基础上，特朗普政府进一步强调联邦政府各部门、政府与私营企业在网络安全事务上的协调和合作，强调各内阁部长和部门领导对本部门的网络安全负责，美国军队应该具备威慑能力、具备超强的网络攻击还击能力。

结　语

随着网络信息的快速发展和中国国际影响力的提升，中美两国在网络信息领域的互动交流增多，两国之间的网络安全冲突也越来越频繁。当前，美国一方面通过技术创新不断增强网络攻防能力，另一方面强化同盟合作关系进一步巩固在网络空间的优势地位。

近年来，美国对中国网络方面的指责有不断增加的趋势，甚至在国际媒体中只能听到一边倒的美国对中国网络问题的攻击和指责。美国充分利用网络话语权，营造中国网络威胁论，在国际上发起对华围攻，借此降低在全球网络空间维持主控权的成本。建议中国加强与美国相对应的针对网络攻击问

① NSA. gov. , https：//www. nsa. gov/about/faqs/.

题的外宣和外交特别应对机制，把握国际舆论的主动权。

美日两国2016年召开网络合作会议，双方达成了网络安全战略合作意向[①]。会议主题为网络安全合作，重点在于如何对中国开展联合防御行动。双方安全战略合作主要包括途经日本的海底网络光缆管理、网络安全互信和联防及下一代网络技术开发等内容。需要注意的是，会议还达成美国、日本和澳大利亚三国建立网络安全合作关系的共识。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战略，在战术上对我国形成了信息情报上的合围，直接影响未来中美两国的网络竞争形势。

随着网络空间在国家安全战略层面地位的提升，网络攻击背后的国家力量日趋明显，国家主权除了传统意义上对领土、领空及领海主权等的控制之外，世界各国对网络空间主权的争夺也日益激烈。而网络空间主权又不同于其他主权，网络安全在技术上打破传统资源规则的限制，国家间网络空间主权的争夺取决于各国网络空间技术的更新程度。网络空间主权的界定取决于网络技术识别。因此落实网络空间主权的技术标准，是维护我国网络空间主权的重要落脚点，建议开展网络空间主权技术相关问题的工作，进一步细化我国网络空间主权的技术标准。

（审读：李恒阳）

① Scott W. Harold, Martin C. Libicki, Motohiro Tsuchiya, Yurie Ito, Roger Cliff, Ken Jimbo, Yuki Tatsumi, "US-Japan Alliance Conference: Strengthening Strategic Cooperation," 2016, https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF351/RAND_CF351.pdf.