基于大数据的网络空间安全战略的构建

□ 李留英 / 南京政治学院上海校区军事信息管理系 上海 200433

摘要：网络空间已成为各国争夺的重要领域和战场。文章在分析各国网络空间安全战略的基础上，分析了大数据对国家安全战略的影响，提出构建基于大数据的网络空间安全战略及需关注的重点领域。

关键词：大数据，网络空间，安全战略
DOI：10.3772/j.issn.1673—2286.2014.02.004

1 各国加紧制定网络空间安全战略

网络空间被称为陆、海、空、天之外的第五维空间，是各国高度关注的重要领域和战场，是国家安全最重要的组成部分[1]。党的十八大报告强调指出“要高度关注海洋、太空、网络空间安全”。

2011年以来，以美国为首的发达国家先后发布完善网络空间安全战略等文件；成立网络安全协调机构、设立协调官，强化集中领导和综合协调；成立网络战司令部，强化网络部队建设，开展大规模攻防演练，招募网络战精英人才，加快军事网络和通信系统的升级改造；推行网络外交，美欧盟友之间网络协同攻防倾向愈加明显，信息安全成为国际多边或双边谈判的实质性内容[2,3]。2013年5月，中美两国同意在战略安全对话框架下设立网络工作组，共同维护和平安全开放合作的网络空间。

美国对网络空间安全的建设最有成效，网络空间战略的发展经历了从被动防御、攻防结合到网络威慑三个阶段，尤其是2011年《网络空间可信标识国家战略》、《网络空间国际战略》和《网络空间行动战略》的相继发布，加速了网络空间的军事化进程，给其他国家发展网络空间作战能力提供了示范效应。

美国网络空间安全战略的核心思想可以归纳为：以“以防掩攻”和“以民掩军”为基调，以多层、主动防御体系为发展重点，通过主导标准、规范和法规等，推动技术创新和人才培养，保持技术领先，确保其在网络空间的主导权。美国各有关部门将根据顶层战略相继出台各自的具体网络空间战略。随着国际合作的深入，美国的网络空间战略体系将日益完善[4]。

紧随美国之后，目前已有40多个国家颁布了国家级网络空间安全战略[5]，组建扩大网络安全部队。德国于2011年出台“德国网络安全战略”，以保护关键基础设施为核心，建立了一系列相关机构，为网络安全提供多重制度保证。英国也于2011年重新修订其网络空间发展战略，组建网络战机构或网络安全部门，竞相发展网络战能力。我国也很早开展了相关研究，2012年12月中国军事学会军队指挥分会举办了“网络与信息安全战略研讨会”，积极探讨我国网络空间安全的发展问题。

2 大数据是国家安全战略的动力

随着移动网络等的发展，数据成井喷式增长。一个国家对数据的占有和控制将成为海权、空权、陆权之后的重要资产。美国政府认为数据是“未来石油”。2012年瑞士达沃斯论坛发布的《大数据，大影响》报告称，数据已经成为新的经济资产类别，未来可能成为最大的交易商品。随着云时代的来临，大数据成为最受追捧的行业利润点，并以前所未有的方式改变世界军事变革和战争形态。

美国是最早关心大数据的国家，2010年美国政府要求各部门实施大数据战略，2012年3月，美国政府发布《大数据研发和发展倡议》，正式将大数据研究提升为国家意志，使大数据成为美国网络安全战略的基础技术。2013年2月6日，包括美国国家科学基金会（NSF）在内的10家国际研究基金会宣布启动第3轮数据挖掘挑

战计划。IBM、微软、Google等美国IT巨头也加快了大数据方面的布局和投资。美国多家机构也在开展与信息网络安全相关的大数据项目[6]。

美军也在加紧推进大数据研发计划，确定了“从数据到决策、网络科技、电子战与电子防护、工程化弹性系统、大规模杀伤性武器防御、自主系统和人机互动”等7个重点研究领域，以实现由数据优势向决策优势的转化。其中最著名的是美国国防部高级研究计划局（DAPRA）启动的“XDATA项目”，是美国大数据与国家信息网络安全相结合的重要项目，标志着美军关于网络空间的技术研发进入新的阶段。DAPRA计划每年投资2500万美元，充分利用开源技术与架构，突破大数据的核心技术，开发大数据计算技术与软件工具，通过在军事领域的示范应用带动商业应用，获得军事和市场的多重优势。

世界其他发达国家也都把大数据的发展摆到国家战略层面加以推动，使大数据成为世界战略资源争夺的一个新焦点。2012年5月联合国发布了《大数据开发：机遇与挑战》报告，英国、德国、法国、日本、加拿大等发达国家积极响应。2012年7月日本推出新的ICT（信息通讯技术）战略，重点关注大数据研究和应用。2013年1月英国政府投入巨资研究医疗卫生、地理观测等方面的大数据技术，跨国企业也纷纷进入大数据领域，Google、Facebook、Microsoft等世界巨头公司成为了最重要的大数据商。

