网络安全篇

强力推进 网络强国战略 丛书

网络强国守护神

网络安全保障

主　编　欧仕金

副主编　于丽先　王志远

知识产权出版社

全国百佳图书出版单位

网络安全篇

强力推进 网络强国战略 丛书

网络强国守护神

网络安全保障

主　编　欧仕金
副主编　于丽先　王志远

知识产权出版社
全国百佳图书出版单位

图书在版编目（CIP）数据

网络强国守护神：网络安全保障/欧仕金主编．—北京：知识产权出版社，2017.10

（强力推进网络强国战略丛书）

ISBN 978-7-5130-5111-8

Ⅰ.①网… Ⅱ.①欧… Ⅲ.①计算机网络—安全技术—研究 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字（2017）第 218540 号

责任编辑：段红梅　张雪梅　　**责任校对：**谷　洋

封面设计：智兴设计室·索晓青　　**责任出版：**刘译文

强力推进网络强国战略丛书

网络安全篇

网络强国守护神——网络安全保障

主　编　欧仕金

副主编　于丽先　王志远

出版发行：知识产权出版社有限责任公司　　**网　　址：**http://www.ipph.cn

社　　址：北京市海淀区气象路 50 号院　　**邮　　编：**100081

责编电话：010-82000860 转 8119　　**责编邮箱：**duanhongmei@cnipr.com

发行电话：010-82000860 转 8101/8102　　**发行传真：**010-82000893/82005070/82000270

印　　刷：北京嘉恒彩色印刷有限责任公司　　**经　　销：**各大网上书店、新华书店及相关专业书店

开　　本：720mm×1000mm　1/16　　**印　　张：**12.25

版　　次：2017 年 10 月第 1 版　　**印　　次：**2017 年 10 月第 1 次印刷

字　　数：210 千字　　**定　　价：**62.00 元

ISBN 978-7-5130-5111-8

强力推进网络强国战略丛书

编委会

总 序

20世纪人类最伟大发明之一的互联网，正在迅速地将人与人、人与机的互联朝着万物互联的方向演进，人类社会也同步经历着有史以来最广泛、最深刻的变革。互联网跨越时空，真正使世界变成了地球村、命运共同体。借助并通过互联网，全球信息化已进入全面渗透、跨界融合、加速创新、引领发展的新阶段。谁能在信息化、网络化的浪潮中抢占先机，谁就能够在日新月异的地球村取得优势，获得发展，掌控命运，赢得安全，拥有未来。

2014年2月27日，在中央网络安全和信息化领导小组第一次会议上，习近平同志指出："没有网络安全就没有国家安全，没有信息化就没有现代化"，"要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。"

2016年7月，《国家信息化发展战略纲要》印发，其将建设网络强国战略目标分三步走。第一步，到2020年，核心关键技术部分领域达到国际先进水平，信息产业国际竞争力大幅提升，信息化成为驱动现代化建设的先导力量；第二步，到2025年，建成国际领先的移动通信网络，根本改变核心关键技术受制于人的局面，实现技术先进、产业发达、应用领先、网络安全坚不可摧的战略目标，涌现一批具有强大国际竞争力的大型跨国网信企业；第三步，到21世纪中叶，信息化全面支撑富强民主文明和谐的社会主义现代化国家建设，在引领全球信息化发展方面有更大作为。

所谓网络强国，是指具备强大网络科技、网络经济、网络管理能力、网络影响力和网络安全保障能力的国家，就是在建设网络、开发网络、利用网络、保护网络和治理网络方面拥有强大综合实力的国家。一般认为，网络强国至少要具备五个基本条件：一是网络信息化基础设施处于世界领先水平；二是有明确的网络空间战略，并在国际社会中拥有网络话语权；三是关键技术和装备要技术先进、

