国家安全知识简明读本

信息安全

黄日涵◎著

INFORMATION
SECURITY

国际文化出版公司

国家安全知识简明读本

信息安全

黄日涵　著

国际文化出版公司

·北京·

图书在版编目（CIP）数据

信息安全/黄日涵著. —北京：国际文化出版公司，2013.6
（国家安全知识简明读本）
ISBN 978-7-5125-0288-8

Ⅰ.①信… Ⅱ.①黄… Ⅲ.①信息安全-国家安全-基本知识-中国 Ⅳ.①D631

中国版本图书馆CIP数据核字（2013）第060550号

国家安全知识简明读本·信息安全

作　　者	黄日涵
责任编辑	李　璞
特约策划	马燕冰
统筹监制	葛宏峰 刘　毅 刘露芳
策划编辑	周　贺
美术编辑	李丹丹
出版发行	国际文化出版公司
经　　销	国文润华文化传媒（北京）有限责任公司
印　　刷	三河市华晨印务有限公司
开　　本	700毫米×1000毫米　16开
	10印张　140千字
版　　次	2014年9月第1版
	2014年9月第1次印刷
书　　号	ISBN 978-7-5125-0288-8
定　　价	29.80元

国际文化出版公司
北京朝阳区东土城路乙9号　邮编：100013
总编室：（010）64271551　传真：（010）64271578
销售热线：（010）64271187
传真：（010）64271187-800
E-mail：icpc@95777.sina.net
http://www.sinoread.com

目 录

国家安全知识简明读本

信息安全

黄日涵　著

国际文化出版公司

·北京·

图书在版编目（CIP）数据

信息安全/黄日涵著. —北京：国际文化出版公司，2013.6
（国家安全知识简明读本）
ISBN 978-7-5125-0288-8

Ⅰ.①信… Ⅱ.①黄… Ⅲ.①信息安全-国家安全-基本知识-中国 Ⅳ.①D631

中国版本图书馆CIP数据核字（2013）第060550号

国家安全知识简明读本·信息安全

作　　者	黄日涵
责任编辑	李　璞
特约策划	马燕冰
统筹监制	葛宏峰 刘　毅 刘露芳
策划编辑	周　贺
美术编辑	李丹丹
出版发行	国际文化出版公司
经　　销	国文润华文化传媒（北京）有限责任公司
印　　刷	三河市华晨印务有限公司
开　　本	700毫米×1000毫米　16开 10印张　140千字
版　　次	2014年9月第1版 2014年9月第1次印刷
书　　号	ISBN 978-7-5125-0288-8
定　　价	29.80元

国际文化出版公司
北京朝阳区东土城路乙9号　邮编：100013
总编室：（010）64271551　传真：（010）64271578
销售热线：（010）64271187
传真：（010）64271187-800
E-mail：icpc@95777.sina.net
http://www.sinoread.com

目 录

第一章　信息安全概论

进入21世纪以来，随着全球信息技术的不断发展，信息技术对社会生活的影响也日益深化，信息安全的内涵也在不断发展。人们对信息安全的认识经历了最初强调信息保密的通信保密时代，到强调信息的完整性、可靠性、可用性的信息安全时代。随着计算机技术的不断进步，信息安全的内涵和范围也逐渐从政治、军事领域扩大到了各个行业，并逐渐成为国家安全的核心组成部分。

第一节　信息安全概念的界定

在古代汉语中，并没有“安全”这个单独的词语，但是“安”字却在许多场合下表达着现代汉语中“安全”的意义，表达了人们通常理解的“安全”这一概念。“安全”这个词语在当今社会表现出来的基本含义为：“远离危险的状态或特性”或者是“客观上不存在威胁”、“主观上不存在恐惧”。在全世界各个领域都存在安全问题，安全是一个普遍存在的问题。

信息一般情况下是指通过在数据上施加某些约定而赋予这些数据的特殊含义。一般意义上，信息是指事物的一种属性，在引入必要的约束条件后可以形成特定的概念。人们对于信息安全的认识是随着互联网的普及而不断发展的，信息的内涵及意义因时代的不同而不同，人们对信息安全的认识也有一个发展和变化的过程，早期的信息安全主要指的是政治领域或者是军事领域，因此信息安全工作也被蒙上了一层神秘的面纱。到了21世纪，每个民众都可能面临信息安全问题，信息安全的涉及领域也更为宽泛，因此社会各界开始加大在信息安全领域的研究。

对于信息安全概念的界定我们一般从狭义和广义两个方面来理解。狭义的信息安全是指信息自身的安全问题，指信息的整体状态安全以及信息状态转移安全，基本包括信息的机密性、可靠性、可控性、有用性及完整性五个方面。广义的信息安全主要是指信息系统的有序性和稳定性。它是指一个国家的信息技术体系以及社会信息化不受外来的侵害或威胁，以维持国家政治、经济、军事、文化、科技、社会生活等系统不受内外环境威胁、干扰、破坏而正常运行的状态。由此可见，广义的概念已经把信息安全上升到国家安全的高度，涵盖了综合国家安全中的各个要素，使得信息安全成为一个复杂而又全面的综合性系统。

