

100 Q&As

ON CYBER SECURITY LAW OF
THE PEOPLE'S REPUBLIC OF CHINA

中华人民共和国 网络安全法 百问百答

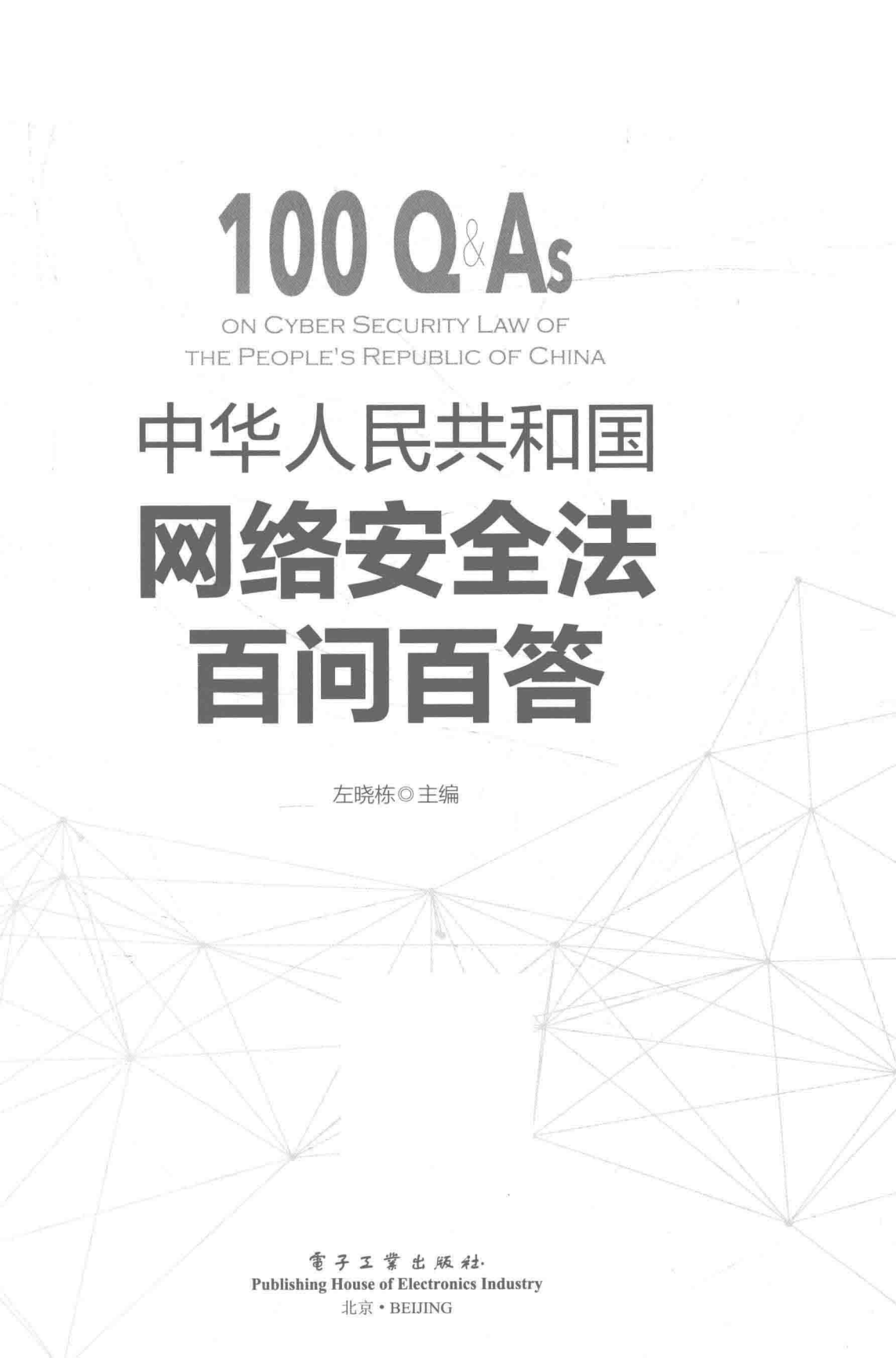
左晓栋◎主编



中国工信出版集团



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>



100 Q&As

ON CYBER SECURITY LAW OF
THE PEOPLE'S REPUBLIC OF CHINA

中华人民共和国 网络安全法 百问百答

左晓栋◎主编

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内容简介

本书针对社会各方面对《中华人民共和国网络安全法》（本书简称《网络安全法》）的关切，整理了100个问题，并给出了回答。按照各项问答对应的《网络安全法》条款的顺序，将这些问答分为“总体”、“网络安全支持与促进”、“网络运行安全一般规定”、“关键信息基础设施运行安全”、“个人信息保护与互联网信息内容安全”、“监测预警与应急处置”、“其他”共七部分。此外，还在附录中提供了为配合《网络安全法》实施而制定的有关政策文件的最新版（含征求意见稿）。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有，侵权必究。

