# 网络安全知识读本

WANGLUO ANQUAN ZHISHI DUBEN

雷　敏◎主编

中国人事出版社

# 网络安全知识读本

WANGLUO ANQUAN ZHISHI DUBEN

雷　敏◎主编

中国人事出版社

**图书在版编目(CIP)数据**

网络安全知识读本/雷敏主编. -- 北京：中国人事出版社，2018

ISBN 978-7-5129-1337-0

Ⅰ. ①网… Ⅱ. ①雷… Ⅲ. ①计算机网络-网络安全 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2018)第 181528 号

**中国人事出版社出版发行**

(北京市惠新东街 1 号 邮政编码：100029)

*

中国铁道出版社印刷厂印刷装订 新华书店经销

880 毫米×1230 毫米 32 开本 4.875 印张 91 千字

2018 年 8 月第 1 版 2018 年 8 月第 1 次印刷

**定价：22.00 元**

读者服务部电话：(010) 64929211/84209101/64921644

营销中心电话：(010) 64962347

出版社网址：http://www.class.com.cn

CONTENTS

# 目 录

# 第一章

# 网络空间安全概述

随着信息化的发展，以互联网为基础的计算、通信和信息共享已经成为社会重要的公共设施，其安全性挑战日益严峻，逐渐成为各方利益冲突和争夺的主战场。进入 21 世纪以来，随着云计算、物联网、大数据等新技术的应用，网络安全又面临着新的挑战，网络空间作为继陆、海、空、天之后的“第五维空间”，已经成为各国角逐权力的新战场。

## 第一节　网络空间安全发展历史

从信息论角度来看，系统是载体，信息是内涵。网络空间是所有信息系统的集合，是人类生存的信息环境，人在其中与信息相互作用并相互影响。因此，网络空间存在更加突出的信息安全问题，其核心内涵仍是信息安全。

信息安全是一个广泛而抽象的概念，从不同领域和不同角度对其阐述会有所不同。在全国信息安全标准化技术委员会发布的《信息安全技术　术语》（GB/T 25069—2010）中，信息安全是指保持、维持信息的保密性、完整性和可用性，也可包括真实性、可核查性、抗抵赖性和可靠性等性质。信息安全的目标是保证信息上述安全属性得到保持，从而对组织业务运行能力提供支撑。在商业和经济领域，信息安全主要强调的是消减并控制风险，保持业务操作的连续性，并将风险造成的损失和影响降到最低。对于建立在网络基础之上的现代信息系统，信息安全是指保护信息系统的硬件、软件及相关数据，使信息不因偶然或者恶意侵犯而遭受破坏、更改及泄露，保证信息系统能够连续、可靠、正常地运行。

随着全球社会信息化的深入发展和持续推进，相比物理的现实社会，网络空间中的数字社会在各个领域所占的比例越来越大。数量的增长带来了质量的变化，以数字化、网络化、智能化、互联化、泛在化为特征的网络社会，为信息安全带来了新技术、新环境和新形态，信息安全开始更多地体现在网络安全领域，反映在跨越时空的网络系统和网络空间之中，反映在全球化的互联互通之中。

因此，网络空间安全可以看作是信息安全的高级发展阶段，其发展历程如图 1—1 所示。

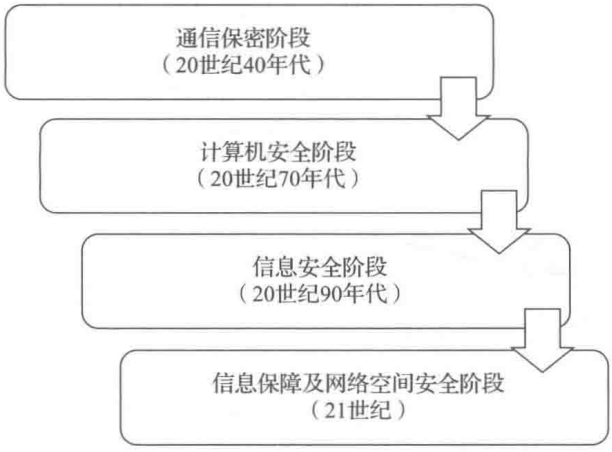


图 1—1　网络空间安全发展历程

### 1. 通信保密阶段

通信保密阶段开始于 20 世纪 40 年代，其标志是 1949 年克劳德·艾尔伍德·香农（Claude Elwood Shannon）发表的《保密系统的通信理论》，该理论首次将密码学的研究纳入了科学的轨道。在这个阶段所面临的主要安全威胁是搭线窃听和密码分析，其主要保护措施是数据加密。该阶段人们关心的只是通信安全，而且关心的对象主要是军方和政府机构。需要解决的问题是在远程通信中拒绝非授权用户的访问以及确保通信的真实性，主要方式包括加密、传输保密、发射保密以及通信设备的物理安全。当时涉及的安全属性有机密性，即保证信息不会泄露给未经授权的人或者主体；可靠性，即保证信道、消息源、发信人的真实性以及核对信息接收者的合法性。在这一阶段，虽然计算机系统的脆