自主可控；四是网络主权和信息资源要有足够的保障手段和能力；五是在网络空间战略对抗中有制衡能力和震慑实力。

所谓网络强国战略，是指为了实现由网络大国向网络强国跨越而制定的国家发展战略。通过科技创新和互联网支撑与引领作用，着力增强国家信息化可持续发展能力，完善与优化产业生态环境，促进经济结构转型升级，推进国家治理体系和治理能力现代化，从而为实现“两个一百年”目标奠定坚实的基础。

实施网络强国战略意义重大。第一，信息化、网络化引领时代潮流，这是当今世界最显著的变革特征之一，既是必然选择，也是当务之急。第二，网络强国是国家强盛和民族振兴的重要内涵，体现了党中央全面深化改革、加强顶层设计的坚强意志和创新睿智，显示出坚决保障网络主权、维护国家利益、推动信息化发展的坚定决心。第三，网络空间蕴藏着巨大的经济、科技潜力和宝贵的数据资源，是我国社会经济发展的新引擎、新动力。它与农业、工业、商业、教育等各行业各领域深度融合，催生出许多新技术、新业态、新模式，提升着实体经济的创新力、生产力、流通力，为传统经济的转型升级带来了新机遇、新空间、新活力。第四，互联网作为文化碰撞的通道、思想交锋的平台、意识形态斗争的高地，始终是没有硝烟的战场，是继领土、领海、领空之后的“第四领域”，构成大国博弈的战略制高点。只有掌握自主可控的互联网核心技术，维护好国家网络主权，民族复兴的梦想之船才能安全远航。第五，国家治理体系与治理能力现代化，需要有效化解社会管理的层级化与信息传播的扁平化矛盾，推动治理的科学化与精细化。尤其是物联网、大数据、云计算等先进技术的涌现为之提供了更加坚实的物质基础和高效的运作手段。

经过20多年的发展，我国互联网建设成果卓著，网络走入千家万户，网民数量世界第一，固定宽带接入端口超过4亿个，手机网络用户达10.04亿人，我国已经是名副其实的网络大国。但是我国还不是网络强国，与世界先进国家相比，还有很大的差距，其间要走的路还很长，前进中的挑战还很多。如何实践网络强国战略，建设网络强国，是摆在中华民族面前的历史性任务。

本丛书由战略支援部队信息工程大学相关专家教授合作完成，丛书的策划、构思和编写围绕以下问题和认识展开：第一，网络强国战略既已提出，那么，如何实施，从哪些方面实施，实施的路径、办法是什么，存在的问题、困难有哪些等。作者始终围绕网络强国建设中的技术支撑、人才保证、文化引领、安全保

障、设施服务、法律规范、产业新态和国际合作等重大问题进行理论阐述，进而提出实施网络强国战略的措施和办法。第二，网络强国战略既是一项长期复杂的系统工程，又是一个内涵丰富的科学命题。正确认识和深刻把握网络强国战略的内涵、意义、使命和要求，无疑是全面贯彻落实网络强国战略的前提条件。丛书的编写既是作者深入理解网络强国战略的认知过程，也是帮助公众深入理解网络强国战略的一种努力。第三，作为身处高校教学一线的理论工作者，积极投身、驻足网络强国理论战线、思想战线和战略前沿，这既是分内之事，也是践行国家战略的具体表现。第四，全面贯彻落实网络强国战略，既有共同面对的复杂现实问题，又有全民参与的长期发展问题。因此，理论研究和探讨不可能一蹴而就，需要作持久和深入的努力，本丛书必然会随着实践的推进而不断得到丰富和升华。

为了完成好本丛书的目标定位，战略支援部队信息工程大学校党委成立了“强力推进网络强国战略丛书”编委会，实行丛书主编和分册主编负责制，对我国互联网发展的历史和现状特别是实现网络强国战略的理论和实践问题进行系统分析和全面考量。