图书在版编目（CIP）数据

中华人民共和国网络安全法百问百答 / 左晓栋主编. — 北京：电子工业出版社，2017.8
ISBN 978-7-121-32222-8

I. ①中… II. ①左… III. ①计算机网络—科学技术管理法规—中国—问题解答
IV. ①D922.170.4

中国版本图书馆CIP数据核字（2017）第167779号

策划编辑：戴晨辰

责任编辑：戴晨辰

印 刷：三河市双峰印刷装订有限公司

装 订：三河市双峰印刷装订有限公司

出版发行：电子工业出版社

北京市海淀区万寿路173信箱 邮编：100036

开 本：720×1000 1/16 印张：10.75 字数：168千字

版 次：2017年8月第1版

印 次：2017年8月第1次印刷

定 价：35.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店缺货，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：dcc@phei.com.cn。

编写组

左晓栋

伍 扬

张 恒

王政坤

前言

《中华人民共和国网络安全法》（本书简称《网络安全法》）已于2017年6月1日正式施行。这是我国网络安全领域的“基本法”，具有里程碑式的重大意义。《网络安全法》的起草坚持问题导向，主要针对实践中存在的突出问题，将近年来一些成熟的好做法作为制度确定下来，为网络安全工作提供切实法律保障。但同时，还有一些制度安排确有必要，但尚缺乏实践经验，《网络安全法》对此进行了原则性规定，为需要制定的配套法规政策预留了接口。在法的施行过程中，无论是国外还是国内，大家都很关心，一些条款的要求如何理解、如何落地？相关的“规定”是什么？“有关部门”是指哪里？如此等等。为此，本书总结了《网络安全法》发布以来的国内外主要关切和社会普遍关心的100个问题，并有针对性地进行了回答。书后还附上了相关部门为落实《网络安全法》而制定的有关政策文件，如《网络产品和服务安全审查办法》、《国家网络安全事件应急预案》等。对一些仍在制定中的政策，本书附上了征求意见稿，如《关键信息基础设施安全保护条例》、《重要数据识别指南》等。本书力求突出实用性，希望为各方面宣贯和施行《网络安全法》提供便利。

需要指出，编写这本百问百答，出自国家网信部门的提议，但对100个问题的梳理和回答，则是站在专家个人的角度，不代表最终的官方决策。由于编者水平有限，不妥之处在所难免，仅供读者参考。

编 者

二〇一七年七月

目录

CONTENTS

第一部分 总 体

- 1 为什么制定《网络安全法》? // 2
- 2 制定《网络安全法》的指导思想和原则是什么? // 2
- 3 如何理解“网络安全”? // 3
- 4 网络空间主权的内涵是什么? // 4
- 5 外企、驻华机构的网络是否适用本法? // 4
- 6 如何理解网络安全与信息化发展并重? // 5
- 7 什么是国家网络安全战略? // 6
- 8 如何理解国家要采取措施应对来源于境内外的网络安全风险和威胁? // 7
- 9 为什么立法加强网络空间国际交流与合作? // 7
- 10 如何理解“和平、安全、开放、合作”的网络空间? // 8
- 11 如何理解“多边、民主、透明”的网络治理体系? // 9
- 12 如何理解国家网信部门负责统筹协调网络安全工作? // 10
- 13 如何理解国家网信部门负责网络安全相关监督管理工作? // 11
- 14 《网络安全法》规定的县级以上人民政府有关部门的网络安全保护和监督管理职责如何落实? // 12
- 15 《网络安全法》明确规定的地方政府的网络安全责任有哪些? // 12