我国政府、科研机构和企业也高度关注大数据。2012年10月成立了中国通信学会大数据专家委员会，举办了关于网络空间大数据的香山科学会议，拟定了网络空间大数据科学共性理论的研究内容与方向，规划了网络空间大数据工程的研究内容与目标，讨论了推进大数据研究的组织形式与资源支持形式。同意向中国计算机学会申请组建关于网络空间大数据的专业组（Task Force），倡议成立我国的共享数据联盟和开源社区。

企业和科研机构纷纷投入大数据的研究。2012年发布的《物联网“十二五”发展规划》将海量数据存储、数据挖掘、信息传输技术、信息安全技术等大数据相关技术列入项目规划中。教育部也积极推进大数据研究工作，支持在中国人民大学建设面向海量数据管理的研究和应用平台[7]。2013年科技部将大数据列入973基础研究计划，国家自然科学基金也重点关注大数据，国家核高基和发改委重大工程均对大数据给出强劲支持。2013年7月上海科委发布《上海推进大数据研究与发展三年行动计划（2013-2015）》。

3 构建基于大数据的网络空间安全战略

随着网络空间争端的急剧升温，尤其是“棱镜门”事件的不断深化，使得大数据的概念再次被热炒，也使我们清醒地认识到制定和发展我国网络空间安全战略，推进大数据的研究及在各行业的应用，是提升我国国力和维护大国地位的有效途径。

与欧美国家相比，我国在网络空间安全技术、行动能力、人才培养等方面存在差距，已成为未来政治、经济、军事、外交发展的重大隐患。针对大数据带来的冲击和网络空间安全问题的日益严峻，需要我们加快建立我国网络空间安全战略框架，加快与网络空间安全相关的大数据技术研究，为维护网络空间安全奠定良好的基础。

3.1 制定基于大数据的网络空间安全战略

网络空间安全是一个系统的全面的安全问题，需要确定国家层面的网络空间安全总体战略。这也是指导网络空间力量建设与运用的依据和指南，更是维护国家安全利益的主要前提。中国是全世界网民最多的国家，既无相关立法，也无明确的网络空间战略性引导，缺乏整体规划，缺乏法律环境。

大数据是美国网络空间安全战略的核心技术保障，通过对重要领域数据的寡头控制，特别是充分利用大数据领域的综合优势，注重基于大数据的整体网络安全态势的感知和掌控，以保证网络空间的行动自由和实际控制，实现对现实世界的掌控能力和攻击能力。大数据技术领域的竞争，将事关国家安全和军事安全。大数据领域的落后，将会失去信息产业战略的制高点，失去数字主权的控制权，导致数字空间的巨大漏洞。

我国必须紧密跟进，制定基于大数据的发展规划。为获取未来网络空间的控制权，根据中国信息化发展规划，制定基于大数据的网络空间安全战略和行动战略，重点关注基于大数据分析的智能驱动型安全战略，从网络空间的基础支持体系、信息战作战体系和信息传播体系出发，构建“三位一体”的网络空间安全国家战略[5][9]，实现网络空间的自主、自强和有效发展，进一步促进相关产业和军事安全的发展。

3.2 确定优先发展方向和领域

（1）确定大数据的发展规划

解决网络空间安全问题需要先进防护技术的支持，而云计算、物联网、移动互联网等的快速发展，为大数据的收集、处理、应用提出新的安全挑战。为解决当前困境，云安全联盟（CSA）成立了大数据工作组，专门研究数据中心安全和隐私问题的解决方案。

同时，大数据时代的数据环境越来越复杂，存在严重的安全问题，如大量的敏感数据分布在大量节点上、软件应用发展迅速、新的网络攻击手段层出不穷，对各国网络防护能力提出了更高要求。我们应集中人力智力财力，加快研发新型网络空间安全技术，有效增强网络空间的防护水平。改进数据销毁、透明式加解密、分布式访问控制、数据审计等技术；突破隐私保护和推理控制、数据真伪识别和取证、数据持有完整性验证等技术。

（2）加快信息基础设施的自主可控

“棱镜门”计划的曝光仅仅揭露了国家信息安全挑战的冰山一角，警醒中国在芯片设计、操作系统、数据库系统网络核心骨干设备等信息产业链上严重依赖美国，也为我国信息基础设施的安全拉响警钟。为此，我们需要确定信息技术发展战略和体系设计，进一步加快信息基础产业的发展，集中力量联合研发适合大数据应用的硬件装备和软件产品，建设大数据公共服务平台，促进大数据技术成果的商业化、民用化。