本丛书共分为八个分册，分别从技术创新支撑、先进文化引领、基础设施铺路、网络产业创生、网络人才先行、网络安全保障、网络法治增序、国际合作助推八个方面，对网络强国建设中的重大理论和实践问题进行了梳理，对我国建设网络强国的基础、挑战、问题、原则、目标、重点、任务、路径、对策和方法等进行了深入探讨。在撰写过程中，始终坚持突出政治性，立足学术性，注重可读性。本丛书具有系统性、知识性、前沿性、针对性、实践性、操作性等特点，值得广大人文社科工作者、机关干部、管理者、网民和群众阅读，也可供大专院校、科研院所的专家学者参考。

在丛书编写过程中，得到了中央网信办负责同志的高度关注和热情鼓励，借鉴并引用了有关网络强国方面的大量文献和资料，与多期“网信培训班”的学员进行了研讨，在此一并表示衷心的谢忱。

邬江兴

目　录

第一章　网络安全的科学内涵

当今，人类社会正在走向愈加高度信息化、网络化便愈加“危险”的时代，网络空间正日益成为关系国际及国家安全的重要领域。对此，习近平总书记在2014年2月27日的重要讲话中明确指出：“没有网络安全就没有国家安全，没有信息化就没有现代化。”面对新时代带来的便捷与危险，每个人都应该深刻理解网络空间安全的科学含义，增强维护网络安全的自觉性，养成依法上网的行为习惯，这对于国家、社会、个人利益的保护，对于推进网络强国战略都具有极其重要的意义。

一、网络安全的含义

伴随着信息网络技术突飞猛进的发展，互联网已经成为创新最活跃、渗透最广泛、影响最深远的领域。互联网以其通用、交互、开放和共享四大本质属性以及便捷、扁平、规模、集聚、普惠的五大优势正加速向经济社会各领域渗透融合，不断催生新产品、新产业、新模式、新业态，深刻改变着个人生活、企业生产、经济运行、社会管理、公共服务等社会发展的方方面面。与此同时，网络攻击窃密、技术漏洞隐患等问题引发的网络安全威胁也日益凸显，主要表现是网络攻击目标广泛、手段翻新、后果严重。以2014年为例，网络攻击目标从政府机构扩大到民众社会生活的各个方面，电信、金融、能源等多领域遭到攻击，导致大量个人、企业、政府信息泄露。“韩国电信”官网遭频繁攻击，1200万用户个

人信息被盗取泄露；美国多家银行、电商遭受网络攻击，海量数据和用户信息被泄露；以色列总理办公室、情报机关、国防部、司法部和国家安全委员会等多家政府网站受到攻击，全面瘫痪。2013 年 6 月，美国中央情报局合同制雇员斯诺登向世界披露了“棱镜”系统的存在，激起了全球震惊，并引发了极大的关注；2014 年 3 月，美国宣布准备放弃商务部通讯管理局对网络地址与名称分配当局（ICANN）的管理，考虑将其转交给一个基于“多边利益相关方模式”构建的国际新机构，再度引发了对全球网络空间基础设施和关键资源如何实施有效管辖的热议；2014 年 5 月，美国司法部起诉所谓中国黑客的举动，再度向世界表露了美国尝试在网络空间构建并护持严格服务于美国国家利益的秩序以及行为准则的战略野心。与此同时，从 2010 年开始至 2014 年下半年，各类非国家行为体，如“维基解密”“匿名”“四月六日青年运动”和后来的 ISIS 等，以及大量通过网络组织动员的行动，从“阿拉伯之春”到“伦敦骚乱”，再到“占领华尔街”“香港占中”等，向全世界展现了跨国活动借助网络的力量挑战国家安全的可能；自 2014 年 12 月开始，索尼影业公司遭遇网络黑客袭击，随后触发朝鲜与美国在网络空间的某种基于对抗的互动博弈；在伊拉克和叙利亚地面高速扩张的极端组织“伊斯兰国”，统一在网络空间展开恐怖行动，宣称支持该极端组织的黑客团体甚至成功入侵了包括美国中央司令部在内的多个账号，一度停留在研究者假设情景中的网络空间的对抗和攻击以人们未能预见的速度迅速转变为某种现实。以上种种都是我国建设网络强国所处的环境和面临的挑战。由此可见，针对政府部门设施、行业领域设施及社会民众生活的大量网络攻击行为已呈现出肆无忌惮、泛滥成灾的特点，消除网络安全威胁已成为各国政府的重要任务和国家战略。