第二部分 网络安全支持与促进

- 16 《网络安全法》规定的网络运营者应该承担的责任，是否适用于个人、家庭及所有企业和机构？ // 13
- 17 为什么鼓励网络相关行业组织制定网络安全行为规范？ // 14
- 18 《网络安全法》对个人和组织提出了哪些明确的行为禁则？ // 14
- 19 如何加强对未成年人的网络保护？ // 15
- 20 个人和组织对危害网络安全的行为如何举报？ // 16
- 21 《网络安全法》是否会限制国外技术和产品？ // 16
- 22 是否会根据《网络安全法》的规定，要求企业向中国政府提供产品源代码？ // 17
- 23 《网络安全法》对网络运营者规定了哪些责任、义务？ // 17
- 24 《网络安全法》对关键信息基础设施运营者规定了哪些责任、义务？ // 18
- 25 如何加强国家网络安全标准体系建设？ // 22
- 26 外国企业能否参与制定行业和国家网络安全标准？ // 23
- 27 “安全可信”的网络产品和服务是什么含义？ // 24
- 28 为什么要鼓励开发网络数据安全保护和利用技术？ // 24
- 29 如何理解创新网络安全管理方式，运用网络新技术，提升网络安全保护水平？ // 25
- 30 国家如何开展经常性的网络安全宣传教育活动？ // 26
- 31 国家如何支持网络安全相关教育与培训活动？ // 27

第三部分
网络运行安全
一般规定

- 32 网络安全等级保护制度与现行的信息安全等级保护制度是什么关系? // 30
- 33 什么样的设备和系统应当留存网络日志不少于六个月? // 31
- 34 什么是国家标准的强制性要求? // 31
- 35 网络产品、服务存在安全缺陷、漏洞等风险时,应如何告知用户并向有关主管部门报告? // 32
- 36 如何理解网络产品、服务的提供者应当持续提供安全维护? // 33
- 37 什么是“网络关键设备”和“网络安全专用产品”? // 34
- 38 在进行安全认证或安全检测时,什么是“具备资格的机构”? // 35
- 39 外国人员携带设备进入中国是否需要检测和认证? // 35
- 40 如何理解第二十三条的强制性市场准入要求? // 36
- 41 我国是否认可国外认证和检测机构的认证及检测结果? // 36
- 42 如何理解《网络安全法》对提供用户真实身份信息所作的要求? // 37
- 43 网络运营者在提供信息发布、即时通讯服务时验证用户真实身份信息在技术和成本上是否可行? // 38
- 44 用户提供真实身份信息是否会影响个人隐私? // 38
- 45 什么是网络可信身份战略? // 39
- 46 发生危害网络安全的事件时,网络运营者应如何报告? // 40
- 47 如何理解开展网络安全认证、向社会发布网络安全信息等应当遵守国家有关规定? // 41

第四部分
关键信息基础设施
运行安全

- 48 企业为公安机关、国家安全机关提供技术支持和协助，是否会损害个人隐私、侵犯知识产权？ // 41
- 49 为什么强调网络运营者之间的网络安全合作？ // 42
- 50 关键信息基础设施的范围有哪些？ // 44
- 51 什么是“关键信息基础设施安全保护办法”？ // 44
- 52 为什么要加强关键信息基础设施保护？ // 45
- 53 关键信息基础设施是否包括外企在中国境内的信息系统？ // 46
- 54 如何理解“自愿参与关键信息基础设施保护体系”？ // 46
- 55 网络安全等级保护制度与关键信息基础设施保护制度是什么关系？ // 47
- 56 什么是“负责关键信息基础设施安全保护工作的部门”？ // 48
- 57 为什么要求关键信息基础设施安全保护部门编制和组织实施本行业、本领域的关键信息基础设施安全规划？ // 48
- 58 如何理解“三同步”？ // 49
- 59 如何对关键信息基础设施安全管理机构负责人和关键岗位的人员进行安全背景审查？ // 49
- 60 接受网络安全教育、技术培训和技能考核的从业人员包括哪些人员？ // 50
- 61 如何对重要系统和数据库进行容灾备份？ // 51
- 62 如何制定网络安全事件应急预案？ // 52
- 63 什么是网络安全审查？ // 53

64	如何判定网络产品和服务可能影响国家安全?	// 54
65	网络安全审查是否要限制国外产品和服务?	// 55
66	如何理解“使用未经安全审查或者安全审查未通过的网络产品或者服务的”要受到处罚?	// 55
67	关键信息基础设施的运营者采购网络产品和服务时如何签订安全保密协议?	// 55
68	《网络安全法》提出数据应当留存在境内,会不会限制数据跨境流动,影响公民出国旅游和企业跨国贸易?	// 56
69	如何理解“境内运营”和“向境外提供”?	// 57
70	什么是需要在境内存储的“重要数据”?	// 57
71	数据出境安全评估如何实施?	// 58
72	跨国公司位于中国和国外的分支机构间传输数据也需要进行安全评估吗?	// 59
73	如何理解第六十六条中对在境外存储“网络数据”或者向境外提供“网络数据”的行为的处罚?	// 59
74	如何理解《网络安全法》对关键信息基础设施提出的自评估要求?	// 60
75	由谁对关键信息基础设施进行抽查检测和应急演练?	// 61
76	如何促进网络安全信息共享?	// 62

