DOI:10.16582/j.cnki.dzzw.2014.07.007

专题报告

网络安全观视角下的网络空间安全战略构建*

网络安全课题组**
国家行政学院电子政务研究中心 北京 100089

摘 要： 网络空间安全已经成为影响国家政治、经济、社会、外交领域的关键因素和重要课题。本文阐述了新形势下网络安全观的时代内涵；分析了网络空间安全战略与网络安全观的内在逻辑；论述了新型网络安全观视角下的网络空间安全战略目标定位，并从网络空间顶层设计、防御体系、法律体系、互联网信息内容治理机制、网络空间国防力量建设、全社会参与、弘扬网络文化和强化国际合作等八个方面探讨了网络空间安全战略的实施路径，以期对保障中国网络空间安全起到一定借鉴作用。

关键词： 网络安全；空间安全；国家治理；网络治理；信息安全；信息社会

一、引言

随着经济社会的不断发展与进步，网络已经成为当今社会不可或缺的一个重要组成部分，中国的网络发展也已进入一个全新的阶段。与网络技术与网络社会不断发展形成鲜明对照的是，近些年针对网络的安全问题层出不穷，尤其是“棱镜门”事件的发生，在更大范围内给全世界各国的网络安全问题敲响了警钟[1]。提到网络安全观就不得不提到国家安全观，国家安全观是指国家根据自己所处的安全环境和所面临的安全问题，基于历史经验和政治思维所得出的观念系统，安全观体现在对国家安全利益的考虑。就中国现阶段国情而言，网络安全观是国家安全观的重要组成部分。在网络社会与网络技术不断发展普及的形势下，网络安全观会对国家整体安全产生极其重要的影响，如何全面地认识网络安全观，以及选择适合的网络安全观都会对国家网络和信息安全战略有决定性作用。

习近平总书记指出：“没有网络安全就没有国家安全”。[2]随着信息社会的飞速发展，政治安全、社会安全、经济安全、军事安全，以及建立在此基础之上的网络安全已经成为21世纪最大的安全问题。显而易见，在信息时代，谁有效驾驭了网络安全，谁就占据了网络的制高点。网络安全概念丰富拓展了国家安全的目标及内涵，也使国家安全关注的重点不断发生变化。目前，网络安全问题呈现国际化、常态化和多元化的发展趋势，安全关系向多边化演进。网络社会的虚拟环境一方面为社会文化的大发展、大进步创造了条件，同时也成为国家安全、社会发展的不稳定因素。就国内形势而言，借助互联网犯罪的行为时有发生，个人隐私泄露和侵犯、网络诈骗、网络色情、网络暴力等负面事件层出不穷，利用互联网进行分裂国家、破坏社会和谐的犯罪行为也不断出现；就国际形势而言，随着中国的综合国力增强，以美国为首的西方国家不断对中国实行“围困”，网络安全与保密形势不容乐观，这些都会在很大程度上影响中国的国家安全与发展。因而，在互联网络不断发

*基金项目：国家行政学院2013年度重大项目招标课题“电子政务环境下的政府信息公开模式研究”。
**通讯作者：丁艺 国家行政学院电子政务研究中心网络安全课题组组长：王益民，成员：宋彭旭、丁艺、刘密霞、陶勇、翟云、胡红梅、魏华、余坦、王鹏。
收稿日期：2014—06—15 修回日期：2014—06—21