（3）积极参与网络空间标准化的制定

由于美军雄心勃勃准备在网络空间中制定一系列新标准，强化网络空间“核心技术”美国化，从而在技术层面给世界各国军队带来更多制约。2012年7月美军出台了《国防部计算机战略》，代表着网络空间动态化、虚拟化、智能化、以及情报收集的细粒化、分散化以及信息收集的定制化、便捷化，最终形成高效作战效能的“网络战斗云”，最终形成美军的网络战争新格局。为此，我们需要积极参与推进网络空间标准化的制定。

3.3 确定网络空间安全的军事战略

网络空间已经成为世界各国重要的对抗战场。美国国防部正资助开展与网络安全相关的若干大数据项目，解决军事和国家安全中的大数据挑战，提升维护国家安全和信息网络安全的能力。为此，我国也需要确定统一的网络空间指挥机构和协调机构，建立一定规模的网络空间作战力量，发展基于大数据的网络空间分析技术、对抗技术、预警检测技术，建立有效的网络空间安全应急保障体系、网络空间军事行动战略等。

可以参照美军的“X计划”，制定我军的网络空间技术创新项目，重点关注负责网络环境下的理解、大数据分析处理和管理网络空间作战的大数据平台、网络空间作战地图的元数据和可视化、作战意图的表述和作战过程的自动管理等。加快军队云计算中心建设，根据网络空间作战样式的变化，研究大数据支撑下的跨网或离网数据攻击和防护。

3.4 加快网络空间人才的培养

为推动网络空间建设，2010年10月，美国启动“国家网络空间安全教育计划”（NICE），于2011年9月颁布《NICE网络空间安全人才队伍框架（草案）》，对网络空间安全人才培养的学历教育、职业培训和专业人才队伍建设具有重要指导性[8]。我国可依据信息安全人才培养计划，构建适合我国国情的网络空间人才培养方案和专业体系建设，构建适合网络空间人才培养目标的国家网络靶场。

在网络空间人才培养方面，应吸收传统信息安全专业人才培养的优点，定期组织信息安全思维培训，重点注重网络空间人才的分析能力、破坏攻击能力、攻击之前的部署防御能力的培养[10]。

3.5 加强网络空间的国际合作

网络的开放性、跨国性决定了网络空间安全是一个全球性的挑战，必须通过国际合作共同破解难题。各国国情和军情不同，对网络空间安全问题的关切也有所不同。为此，应坚持求同存异，加强交流，务实合作，在差异中求和谐，在合作中促发展，形成公正、合理、友好的国际网络空间发展环境。

4 结语

本文在分析各国网络空间安全战略现状的基础上，以大数据技术为核心，从总体上分析了各国网络空间安全战略的特点，提出构建以大数据为核心的网络空间安全战略，为夺取我国网络空间安全优势而服务。

参考文献

[1] 惠志斌.我国国家网络空间安全战略的理论构建与实现路径[J].中国软科学,2012(5):27-32.

[2] 蔡翠红.美国国家信息安全战略[M].上海:学林出版社,2009.

[3] 李晓岩.美国20世纪末以来网络空间安全战略研究[D].北京: 北京外交学院,2012.

[4] 陈治科,熊伟.美国网络空间发展研究[J].装备学院学报,2013(1):90-95.

[5] 张显龙.筹划网络空间战略,促进网络文化发展[J].中国信息安全,2013(9):50-52.

[6] 冯伟.大数据时代面临的信息安全机遇与挑战[J].装备学院学报,2013(1):49-53.

[7] 贺德方.大数据环境下的情报学[J].数字图书馆论坛,2012(11):3-6.

[8] 韩臻,王星,黄学臻,等.美国NICE网络空间安全人才队伍框架探析[J].保密科学技术,2012(9):53-57.

[9] 吴世忠,秦安.信息安全进入“控”时代,亟待培育国家网络空间安全人才[J].中国信息安全,2013(6):36-39.

[10] 潘柱廷.信息安全学科教育之路-从信息安全学科的“解剖学”课程开始[J].中国计算机学会通讯,2013,9(9):43-47.

作者简介

李留英（1972-），女，博士，南京政治学院上海校区军事信息管理系教授，硕士生导师，研究方向：信息安全、信息化。E-mail: lly003@vip.sina.com

Construction of State Cyberspace Security Strategy Based on Big Data

Li Liuying / Department of Military Information Management, Shanghai Branch of Nanjing Political College, Shanghai, 200433

Abstract: Cyberspace has become an important national competition and battlefield. According to the analysis of state cyberspace security strategies, the paper analyzes the impact of big data on state security strategy, and proposes to build a cyberspace security strategy based on big data in China and key areas to focus on.

Keywords: Big data, Cyberspace, Security strategy

（收稿日期：2014-01-08）