第五部分 个人信息保护与互联网 信息内容安全

77	《网络安全法》为什么加强对个人信息的保护?	// 64
78	《网络安全法》体现了哪些个人信息保护原则?	// 64
79	如何理解《网络安全法》的“明示”要求	// 65
80	如何理解《网络安全法》的“同意”要求	// 66

- 81 如何理解收集个人信息的“合法、正当、必要”原则? // 67
- 82 发生或可能发生个人信息安全事件时,应如何告知用户并向主管部门报告? // 68
- 83 《网络安全法》规定,个人有权要求网络运营者删除个人信息和纠正不准确的个人信息,这是否会加重企业负担、妨碍企业发展? // 69
- 84 个人如何“发现”网络运营者违法或违约定收集、使用个人信息或收集、存储的个人信息有错误? // 70
- 85 如何理解不得非法出售或者非法向他人提供个人信息? // 70
- 86 《网络安全法》规定,网络运营者应当加强对其用户发布的信息的管理,这是否会妨碍网上言论自由和信息自由流动? // 71
- 87 网络运营者删除用户发布的信息,应当遵循哪些要求? // 72
- 88 《网络安全法》中的“电子信息发送服务提供者”、“应用软件下载服务提供者”有哪些? // 72
- 89 如何理解电子信息发送服务提供者和应用软件下载服务提供者的安全管理义务? // 73
- 90 《网络安全法》要求采取技术措施和其他必要措施阻断境外非法信息的传播,这是否意味着要对国外网站进行更严格的封堵? // 74

第六部分 监测预警与应急处置

- 91 为什么要建立网络安全监测预警和信息通报制度,并加强统筹协调? // 76
- 92 各行业、各领域的网络安全监测预警信息如何报送? // 76
- 93 各行业、各领域网络安全应急预案与国家网络安全应急预案的关系是什么? // 77

94	网络安全事件如何分级?	// 78
95	如何理解网络安全事件处置的属地管理规定?	// 78
96	发现安全风险或发生安全事件时, 如何对该网络运营者进行约谈?	// 79
97	什么情况下需要采取通信管制临时措施?	// 80

第七部分 其 他

98	如何区分“网络运营者”中“网络的所有者、管理者和网络服务提供者”?	// 82
99	违反《网络安全法》的行为如何记入信用档案?	// 83
100	如何对来源于境外的机构、组织、个人危害国家关键信息基础设施的活动追究其责任?	// 84

附 录

附录 A	中华人民共和国网络安全法	// 85
附录 B	网络产品和服务安全审查办法(试行)	// 101
附录 C	重要数据识别指南(征求意见稿)	// 105
附录 D	关于发布《网络关键设备和网络安全专用产品目录(第一批)》的公告	// 129
附录 E	国家网络安全事件应急预案	// 133
附录 F	关键信息基础设施安全保护条例(征求意见稿)	// 149

第一部分
PART 1 / 总 体

1 为什么制定《网络安全法》？

当前，网络和信息技术迅猛发展，已经深度融入我国经济社会的各个方面，极大地改变和影响人们的社会活动和生活方式，在促进技术创新、经济发展、文化繁荣、社会进步的同时，网络安全问题也日益凸显。一是，网络入侵、网络攻击等非法活动，严重威胁着电信、能源、交通、金融，以及国防军事、行政管理等重要领域的信息基础设施的安全，云计算、大数据、物联网等新技术、新应用面临着更为复杂的网络安全环境；二是，非法获取、泄露甚至倒卖公民个人信息，侮辱诽谤他人、侵犯知识产权等违法活动在网络上时有发生，严重损害公民、法人和其他组织的合法权益；三是，宣扬恐怖主义、极端主义，煽动颠覆国家政权、推翻社会主义制度，以及淫秽色情等违法信息，借助网络传播、扩散，严重危害国家和社会公共利益。

党的十八大以来，以习近平同志为核心的党中央从总体国家安全观出发，就网络安全问题提出了一系列新思想、新观点、新论断，对加强国家网络安全工作作出重要部署。党的十八届四中全会决定要求完善网络安全保护方面的法律法规。广大人民群众十分关注网络安全，强烈要求依法加强网络空间治理，规范网络信息传播秩序，惩治网络违法犯罪，使网络空间清朗起来。全国人大代表也提出许多议案、建议，呼吁出台网络安全相关立法。为适应国家网络安全工作的新形势新任务，落实党中央的要求，回应人民群众的期待，制定出台了《网络安全法》。