展、虚拟社会逐渐成型的当今，政府治理模式转型迫在眉睫，互联网的发展对国家网络安全观的内涵提出了更多更新的要求。

围绕网络安全观和网络空间安全战略，国内外已经有相关学者开始关注。有的文献认为，需要借鉴美国的做法，从战略高度对网络安全重新认识。[3]网络安全本身是为了发展，只有在发展中求安全才能真正实现安全；必须坚持在发展中求安全，用安全来保发展，二者相辅相成。有的文献针对世界安全形势多样化、复杂化的局面，吸收了20世纪70年代后世界上出现的各种新安全观研究成果的精华，在安全实现的前提、特征、目标及其有效途径上进行了创新性的阐释，给中国的新安全观赋予了独特鲜明的理论意涵和非凡特质。[4]在网络信息技术迅猛发展的背景下，有文献提出，在网络空间中，中国意识形态的安全面临着前所未有的挑战，而这种挑战正在从网络空间快速向现实空间渗透，当务之急是建立区别于传统网络意识形态的安全观。[5]还有文献列举了美国对网络空间概念的定义，阐述了网络空间的特点；从观念变化和制度变迁两个角度分析了网络空间对美国国家安全的影响；并进而从政治、经济、军事、文化、信息等领域进一步分析网络空间对美国国家安全的影响。[6]

可见，当前网络安全观和网络空间安全战略已经成为新的研究热点，相关学者已经针对该问题提出了一些观点。但截至目前，我们还没有看到网络安全观和网络空间安全战略的有机融合，没有学者从方法论和系统论的角度分析两者的辩证关系。基于此，本文拟以网络安全观为基础，研究新技术背景下以网络安全观为方法论指导的网络空间安全战略体系的构建路径。全文安排如下：首先阐述网络安全观的时代内涵；继而分析网络空间安全战略与网络安全观的内在逻辑；最后提出网络空间安全战略与实施路径。

二、网络安全观的时代内涵

要全面、准确把握网络安全观的时代内涵，就需要通过正确界定网络安全的边疆，全面把握中国网络安全受到的威胁，并探究威胁根源来掌握网络安全观的基本内容，充分了解网络安全对手，真正做到知己知彼、百战不殆。

（一）正确界定网络安全的边疆

在安全空间边界方面，网络空间区别于实体空间，有其自身的特点。目前，中国传统思维的网络边疆基本是与实体疆域相重合的。要树立正确的网络安全观，就要正确、全面地界定国家网络安全边疆。

从形态上看，国家网络边疆至少包括有形部分、无形部分和其他部分。有形部分主要指国家网络基础设施，显而易见，国家网络边疆的有形部分应该具有最高级别的安全要求，应能有效应对任何国家、任何途径的网络攻击。无形部分主要指按照国际协议给国家分配的专属互联网域名及其域内；无形部分的安全级别也非常高，要求能对各种网络违法活动进行有效打击，能有效应对恶意屏蔽。除此之外，国家的一些核心网络信息系统，诸如金融网络信息系统、通信网络信息系统、能源网络信息系统等都与国计民生和国家安全息息相关，显而易见，这些系统的安全也属于国家网络安全的有机组成部分，应受到重视和关注。

正确认识值守网络边疆的内涵，守护网络边疆，从本质上看是角色认证和权限分配过程，即要得到允许才能进入。网络边疆的守护分为两个层次：从宏观层次看，关系国计民生和国家安全的重要系统，比如金融系统、能源系统、军事系统等的安保、屏蔽措施，是网络边疆的“值守者”；从微观层次看，诸如保障网上交易

系统、金融事务、网站密码等安全措施也属于网络边疆的“值守者”。

尽管各种密码设施、授权认证等基本保障了网络边疆安全可控，但要完全抵御外来入侵，还需要建立网络安全巡查检测机制，对外部的监听和入侵行为进行实时监测。

（二）全面把握中国网络安全的威胁

对威胁的理解即安全威胁观念是国家安全观的构成要素，不同的国家往往对威胁有不同的理解和取向。对主要威胁的判断，决定着战略力量的投入方向和分配比例。从目前的情况来看，中国在网络安全方面面临的现实或潜在威胁大致可以归纳为以下几个方面：

第一，从国家政治层面看，美国及其盟国利用网络既有优势，打着“网络自由”的旗号，对中国进行政治和意识形态渗透，包括散布虚假信息、挑战党的执政合法性，甚至公然纵容和支持那些鼓吹分裂或颠覆中国政府的政治势力。