我国推进网络强国的战略，根本的要求是要与“两个一百年”奋斗目标同步推进，即各地区、各部门要把网络工作放在实现“两个一百年”奋斗目标的工作大局中一同谋划，一同部署，一同推进，就是“要建设战略清晰、技术先进、产业发达、攻防兼备的网络强国”，具体来说，即技术要强、内容要强、基础要强、人才要强、国际话语权要强。这样的网络强国，必然是在技术先进、产业发达、攻防兼备基础上的制网权尽在掌握、网络安全坚不可摧的国家。我们必须占领信息化的制高点，牢牢掌握网络安全主动权。

网络安全是网络空间意识形态安全、数据安全、技术安全、应用安全、资本

安全、渠道安全、关防安全的总称。一切通过网络空间进行的活动及其数据链路、设备运转、关口设防等都要确保安全。网站要不被黑客攻击，系统要不被病毒感染，信息数据要不被泄露窃取，上网行为要依法规范约束，风险隐患要有效监察管控等。总之，网络安全就是要实现网络空间内容健康、上网秩序规范良好、依法治网卓有成效、防控攻击手段管用、推进发展助力正能量的功效。一言以蔽之，即依法掌握制网权。

网络信息安全在当今“互联网＋”和“＋互联网”中的地位和作用更加突出。近年来，基于信息网络的技术创新、变革突破、融合应用空前活跃，云计算、大数据等新技术高速发展，工业互联网、电子商务、互联网医疗、互联网金融以及“可穿戴”“智慧城市”“移动健康”等广泛的新业务持续创新应用，深入融合到各行各业。互联网自有的安全风险与各行各业的安全问题相互交织、互相影响，呈现出更加复杂的局面，伴生性网络安全威胁和传统网络安全问题相互渗透、持续发酵，网络安全已经成为推进“互联网＋”和“＋互联网”的重要保障。日益凸显的网络安全威胁趋势和难题主要表现在以下几个方面：一是传统网络安全威胁迅速向各新兴领域蔓延，与各行各业的安全问题交织渗透、相互影响，安全问题更趋复杂；二是网络数据资源和用户信息安全问题更加突出，如何保护网络数据已成为一个世界性难题；三是传统安全保护手段难以应对新兴安全威胁和新的保护需求；四是适应“互联网＋”和“＋互联网”领域的针对性安全技术有待突破，安全产业保障新网络安全的能力亟须提升；五是安全管理遇到新的挑战，管理模式亟待调整完善。为此，《关于积极推进“互联网＋”行动的指导意见》中提出了保障网络安全的具体举措：制定国家信息领域核心技术设备发展时间表和路线图，提升互联网安全管理、态势感知和风险防范能力，加强信息网络基础设置安全防护和个人信息保护。实施国家信息安全专项，开展网络安全应用示范，提高“互联网＋”安全核心技术水平和产品等级。按照信息安全等级保护制度和网络安全国家标准要求，加强“互联网＋”关键领域主要信息系统的安全保障。建设完善网络安全监测评估、监督管理、标准认证和创新能力体系。重视融合带来的安全风险，完善网络数据共享，利用有效安全的管理和技术措施，探索建立以行政评议和第三方评估为基础的数据安全流动认证体系，完善数据跨境流动管理制度，确保数据安全。国家的关注和筹划建设是网络安全的基础和关键。