弱性已被一些机构所认识，但由于当时计算机速度和性能比较落后，使用范围有限，因此，通信保密阶段重点是通过密码技术解决通信保密问题，保证数据的机密性和可靠性。

### 2. 计算机安全阶段

计算机安全阶段开始于20世纪70年代。这一阶段的标志是1977年美国国家标准局公布的《数据加密标准》和1985年美国国防部公布的《可信计算机系统评估准则》。这些标准的提出意味着信息安全问题的研究和应用跃上了一个新的高度。

此阶段主要在密码算法及其应用和信息系统安全模型及评价两个方面取得了很大的进展。1977年，美国国家标准局采纳了新开发的分组加密算法；1977年，罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）根据威特菲尔德·迪菲（Whitfield Diffie）和马丁·赫尔曼（Martin Hellman）在《密码学的新方向》开创性论文中提出的思想，创造了RSA公开密钥密码算法；1985年尼尔·科布利茨（Neal Koblitz）和维克多·米勒（Victor Miller）提出了椭圆曲线离散对数密码体制，该体制的优点是可以利用更小规模的软件、硬件实现有限域上同类体制的相同的安全性。

1985年，美国国防部推出了《可信计算机系统评估准则》，该标准是信息安全领域中的重要创举，为后来英国、法国、德国、荷兰四国联合提出的包含保密性、完整性和可用性概念的

《信息技术安全评价准则》及《信息技术安全评价通用准则》的制定打下了基础。

### 3. 信息安全阶段

20 世纪 90 年代以来，通信和计算机技术相互依存，数字化技术促进了计算机网络发展成为全天候、通全球、个人化、智能化的信息高速公路，互联网（Internet）成为一项家用技术平台，安全的需求不断地向社会各个领域扩展，人们关注的对象已经逐步从计算机转向更具本质性的信息本身，信息安全的概念随之产生。

由于网络的发展，特别是电子商务的发展，人们除了要求在信息的存储、处理和传输过程中不被非法访问或者更改，确保对合法用户的服务并限制非授权用户的服务外，还要求必要的检测、记录和抵御攻击的措施。于是，除了信息的机密性、完整性和可用性之外，人们对信息的安全性有了新的要求，即可控性、不可否认性以及可审计性。在这一时期，公钥技术得到了长足的发展，著名的 RSA 公开密钥密码算法获得了日益广泛的应用，用于完整性校验的哈希（Hash）函数的研究应用也越来越多。

在该阶段，美国国防部提出了信息保障的概念：保护和防御信息及信息系统，确保其可用性、完整性、保密性、可审计性和不可否认等特性。这些特性包括在信息系统的保护、检测、反应功能中，并提供信息系统的恢复能力。

信息保障除了强调信息安全的保障能力外，还提出了要重视系统的入侵检测能力、系统的事件反应能力以及系统在遭到入侵破坏后的快速恢复能力。它关注信息系统整个生命周期的防御和恢复。

### 4. 信息保障及网络空间安全阶段

由于针对信息系统的攻击日趋频繁以及电子商务的快速发展，安全的概念发生了以下的变化。

第一，信息的安全不再局限于信息的保护。人们需要对整个信息和信息系统进行保护和防御，包括保护、检测、反应和恢复能力。

第二，信息的安全与应用更加紧密。其相对性、动态性、系统性等特征引起人们的注意，追求适度风险的信息安全成为共识。安全不再单纯以功能或者机制技术的强度作为评价指标，而是结合了不同主体的应用环境和应用目标的需求，进行合理的计划、组织和实施。

从信息安全各阶段的发展可以看出，随着信息技术本身的发展和信息技术应用的发展，信息安全的外延不断扩大，包含的内容从初期的数据加密到后来的数据恢复、信息纵深防御直到如今网络空间安全概念的提出。只有把握了信息安全及网络空间安全发展的趋势，才能更好地建立满足现在和未来需求的网络空间安全体系。

## 第二节　网络空间安全形势

2013 年，“棱镜门”事件在全球持续发酵，隐藏在互联网背后的国家力量和无所不在的“监控”之手，引起了舆论哗然和网络空间的一系列连锁反应。全球范围内陡然上升的网络攻击威胁，导致各国对网络安全的重视程度急剧提高，越来越多的国家将网络安全列为国家核心安全利益，网络安全进一步成为大国竞争的战略基点，其较量和博弈逐步深化升级。

当前，我国网络空间环境日趋复杂，随着迅速发展的信息技术与服务不断超越现有的互联网监管体制，各种危及国家安全和社会稳定的网络违法和犯罪活动越来越猖獗，比如病毒入侵、网络诈骗和网络泄密等。同时在利益的驱动下，网络犯罪变得更加有组织、有目标，隐蔽性和复杂性更强，危害性更大，其影响力和破坏程度也与日俱增。网络安全问题给互联网的健康发展带来极大的挑战，这些问题主要体现在以下三个方面。