第二，从国家经济和社会层面来看，中国的网络关键基础设施信息系统发展较晚，整体技术落后，抗外部入侵和攻击能力较弱。这些关键基础信息系统一旦停止运行或者崩溃，不仅会影响到国家的网络安全，给国家经济带来重大损失，甚至会严重影响到社会稳定。随着国际网络技术交流和合作的深入，由于中国在一些核心设备和关键技术上仍受制于人，造成了一些行业和领域系统运行状况乃至系统数据毫无安全可言，面临着严重威胁。同时，中国基础设施信息系统应对网络黑客攻击的防御意识不强，防御能力落后，很容易在出现类似伊朗“震网”式病毒袭击时，丧失反击能力，给国家造成重大损失。

第三，从军事层面看，信息化条件下的军事对抗和军事战争已经越来越依赖于网络。在国家防务上，网络空间不仅仅开辟了一个全新的作战领域，更重要的是相对于传统战场的“融入其中、控制其内、凌驾其上”，直接引起和影响现代战争形态改变。目前，美国已经制定了网络战的规则，这方面中国还相对滞后。联合国裁军研究所调查结果显示，目前已有46个国家组建了网络战部队，这一数量约占全球国家数量的1/4。[7]

（三）探究网络安全威胁的根源

中国面临的网络安全问题仍然严重，究其原因，至少可以从以下几个方面加以研究：

第一，国家信息基础设施瘫痪这一威胁一旦成为现实，会带来牵一发而动全身的负面效应，不仅会对中国经济社会造成影响范围广、时间长、代价高、难恢复的严重损害，还会引发连锁反应，导致社会矛盾的集中爆发。

第二，对关键基础设施的信息安全问题关注不够，这是防护较薄弱的环节。目前，一些关乎国计民生的重要行业和领域的网络装备（如操作系统、数据库、芯片等）多被外国品牌把持，信息系统的防御能力较弱。

第三，对信息化基础设施的内控机制不到位，也可能为不法分子的蓄意破坏留下漏洞。随着反腐败力度的不断加大，这种攻击也可能来自内部或内外勾结。

第四，美国已经明确表示要把关键基础设施信息系统作为未来网络战的主要打击目标。2013年，全国大范围的高级持续性威胁(APT)攻击愈演愈烈，且诸多攻击目标专门指向电厂、水利等国家关键基础设施，意味着网络攻击对象和范围不断拓展，已经从传统计算机网络向物理信息系统方向拓展和延伸。

第五，目前中国还没有认识到“网络战略武器”的威力，之所以现在没有出现大的问题，主要是还没有到使用“战略武器”的时候，特别是我们在网络安全方面还比较落后，还没有形成战略威胁和博弈能力。可见，

树立正确的网络安全观已成为保障国家网络空间安全的历史趋势和必然选择。

三、网络空间安全战略与网络安全观的内在逻辑

网络空间安全问题日益严峻，已引起各国政府的高度关注。发达国家尤其是美国、日本、俄罗斯等先后调整了国家安全战略，其网络空间安全战略在国家安全战略诸要素中的地位开始上升，已成为国家安全战略中不可或缺的重要组成部分[8]。

在目前形势下，构建新型的网络空间安全战略必须以围绕中国政治、经济、社会、军事等各个层面相关的网络安全观为指导，准确把握网络安全观对空间安全战略的引领作用，找准网络空间安全战略的立足点和出发点，规划网络空间安全战略的任务书、路线图和时间表。

（一）网络安全观为空间安全战略的制定提供方法论基础

空间安全战略的制定需要方法论的理论支撑，否则，空间安全战略就难免成为空中楼阁，难以有效发挥其在保障国家网络空间安全、有效维持网络空间生态中的重要作用。作为国家安全观的重要组成部分，网络安全观应为网络空间安全战略提供方法论基础，从网络安全观的视角认识和分析网络空间安全战略，进而通过网络安全观来寻求网络空间安全战略的任务书、路线图和时间表，这是优化中国网络空间安全战略的重要依据，安全观正逐步发展成为空间安全战略的方法论依据。因此，借鉴安全观的基本理念和观点来研究网络空间安全战略是科学有效的途径。