二、网络安全的体系结构

网络安全具有严密的体系结构，它由网络安全的思想观念、管理体制机制、内容体系、法律体系、管控手段等组成。

（一）网络安全的思想观念

网络安全在国家安全中具有重要的地位，是国家总体安全的重要组成部分。国家总体安全包括国家主权政权意识形态安全、领土领海领空安全、经济政治文化社会安全、能源交通安全等，也包括网络安全。其中，网络安全威胁为非传统安全威胁的重要内容，其固有的基础性、渗透性、融合性、广延性等特点使其渗透于其他传统安全领域的全方位、全要素、全过程。信息网络无孔不入的延展使网络安全问题无处不在、无时不有，使之成为牵一发而动全身的国家安全因素。因此，习近平总书记反复强调："没有网络安全就没有国家安全。"

当前，我国网络安全面临严峻挑战，网络病毒、网络攻击、网络窃密等事件频繁发生，维护网络安全制度不健全、手段不先进、措施不得力。我国金融、能源、通信、交通、广播电视、水利、环境保护、民用核设置等重点行业中，半数行业安全防护水平比较低，难以抵御一般性的网络攻击，几乎所有的行业都难以抵御有组织、大规模的网络攻击。以 2013 年为例，当年我国共有 2430 个政府网站被篡改，同比增长 34.9%。2014 年 6 月，乌克兰、美国、韩国以及中国香港地区等的 2322 个 IP 地址通过植入"后门"对国内 3841 个网站实施了远程控制。可见，当今作为非传统安全威胁的网络安全威胁已成为国家安全的一大隐患。对此，各级政府部门和广大网民要高度重视，并强化防范意识和安全保障措施。

要形成全新的国家网络安全观。首先，全新的国家网络安全观的核心要义在于理解当前国际相互依存又彼此激烈竞争的新环境。要求世界各国在制定本国的网络安全战略中，能够有效地超越传统安全观的影响，在充满不确定性的复杂安全环境中，构建自身的国家网络安全战略。这种战略必须在生存和发展之间找到一个有效的均衡点，以可持续、可承受的方式，在网络空间有效保障包括主权在内的国家核心利益，同时确保国家可以持续有效地享受到信息技术快速发展带来的对整体国家力量的种种增益效果。其次，这种国家网络安全观必须包含全球网

络空间秩序建构的内容。当下，不同国家的网络安全观可根据其对全球网络空间秩序的理解来区分。以美国为例，其对全球网络空间秩序的理解建立在“先占者主权”这一从殖民时代的大冒险中遗留下的原则基础上，强调占有量领先优势的行为体能够在网络空间享有最大限度的自由。再次，这种国家网络安全观必须提供新的政策工具，以便在开放性的全球网络空间避免大国政策的悲剧，超越安全困境的局限。美国在全球网络空间追求霸权的行动，无论是2000年运用“梯队系统”监听欧洲商业对手的机密通信，还是2001年“9·11”恐怖袭击事件之后屡次被曝光的监听项目，又或者是2013年被披露的“棱镜”系统，总体上都可以看作传统领域谋求绝对安全和霸权优势的安全战略在网络安全领域的投影。全球网络空间不可能完全置身于事外而不受传统大国政治与安全博弈的影响，但全球网络空间自身固有的特性，如自愿基础上的开放互联为持续存在的前提条件，也为超越传统安全困境提供了重要的条件。最后，任何国家追求的网络安全观本质上都是国家主权在网络空间的投影和实践，主要的区别在于：霸权国家谋求的是自我中心和排他性的实践，淡化乃至阻止其他国家使用主权观念，只顾自身谋求主权扩张，妄图将全球网络空间置于单一主权的管辖之下；发展中国家和新兴大国关注的是以主权平等为基础的“游戏规则”，真正使全球网络空间成为推动人类社会整体发展的全新疆域、重要平台和普适工具。只有这样，才能为那些技术上处于相对弱势的行为体提供合理利用网络空间资源的制度保障和法律基础，而不是把主权作为屏障，阻挡全球网络空间的成长、拓展和数据的跨国流动。我国的出路在于，推动构建多数国家能够从中均等获利的网络治理新秩序。

