第 2 卷◆第 4 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

美国网络空间建设历程与特点分析

吕忠泽　刘凌旗
中国电子科技集团有限公司发展战略研究中心
中国电子科技集团有限公司电子科学研究院
中电科发展规划研究院有限公司
DOI:10.12238/acair.v2i4.10361

[摘　要] 通过梳理总结美国网络安全战略的演变历程和网络空间力量建设与编成,对其在网络空间领域的战略规划、组织构建和国际合作等方面进行特点分析。
[关键词] 网络空间；建设；特点
中图分类号：F282　文献标识码：A

Analysis of the history and characteristics of cyberspace construction in United States

Zhongze Lv　Lingqi Liu
Development Strategy Research Center of CHINA ELECTRONICS TECHNOLOGY GROUP CORPORATION
China Academy of Electronics and Information Technology
CETC Development Planning and Research Institute Co., Ltd.

[Abstract] This paper traces the evolution of U.S. cybersecurity strategy and the examining the development of cyber forces,then identifys the key features of its strategic planning, organizational structure, and international cooperation in the cyberspace domain.
[Key words] cyberspace; Construction; peculiarity

引言

随着信息技术的迅猛发展,网络空间已成为国家安全与利益的关键领域之一。美国作为全球信息技术的领导者,在网络安全战略与力量建设方面积累了丰富的经验。从2003年小布什政府时期首次将网络安全战略正式化以来,美国的网络安全战略经历了从防御到威慑的演变,这一历程反映了美国对网络安全威胁认知的变化以及其对维护其网络空间主导地位的决心。

1 美国网络安全战略演变与现状

美国的网络安全战略经历了从防御到威慑的演变,这一历程反映了美国对网络安全威胁的认知变化以及对维护其网络空间主导地位的决心。从小布什政府时期至今,美国的网络安全战略逐步成熟,成为一个涵盖战略规划、组织构建、技术开发、国际合作以及法律规制等多个维度的综合体系。

1.1小布什政府时期。小布什政府首次将网络安全战略正式化,并确立了初步框架,主要聚焦于本土网络防御。2003年,《网络空间安全国家战略》报告的发布标志着美国正式确认网络安全政策的独立地位。该报告设定了三个战略目标：防范针对美国关键基础设施的网络攻击、降低国家面对网络攻击时的脆弱性、最大限度地减少网络攻击造成的损害和缩短恢复时间[1]。此外,报告还提出了五项优先计划,旨在增强美国本土的网络防御能力。

2006年,小布什政府发布的《网络空间作战的国家军事战略》首次将网络空间视为与陆、海、空和太空同等重要的作战领域,并明确了在网络空间的主要任务,包括保护美国的网络资产、确保军事行动在网络空间的自由行动以及在必要时对敌对网络活动进行反击[2]。这一战略强调了在和平时期和冲突时期都必须维持网络作战能力,标志着美国军事战略对网络空间重要性的正式认可。

1.2奥巴马政府时期。奥巴马政府时期,网络安全政策逐渐成为美国国家安全的优先事项,并正式引入了网络威慑的理念。2011年,《网络空间国际战略——网络化世界的繁荣、安全和开放》报告的发布标志着美国在全球网络空间治理中的主导地位得到强化[3]。该战略提出了网络威慑的概念,并倾向于实施“惩罚威慑”,对敌对网络行动进行惩罚,同时强调在应对网络威胁时不会以牺牲网络空间的开放性为代价。这是美国首次全面阐述其网络空间国际政策的文件,体现了政府对网络安全威胁认知的转变。

2015年,《网络威慑战略》明确提出将综合性采用拒止和惩罚等手段来实施网络威慑[4]。同年,《美国国防部网络战略》的发布进一步明确了网络威慑的关键地位,提出以惩罚的手段进行威慑,在主要对手对美国发起网络攻击前采取适当权力工具进行威慑,使其意识到对美国进行恶意行动会得不偿失[5]。

1.3特朗普政府时期。特朗普政府时期的网络安全战略更加具有进攻性,侧重于通过网络攻击来削弱主要对手的网络能力,旨在通过积极的网络行动来预防潜在的网络威胁。2018年,特朗普总统签署的《第13号国家安全总统备忘录》(NSPM-13)显著增强了美国网络司令部的自主权,以便更快速和高效地执行网络行动[6]。同年,美国国防部发布的《网络空间战略概要》要求构建更强大的网络力量,通过“前置防御”来主动塑造网络领域的竞争格局[7]。“前置防御”旨在源头遏制及打断恶意网络行为,确保威胁在触及目标前就能被中止。

同年,《国家网络战略》的发布强调了美国将不断深化其在网络攻防领域的“非对称性”布局,倾向于“以战止战”的主动策略,推崇“最好的进攻就是最好的防御”的作战理念,试图绕过网络战的限制条件对外实施低烈度网络攻击[8]。