2 制定《网络安全法》的指导思想和原则是什么？

制定《网络安全法》的指导思想是：坚持以总体国家安全观为指导，全面落实党的十八大和十八届三中、四中全会决策部署，坚持积极利用、科学发展、依法管理、确保安全的方针，充分发挥立法的引领和推动作用，针对当前我国网络安全领域的突出问题，以制度建设提高国家网络安全保障能力，掌握网络空间治理和规则制定方面的主动权，切实维护国家网络空间主权、安全和发展利益。

制定《网络安全法》把握了以下几点原则。

第一，坚持从国情出发。根据我国网络安全面临的严峻形势和网络立法的现状，充分总结近年来网络安全工作经验，确立保障网络安全的基本制度框架。重点对网络自身的安全作出制度性安排，同时在信息内容方面也作出相应的规范性规定，从网络设施设备安全、网络运行安全、网络数据安全、网络信息安全等方面建立和完善相关制度，体现中国特色。同时，注意借鉴有关国家的经验，主要制度与国外通行做法是一致的，并对内外资企业同等对待，不实行差别待遇。

第二，坚持问题导向。《网络安全法》是网络安全管理方面的基础性法律，主要针对实践中存在的突出问题，将近年来一些成熟的好做法作为制度确定下来，为网络安全工作提供切实法律保障。对一些确有必要但尚缺乏实践经验的制度安排作出原则性规定，同时注重与已有的相关法律法规相衔接，并为需要制定的配套法规预留接口。

第三，坚持网络安全与信息化发展并重。网络安全和信息化是一体之两翼，驱动之双轮。维护网络安全，必须处理好与信息化发展的关系，坚持以安全保发展、以发展促安全的要求，通过保障安全为发展提供良好环境。本法注重对网络安全制度作出规范的同时，注意保护各类网络主体的合法权利，保障网络信息依法、有序、自由流动，促进网络技术创新和信息化持续健康发展。

3 如何理解“网络安全”？

伴随信息革命的飞速发展，互联网、通信网、计算机系统、自动化控制系统、数字设备及其承载的应用、服务和数据等组成的网络空间，正在全面改变着人们的生产生活方式，深刻影响着人类社会历史发展进程。当前，网络空间已经成为信息传播的新渠道、生产生活的新空间、经济发展的新引擎、文化繁荣的新载体、社会治理的新平台、交流合作的新纽带、国家主权的新疆域。

“网络安全”是“网络空间安全”的简称，不是“network”的安全，而是“cyber”或“cyberspace”的安全。网络安全涵盖传统意义上的信息安全、互联网安全、通

信安全、计算机安全等方面，包括互联网、通信网、计算机系统、自动化控制系统安全，同时包括这些网络和系统承载的应用、数据和信息内容的安全。

4 网络空间主权的内涵是什么？

第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

国家网络空间主权主要包含以下四方面内容：

- 一是各国根据本国国情，借鉴国际经验，制定本国有关网络空间的法律法规；
- 二是各国根据本国法律法规，管理本国网络空间；
- 三是采取必要措施，监测、保护、抵御来自国内外的网络空间威胁和攻击；
- 四是依法防范、阻止违法信息在本国网络空间的传播。

5 外企、驻华机构的网络是否适用本法？

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

根据《网络安全法》第二条，外企和驻华机构的网络如果在中华人民共和国境内，则适用于本法。

但外国驻中国使领馆、享有外交特权的国际组织驻华机构的网络，遵照《中华人民共和国领事特权与豁免条例》等外事相关规定执行。

6 如何理解网络安全与信息化发展并重？

第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

中央网络安全和信息化领导小组第一次全体会议指出，网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。做好网络安全和信息化工作，要处理好安全和发展关系，做到协调一致、齐头并进，以安全保发展、以发展促安全，努力建久安之势、成长治之业。

“以安全保发展、以发展促安全”的要求，充分体现了马克思主义的辩证法，体现了科学的发展观。网络安全是信息化推进中出现的新问题，只能在发展的过程中用发展的方式加以解决。没有网络安全，信息化发展越快，造成的危害就可能越大。而没有信息化发展，经济社会发展将会滞后，网络安全也没有保障，甚至已有的安全也会丧失。

不发展是最大的不安全。不能简单地通过不上网、不共享、不互联互通来保安全，或者片面强调建专网。这样做的结果只能是造成不必要的重复建设，大量网络资源得不到充分利用，增加信息化的成本，降低信息化效益，失去发展机遇。要以改革的精神、开放的理念、创新的机制来科学治理和化解信息化发展中出现的问题与风险，掌握国家网络空间安全战略主动权，维护网络空间安全，促进国家发展。