（二）网络安全的管理体制机制

要变“九龙治水”为“一龙治水”。网络安全的管理体制机制对网络安全起着把关定向的作用。我国原有互联网管理体制存在明显弊端，主要是多头管理、职能交叉、权责不一、效率不高。这些体制机制弊端严重影响到我国互联网的健康发展，影响到网络安全威胁的有效治理。因此，加快完善我国互联网管理领导体制，成为党的十八届三中全会60项改革任务中的一项重要内容。这一改革任务的提出，就是要把“九龙治水”的混乱局面变为“一龙治水”的权责共担，就是要整合相关机构职能，形成从技术到内容、从日常安全到打击犯罪的互联网管理合力，确保网络的正确运用和安全，从而将互联网治理体系现代化纳入国家治

理体系和治理能力现代化的建设之中，并成为其重要的组成部分。为此，我国成立了以习近平总书记任组长的中央网络安全和信息化领导小组，旨在设立一个中央层面的更加强有力、更有权威性的领导机构，实现集中统一领导，切实解决长期以来有机构、缺统筹，有发展、缺战略，有规模、缺安全的系列问题，确保网络安全和信息化健康发展。领导小组发挥集中统一领导作用，在关键问题、复杂问题、难点问题上起决策、督促、指导作用，统筹协调涉及经济、政治、文化、社会、军事等各个领域的网络安全和信息化重大问题。在其之下成立了中央网络安全和信息化办公室，贯彻落实领导小组作出的决定事项和部署要求，做好网络意识形态、网络安全和信息化重点工作。同时，汇总各地区各部门网络安全信息、信息化建设情况，及时向中央领导小组和党中央汇报。各成员单位要同中央网络安全和信息化办公室建立工作机制，领导小组成员单位要团结合作、齐心协力，抓紧抓好网络安全和信息化工作。各省区市建立相应机构，全面推进网络安全和信息化各项工作。目前，中央网信办的组织机构在不断健全，全国各省市的网络安全和信息化领导小组成立运行，一个覆盖中央和地方的网络安全和信息化领导体系已经形成，统筹管理、协调一致的国家网络空间治理新常态展现在世人面前。

（三）网络安全的内容体系

网络安全是一个复杂的体系安全问题，就其核心内容而言主要包括意识形态安全、数据安全、技术安全、应用安全、资本安全、渠道安全、关防安全等。其中，意识形态安全是第一位的，是政治安全即政权安全、制度稳固的基础。要维护政权安全和制度安全，关键之一是维护网络意识形态安全。因为在政治安全中意识形态安全地位独特，在整个意识形态中网络意识形态又有其特殊的定位，互联网已经成为舆论斗争的主阵地、主战场、最前沿，所以必须掌握网络意识形态斗争的主动权，打好网络意识形态主动仗。可以说，掌握网络意识形态主导权，就是守护国家的主权、政权和发展权。而数据安全、技术安全、应用安全、资本安全、渠道安全和关防安全则要依靠不断的技术进步和依法治网动态地实现。

（四）网络安全的法律体系

推动网络安全立法，建设完善网络安全法律体系。网络安全立法是依法治网

的重要环节，更是规范网络秩序的重要手段。只有给网络建设的各个环节和网上一切行为画出底线、红线，并对触碰者严惩不贷，网络安全风险隐患的治理、网络秩序的维护才能蔚然成风，成为自觉。美国前总统奥巴马于 2014 年 12 月 18 日签署了四个法案，分别是《联邦信息安全管理法案》《边境巡逻员薪资改革法案》《国家网络安全保护法案》及《网络安全人员评估法案》。四个法案旨在加强美国抵御网络攻击的能力。