1.4拜登政府时期。拜登政府时期将多边竞赢作为美国网络安全的主要战略目标,侧重于在网络空间领域采取“小多边”的方式,对主要对手进行综合性遏制。2023年,《国家网络安全战略》[9]的发布提出了以“建立可防御、有韧性的数字生态系统”为愿景,未来十年里美国将与世界各地的盟友和伙伴共同努力,提高集体网络防御能力,共同挫败主要对手对互联网未来的“黑暗愿景”。

同年,《国家网络安全战略实施计划》明确了如何将战略转变为具体行动的路线图,包括加强国家安全和提高针对重大网络攻击长期防御能力的具体要求与举措[10]。此外,《2023年国防部网络战略》强调了美国国防部在网络防御方面的行动,包括投资和确保其网络和基础设施的防御性、可用性、可靠性和弹性,并支持非国防部机构发挥其相关作用,以保护美国国防工业基地[11]。战略还致力于通过建设盟友和合作伙伴的网络能力来提高美国集体网络弹性。

2 美国网络空间力量建设与编成

美国网络空间力量建设通过成立和发展网络司令部及其网络任务部队,实现了从防御到攻防兼备的战略转型。网络司令部的升级、网络任务部队细致的专业分队编成,以及持续的部队扩张,加上“网络旗帜”演习等国际合作,共同构建了一套高效、全面的网络作战体系,体现了美国在网络领域的领导力、防御决心和对全球安全合作的重视,旨在维护和提升其在网络空间的主导优势。

2.1美国网络司令部发展历程。美国网络司令部成立于2009年6月23日,作为美国国防部下属的专门指挥机构,负责计划、协调和执行网络空间内的军事行动[12]。最初,它作为美国战略司令部下的一个次级联合司令部于2010年5月21日正式运行,由时任国家安全局局长凯斯·亚历山大中将兼任首任司令。2012年,随着网络任务部队的成立,美国网络司令部开始承担更多责任,包括保护国防部信息网络、支持军事行动和防御关键基础设施。

2018年5月4日,美国网络司令部正式升级为第十个一级联合作战司令部,这意味着它在执行任务时可以直接向国防部长报告,并在必要时通过参谋长联席会议主席向总统报告。这一升级确立了“总统-国防部长-网络司令部”的网络战指挥机制,并强化了网络司令部在整个美军中的地位。升级后的网络司令部下辖陆军网络司令部、海军网络司令部、空军网络司令部和海军陆战队网络司令部,形成了一个全面覆盖各军种的网络作战体系。

为了加强国际合作和应对网络威胁的准备,美国网络司令部定期举行“网络旗帜”系列多国战术演习。例如,2024年的“网络旗帜”[13]演习吸引了来自“五眼”联盟成员国和韩国在内的18个国家参与,演习期间各国通过研讨会和网络实地训练等方式合作模拟针对复杂网络攻击的防御。

2.2美国网络任务部队力量编成。美国网络任务部队是美国网络司令部的核心组成部分,是一支高度专业化的网络作战力量。从2013年到2018年,美国网络司令部与各军种共建成了133支作战力量的网络任务部队,大约拥有6200名成员。这些部队必须满足高标准的要求,包括接受高级培训、获得相应资格认证等,以确保全面作战能力。

2018年,网络任务部队宣布达到全面作战能力,表明它们已准备好执行计划中的网络任务。这些部队细分为五种类型,分别是国家任务分队、网络防护分队、网络作战分队、作战支援分队和国家网络支援分队。这些分队的具体编成如下：

表1 美国网络任务部队编成数据具体细分

	陆军	海军	空军	海军陆战队	类型合计
国家网络任务分队	4	4	4	1	13
网络防护分队	20	20	20	8	68
网络作战分队	8	8	8	3	27
作战支援分队	6	5	5	1	17
国家网络支援分队	3	3	2	0	8

网络任务部队的每个分队都有特定的任务和职责：

(1)国家任务分队(National Mission Teams,NMT)：主要负责保护国家关键基础设施和民主进程免受网络攻击。(2)网络作战分队(Combat Mission Teams,CMT)：执行进攻性网络作战任务,以支持军事行动和战略目标。(3)网络防护分队(Cyber Protection Teams,CPT)：负责保护国防部信息网络的安全。(4)作战支援分队(Cyber Support Teams,CST)：提供必要的支援和增强能力,以支持其他网络任务分队的行动。(5)国家任务支援分队(National Support Teams,NST)：为国家任务分队提供额外的支持和资源。

2022年12月19日,美国网络司令部将其网络任务部队改制为二级联合司令部,标志着网络任务部队在网络空间保卫美国的持久使命进入了新的发展阶段。这一改革使得网络任务部队能够更快地做出反应,从而更快地发挥作战效能。