（二）网络安全观为空间安全战略的制定提供目标依据

网络安全观不是空洞的理念和观点，而是以正确界定网络安全的边疆为前提，由国家政治、经济、社会、军事、外交等各领域的网络安全组成的有机整体。在网络安全观的正确指导下，制定网络空间安全战略的过程中也必然考虑和借鉴国家政治、经济、社会、军事、外交等各领域的发展现状和存在问题，以保障国家空间安全为根本目标，在分析比较国内外国家空间安全战略制定现状的基础之上，合理规划制定中国空间安全战略的目标和实施路径。

（三）网络安全观与网络空间安全战略在安全发展中呈现动态交互关系

网络安全观和空间安全战略都不是一成不变的，而是在国际网络安全演化和发展进程中，伴随着国际政治、经济、军事、外交环境的变化，在目标、内容、重点等各个方面均发生着动态交互变化。一方面，网络安全观为网络空间安全战略提供了新的方法论指导；另一方面，网络空间安全战略随着时间演变，其目标及内容也在不断发生着变革，这种变革也给网络安全观内涵的变化提出了新的、更多的要求。这种动态的交互关系既丰富了网络安全观和空间安全战略的时代内涵，也给两者赋予了实实在在的动态关联，为两者的协同发展提供了重要依据。

四、网络空间安全战略与实施路径

（一）网络空间安全的战略目标

网络空间安全战略目标是维护和谋求国家网络空间安全利益的指标性任务，反映不同阶段国家网络空间安全的总体发展愿景[9]。中国网络空间安全的战略目标主要应包括：建立起安全可控的网络安全保障体系，使国家网络空间安全保障能力大幅度提升；强化网络及信息安全的管理、防范和控制能力；促进国家网络空间健康、稳步发展，保障国家安全、社会稳定和经济发展。

为了保证上述战略目标的实现，须明确国家网络空间安全战略的时间表和路线图，建议2015年前规划出中国网络空间安全战略的指导思想，确定网络空间安全发展的战略重点，提出网络空间安全发展的保障措施；到2020年，国家网络空间安全保障体系基本形成，重要信息系统、基础信息网络和信息内容安全防护能力大幅提升，网络空间治理水平明显提高，国家网络空间安全标准规范体系不断健全，技术攻关和产业发展健康推进，安全法律体系日臻完善，国际合作体系更加完备。

（二）网络空间安全战略的实施路径

第一，重视网络空间安全战略顶层设计。2014年2月27日，中央网络安全和信息化领导小组宣告成立，标志着中国把网络安全上升为国家战略，将从战略地位和政策上解决国家网络安全缺少顶层设计的问题。而要让中央网络安全和信息化领导小组真正发挥集中统一领导的作用，就必须着眼国家安全和长远发展，统筹协调各个地区、领域的网络和信息安全重大问题，完善组织管理体系。国家信息安全相关职能部委须进一步明确管理职责、整合管理资源、健全信息共享机制，全面优化国家网络空间安全的组织体系。

第二，建立攻防兼备的网络空间防御体系。要实现网络空间安全的战略目标，首先要建立攻防兼备的网络空间防御体系，夺取网络空间的控制权。这主要包括构建大规模网络安全态势分析及预测指标体系，打造基于骨干网、重要公共基础设施的网络安全防御与预警体系，加强关键基础设施安全的建设力度。

第三，构建国家网络空间安全的法律体系。国家网络和信息安全法律体系已成为推动国家网络空间安全、健康发展，确保国家安全和维护社会稳定的重要基石和有力保障。要充分借鉴发达国家的经验，结合中国实际，开展《网络信息安全法》《网络信息管理法》《网络信息安全教育法》《数据法》的立法调研；网络安全法律法规的制定或修订应从国家安全战略出发，站在信息化、全球化的制高点统筹考虑，相互衔接；切实做好普法工作，要把网络和信息安全领域已有的法律、法规和部门规章纳入全民普法范畴，使公民对网络空间安全领域的法律法规做到知法、懂法、守法、护法。