我国也正在推出和实践依法治网的基本策略，加紧制定网络规则和推动网络安全立法。党的十八届四中全会以后，我国网络空间法制化进程加快，网络立法、司法、执法并行并重。中央网信办落实四中全会“依法治国”精神，举办“学习宣传党的十八届四中全会精神，全面推进网络空间法制化”座谈会，提出依法管网、依法办网、依法上网，全面推进网络空间法制化，发挥法治对引领和规范网络行为的主导作用。实践中，中央网信办聚焦制定立法规则，完善互联网信息内容管理、关键信息基础设施保护等法律法规，对重要产品和服务提出安全管理要求。召开重点网站管理人座谈会，研讨重点网站如何做依法办网的践行者和推进网络空间法治的引领者。此后，中央网信办加快推动制定网络空间未成年人保护法、电子商务法等。其余相关法律也在制定中。

依法治网是统筹推进网络强国战略的根本之举。要聚焦长治久安，践行依法治网的网络强国理念，完善网络空间政策法规和规章制度，创新协同多元力量参与完善国家网络法治体系的新模式，使依靠法制规范管理网络行为的能力越来越强，尽快构建起驱散“网络雾霾”的国家网络空间治理长效机制。

（五）网络安全的管控手段

一是建立网络安全审查制度。为了维护国家网络安全、保障中国用户合法利益，我国即将推出网络安全审查制度，关系国家安全和公共利益的系统使用的重要技术产品和服务必须通过网络安全审查。中央网信办即将出台 APP 应用程序发展管理办法，并提出网络安全标准的制定和完善办法，以公正、公平的方式推进网络安全标准化建设，堵住网络设备软硬件各种漏洞和人为预留的“后门”。

二是建议开发国家网络空间安全态势感知预警系统。基于大数据的国家网络空间安全态势感知预警系统的研发，对于推进国家网络信息大数据战略、开创网

络空间大数据技术处理新时代、支撑网络治理、维护网络主权、掌握网络空间意识形态斗争主动权都具有十分重要的战略意义。首先，该系统有利于最大限度地知己知彼，掌握网络空间意识形态斗争主动权，助力提升我国国际话语权和影响力。该系统可实现对网络空间信息大数据高速筛选分析和隐患风险及时预警，大幅提高工作效率；终结对网络空间隐患风险的抓取、分析、处置人海战术低效运作局面；拓展大数据利用功效，对大数据资源去粗取精、去伪存真，分类储存，然后提供给相关部门开发、利用和保护，以服务于经济、政治、文化、社会、国防、外交等的建设发展；知己知彼，掌握主动，提升我国国际话语权和影响力，进而影响世界格局，掌握国际规则主导权。其次，该系统有利于最大限度地用好技术力量和成果资源，开发、集成综合高效平台，助力有效管控网域资源和维护国家网络主权。要充分利用信息技术和网络空间安全学科国家人才优势，研发大数据在线分析为主的国家网络空间安全态势感知预警系统、总控操作平台和安全态势大数据资源分类储存及更新库；组织军地技术精英集成优化已有的“中国网信大数据库”“国家互联网舆情分析大数据平台”“国家互联网基础资源大数据平台”，同时关联“大数据安全关键标准和验证平台”；链接各省、自治区、直辖市网信办舆情监察系统，发挥地方积极性。最后，该系统有利于最大限度地满足需求功能，精心进行系统设计，以助力提升网信中心的感知预警能力。充分利用大数据技术及国产化成果，建立一个自主可控、高效能、高可用、低功耗、可线性扩展的国家网络空间安全态势感知预警系统，以胜任全面感知、支撑治理、预测预警、应急调控、形成威慑的任务。这一系统将高度集成国产化的大数据平台、大数据在线分析系统、系统调度控制平台、国家网信大数据等资源，以及军地相关先进技术成果，拥有超算容错、在线分析、智能关联、追踪溯源、态势预测、规模存储、可视化展示等能力，可以极大改善网信机构的手段和能力，全面提升国家网络空间安全态势的感知预警水平。

三、网络安全的核心内容

网络安全的核心内容主要包括“七个安全”，即意识形态安全、数据安全、技术安全、应用安全、资本安全、渠道安全、关防安全，其中意识形态安全居于首位。皮之不存，毛将焉附？每个安全都要认真研究，把好关口。