第一，针对网络信息的破坏活动日益严重，网络犯罪案件个数逐年上升。鉴于互联网具有传播速度快、覆盖面广、隐蔽性强和无国界等特点，传统领域的违法犯罪活动逐渐向互联网渗透，越来越多的高新技术被违法犯罪分子利用，网络犯罪案件个数逐年大幅上升，犯罪类型不断扩展，作案手段不断翻新，危害后果日趋严重。同时对网络犯罪的安全防范难度越来越大，安全保障

的要求越来越高。

第二，安全漏洞和安全隐患增多，对信息安全构成严重威胁。网络安全事件的发生，绝大多数都与信息技术自身的缺陷有关，安全漏洞和安全隐患的存在已经成为我国网络与信息安全的长期威胁。首先，安全漏洞广泛且客观存在，易为人所用。信息技术的漏洞无处不在，涉及软硬件等各个方面，是病毒、黑客攻击等安全问题的重要根源，是网络环境下失、窃密的重大隐患。其次，安全漏洞数量多，消除难度大。近年来安全漏洞随信息技术和产品的广泛应用出现呈倍增趋势，而且从公开至被利用的时间间隔越来越短，安全漏洞消除工作变得十分复杂且难度很大。最后，新业务、新应用安全风险高。随着云计算、物联网等互联网新业务、新应用的流行，新的问题和安全隐患凸显，这将是未来我国网络治理面临的难题之一。

第三，黑客攻击、恶意代码对重要信息系统安全造成严重影响。重要信息系统一旦遭受攻击者攻击或恶意代码侵害，后果将十分严重，轻则导致系统瘫痪，影响社会和经济活动，重则造成大范围动荡。近年来发生的网络与信息安全事件表明，黑客攻击、恶意代码对我国重要信息系统的危害已成现实威胁。黑客攻击正在从以往单纯的、零散的技术活动，向有组织、趋利性、规模化和跨国流动性的方向发展，尤其是以获取经济利益为目的的信息技术犯罪增长迅速。

## 第三节　中华人民共和国网络安全法

为遏制日益猖獗的网络犯罪活动，完善互联网监管体制刻不容缓。《中华人民共和国网络安全法》（以下简称《网络安全法》）由全国人民代表大会常务委员会于2016年11月7日发布，自2017年6月1日起施行。其立法说明中清晰而明确地阐述了如何在现有条件下，尽力尝试将已有的网络安全实践上升为法律制度，并使其符合中国的网络空间安全需求。其中，有以下一些特色比较鲜明的描述。

其一，明确了我国维护网络空间安全以及参与网络空间国际治理所坚持的指导原则是网络主权原则，并在第二章提出了有关国家网络安全战略和重要领域安全规划等问题的法律要求。这体现出中国在国家网络安全领域的明晰战略意图，不仅能够提升中国保障自身网络安全的能力，还有利于中国与其他国家或行为主体就网络安全问题展开有效的战略博弈。

其二，明确了保障关键信息基础设施安全的战略地位和价值。保障关键信息基础设施安全，在公布的《网络安全法》中占据了相当大的篇幅，第三章第二节专门用于规范关键信息基础设施的安全。此次列入关键信息基础设施范围涉及国家安全、经济安全和保障民生等领域，具体范围包括基础信息网络、重要行业和领域的重要信息系统、军事网络、重要政务网络、用户数量

众多的商业网络等。保障关键信息基础设施的安全，从全球各国的实践来看，是国家网络安全战略中最为重要和主要的内容，这与人们日常生活对网络关键基础设施的强烈依赖密不可分。有效地识别和分析威胁的来源，并采取相应的安全保障措施，是成功保障关键信息基础设施的关键。

其三，在国家网络安全监测预警与应急处置方面，《网络安全法》进行了有益的尝试。其中，第五十一条规定：国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。第五十二条规定：负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。第五十三条规定：国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。第五十五条规定：发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。第五十六条规定：省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

## 第四节　国家网络空间安全战略

为进一步深化推进我国网络空间安全保障工作，2016 年 12 月 27 日，经中央网络安全和信息化领导小组批准，国家互联网信息办公室发布我国首部《国家网络空间安全战略》（以下简称《网络空间战略》）。《网络空间战略》作为我国网络空间安全的纲领性文件，重点分析了目前我国网络安全面临的“七种机遇和六大挑战”，提出了国家总体安全观指导下的“五大目标”，建立了共同维护网络空间和平安全的“四项原则”，制定了推动网络空间和平利用与共同治理的“九大任务”。

### 1. 五大目标

国家的总体安全观是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。《网络空间战略》提出了在总体国家安全观指导下，通过统筹国内、国际两个大局和统筹发展、安全两件大事的基础上，推进网络空间“和平、安全、开放、合作、有序”的发展战略目标。

“和平与安全”是构建“开放、合作、有序”网络空间的前提，维持国际和平与安全是《联合国宪章》的宗旨，只有在“和平与安全”得到充分保证的前提下，才能构建“开放、合