第四，完善互联网信息内容治理机制。对于涉及复杂利益博弈、多重价值目标交叉的互联网管制领域，并非靠某一种手段，而是要针对互联网的不同问题，采取不同的监管机制和措施，由此形成政府、行业、领域和社会密切联系、互相配合的共管机制，尽可能地在维护网络安全和秩序的前提下，确保信息的自由流通和意见的充分表达，促进互联网相关产业发展。其主要方式是通过协同管理、社会监督以及刑事制裁，使得政府部门行使职权、自律组织发挥作用，从而维护互联网信息的安全流动。

第五，加强网络空间国防力量建设。在网络空间国防建设中，坚持高科技路线不动摇的同时，要保持适度规模化的体量。中国目前尚未建立真正意义的网络国防力量，距离规模化更是相差甚远。为获得网络空间战略地位的革命性跃升，应加快构建以作战力量为主体、网络战场为导向、产学研相结合的技术创新体系，更需要突破性创新管理的思维，建设网络国防，为网络空间安全保驾护航。

第六，强化全社会网络空间安全的“立体式”参与。新时期中国的网络安全工作应鼓励和动员全社会对网络安全建设的参与，建立健全“自上而下”的“立体式”网络安全战略和政策实施体系，通过实施主体的体系化促进国家网络空间安全能力的构建与提升[4]。一方面，政府应加大对网络安全防护体系的投入力度，将网络安全防护工作细化至国家机关各部门，进而实现“立

体深化”；另一方面，要利用政策引导，鼓励全社会民众以各种形式参与国家网络安全防护工程。

第七，加大中国网络文化的弘扬力度。中国的传统文化向来倡导“和”，重视“和谐”“和为贵”，这种“尚和”文化自然将延伸至网络空间，中国网络文化内涵中的“和谐网络世界”理念符合全世界各民族国家的共同利益。因此，应加大中国网络文化的弘扬力度，让世界了解中国，理解中国在传统国际政治领域和网络空间的行为与意图，消除对中国的猜疑，这是中国在未来扭转被动局面的重要保证[4]。

第八，加强网络安全国际交流与合作。网络空间安全应该放在国际环境中审视，因此需要加强全方位的国际交流和合作。首先，要倡导建立全球网络空间安全的国际合作机制。在具体操作过程中，既可以采取多边合作模式也可以采用双边合作模式，通过广泛开展国际网络空间合作，多方发力，共同采取措施保障网络空间安全。其次，建立和完善国际网络空间安全合作新秩序。当前，互联网发展过程中全球性网络安全问题不断涌现，诸如网络犯罪、网络恐怖主义、网络知识产权纠纷、全球或地区性网络危机等，对这些全球性新课题必须通过建立和完善国际网络空间安全合作新秩序来解决。最后，切实保障世界各国的网络空间主权。各国目前在政治、经济、文化、社会现状等方面发展水平参差不齐，对网络空间安全有不同的关切和利益需求，在开展国际合作过程中，应互相尊重各自的差异，在全球网络空间安全规范和治理方面平等相处。

参考文献：

[1]汤镕昊．从“棱镜门”事件看美国的情报监督机制[J]．情报杂志，2013(9)．

[2]习近平．把我国从网络大国建设成为网络强国[EB/OL]．(2014—02—27)[2014—06—20]．http://news.xinhuanet.com/politics/2014—02/27/c_119538788.htm．

[3]吴铭．中国网络安全面临威胁[J]．党政论坛，2014(1)．

[4]王柏松，刘彤．中国新安全观的理论意涵[J]．天津行政学院学报，2014(1)．

[5]赵惜群，翟中杰，黄蓉．网络意识形态安全观内涵解读[J]．当代教育理论与实践，2014(1)．

[6]李翔．网络空间对美国国家安全的影响[D]．北京：中国青年政治学院，2013．

[7]46个国家组建网络战部队 网络安全已成“国家安全问题”[EB/OL]．(2013—4—29)[2014—06—26]．http://news.xinhuanet.com/world/2013—04/29/c_124647986.htm．

[8]刘勃然．21世纪初美国网络安全战略探析[D]．长春：吉林大学，2013．

[9]惠志斌．中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)．

通讯作者简介：

丁艺，男，博士，助理研究员，主要研究领域为电子政务、公共管理。