近年来,美国不断扩充网络任务部队,发展其进攻性网络力量。2022财年,美国国防部新增4个战斗任务分队,将原有的133

个网络任务部队扩大到137个，并计划在2023年和2024年再新建10个网络任务部队，这意味着网络任务部队将从拜登政府上台前的133支增加到147支。

美国网络任务部队也是执行“前出狩猎”行动的主要力量。2023年，美国网络任务部队在17个国家开展了22次“前出狩猎”行动，曝光了90多个恶意软件样本，限制了对手的机动自由，支持了合作伙伴加强网络防御，并为加强自身防御获取了重要见解。这些行动展示了美国在网络空间的领导力和防御决心，以及对全球安全合作的重视。

3 特点分析

美国通过持续演进网络安全战略视角、加强组织灵活性与力量建设、促进技术创新与智能化作战、深化国际合作与多边主义，来提升自身的网络安全能力，旨在保持其在网络空间领域的霸主地位。

3.1持续演进的战略视角是网络安全发展的基石。美国网络安全战略从防御到威慑的转变，反映了对网络安全威胁认知的不断深入以及对维护网络空间主导地位的决心。从小布什政府的初步框架到奥巴马政府引入网络威慑理念，再到特朗普政府的积极进攻性策略，直至拜登政府强调多边竞赢和韧性数字生态系统的构建，这些演变显示了战略视角的持续演进对于适应网络安全挑战的重要性。

3.2组织灵活与力量建设是提升网络作战能力的基础。美国网络司令部的升级与网络任务部队的专业化展现了美国在网络空间领域的组织灵活性。网络司令部从2009年成立以来经历了多次重大改革，包括2018年升级为一级联合作战司令部，这大大增强了其自主权和灵活性。网络任务部队的建立与发展，特别是不同类型的分队分工明确，展现了高度专业化和灵活性，这些组织结构的调整和优化对于提升网络作战能力至关重要。

3.3国际合作与多边主义是维护网络安全的重要途径。美国通过与盟友的合作，在网络空间领域建立了广泛的合作伙伴关系，促进了网络安全领域的多边主义。通过技术转移和支持合作伙伴的网络能力提升，影响着全球网络空间的技术水平和安全态势，这种国际合作有助于构建更安全、更稳定的网络空间环境。

4 结语

美国在网络空间的探索与实践，不仅彰显其在全球信息技术领域的领导地位，也揭示了战略动态调整与创新的重要性。从防御到威慑，美国通过不断优化其网络安全战略，强化组织机构与力量建设，推动技术创新及深化国际协作，构建了一个多层次、全方位的网络空间安全保障体系。随着网络威胁的日益复杂化，美国持续推动跨领域融合与多边合作，以适应不断变化的网络空间局势，确保其在网络空间中的领先地位，同时为全球网络空间治理贡献力量。

[参考文献]

[1]The White House.The National Strategy to Secure Cyberspace[EB/OL].(2003-02-14)[2019-05-27].https://www.uscert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

[2]Chairman of the Joint Chiefs of Staff Washington,D.C. The National Military Strategy for Cyberspace Operations [R].(2006.11)https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf.

[3]The White House,International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, National Security Archive, May 2011, https://nsarchive.gwu.edu/document/20843-04.

[4]Defense Science Board, “Defense Science Board (DSB) Task force on Cyber Deterrence,” 2017, https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/AD1028516.xhtml.

[5]U.S.Department of Defense, “The DoD Cyber Strategy,” April 2015, https://www.hsdl.org/?view&did=764848; “Perspective on 2015 DoD Cyber Strategy,” RAND Office of External Affairs,September2015.

[6]廖蓓蓓,邢松,孟繁瑞,等.奥巴马和特朗普时期美国网络安全战略体制研究对我国的启示[J].信息安全与通信保密,2021(3):83-90.

[7]孙璞,张辉,刘骄剑.美国《2018国防部网络战略概要》解析[J].网信军民融合,2018,(09):67-69.

[8]The White House. National CyberStrategy of United States of America[R].Washington:The White House,2018.

[9]Briefing Room, “Fact Sheet:Biden-Harris Administration Announces National Cybersecurity Strategy,” The White House, March 2, 2023, https://www.whitehouse.gov/briefingroom/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

[10]The White House, Natioanl Cybersecurity Strategy Implementation Plan,May 2024, https://www.whitehouse.gov/wp-content/uploads/2024/05/National-Cybersecurity-Strategy-Implementation-Plan-Version-2.pdf.

[11]Department of Defense, 2023 DOD Cyber Strategy, September 12,2023,available at: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF,2023.10.1.

[12]陈亚飞,王暖.美国网络司令部转型发展分析[J].航天电子对抗,2023,39(06):56-59+64.

[13]樊伟.美军年度网络演习动态与趋势[J].中国信息安全,2022,(02):68-71.

作者简介：

吕忠泽(1994--),男,汉族,辽宁大连人,博士,工程师,现就职于中国电子科技集团有限公司发展战略研究中心,研究方向:网络安全战略。

刘凌旗(1990--),女,汉族,山西运城人,博士,高级工程师,现任中国电子科技集团有限公司发展战略研究中心网络安全研究部副主任,研究方向：网络空间和认知安全。