进入了21世纪以来，信息安全的定义也随着信息技术的进步而动态发展。有一种观点认为，信息安全就是计算机安全延伸；另一种观点是

从国家安全的角度出发，认为信息安全是指一个国家的信息化状态不受到外来的威胁与侵害，或者是一个国家的信息技术体系不受到外来的威胁与侵害。

根据上述信息安全的定义，一般情况下而言，信息安全的首要任务，是指采取技术手段以及有效管理的方法让信息资产免遭威胁，或者将威胁带来的后果降到最低程度，以此维护组织的正常运作。[1] 所以，凡是涉及保密性、可追溯性、可用性、完整性、可靠性和真实性保护等方面的技术和理论，都是信息安全所要研究的范畴，也是信息安全所要实现的目标。

第二节　信息安全的主要内容

在互联网时代下的国家安全中，信息安全已经上升到一个至关重要的地位。信息安全不仅关系到国家层面的重大安全，也与普通百姓的生活息息相关。我们在本书中讨论的信息安全主要是指综合性的信息安全，涉及政治、经济、军事、文化、科技、思想文化、社会稳定、生态环境等各个领域，是一个复杂全面的综合性系统，随着信息化程度的日益加深，信息安全已经上升到了一个全局性的战略高度。如下图所示：

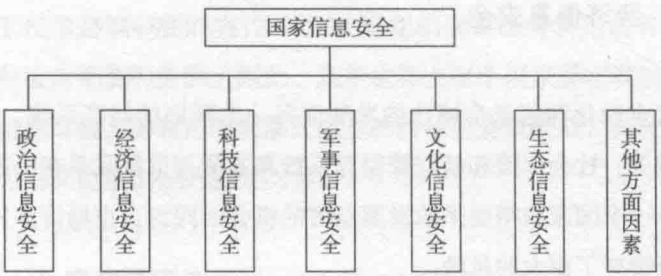

图1-1　国家信息安全系统

通过上图我们可以知道国家信息安全的构成是丰富多样的，涉及方方

[1] 袁峰：《点击未来军事热点》，《解放军报》网络版（www.pladaily.com.cn）。

面面的内容。所以随着互联网与计算机技术的飞速发展，国家信息安全中产生的新热点依然值得我们不断深入思考、努力发掘规律、逐步指导实践。

信息技术革命的飞速发展，使得信息网络渗透到了国家社会生活的各个领域，信息安全问题也在各领域逐步显现出来。在信息时代中信息安全是国家安全中最突出、最核心的问题，无论在国家的哪个领域，其安全的核心就是信息技术及其内容——信息。

一、政治信息安全

通常来说，政治活动对于一个国家来说是最重要的活动，政治信息往往与政府的稳定、前途甚至命运密切相关。政治信息公开化的状况对于信息安全来说如同一把双刃剑，一方面推动了现代民主的发展，另一方面也带来了很强的负面效应，即国家的政局稳定、政府形象极易受到外部势力的侵蚀。敌对国家可以利用先进的媒体手段，尤其是大型的跨国互联网企业，对一国的政治施加有效的影响，甚至控制一个国家的政治舆论，从而达到颠覆对方政权的目的。2011 年爆发的“阿拉伯之春”就是一个典型的案例。

二、经济信息安全

经济全球化和信息全球化的发展使每一个国家的经济系统，如金融、银行、税务、社会保险和航空管制等系统都紧紧与世界联系在一起，在全球化给予一个国家获得更多的发展经济的机会的同时，也给许多国家经济信息安全带来了更大的风险。

三、军事信息安全

21 世纪，全民进入了网络时代，由于信息网络技术的普及，人们的

信息触角大大延伸，给国家信息安全带来了严峻的挑战。国家军事信息失去以往深墙高院的有形保护，而代之以还远未成熟的无形防火墙保护。美国作为军事信息技术发展得最早、信息安全技术最为发达的国家，其军事信息系统仍经常受到网络间谍和计算机病毒的攻击和破坏，更不用说信息技术较为落后的发展中国家。

四、文化信息安全

人类社会信息化程度的提高并未弥合不同文化之间的矛盾与差异。信息网络技术的发展给文化信息的传播与交流带来了革命性的变化。同时，与文化相互封闭时期相比，文化自我保护的难度也加大了。特别是进入21世纪以来，美国凭借国内先进的互联网信息技术，通过大型互联网公司，如Google、Facebook、Twitter等，大力推行“网络文化入侵”以及“网络文化扩张”，使发展中国家的文化信息安全受到空前威胁。

五、科技信息安全

科学技术是第一生产力，对于21世纪的国家综合实力而言，科技信息是一种极为重要的资源。因此，几乎世界上每个国家都在设法搜集别国的科技信息情报，国家之间也展开激烈的科技信息情报战，科技信息安全已经成为国家信息安全的重要内容。

六、生态信息安全

生态环境信息主要指人类对生态环境的监测记录和国家面对生态恶化状况所作出的反应，又被称为“绿色安全”或“生态安全”。目前，本着维护世界生态平衡、保障生态环境的目标，在这个领域世界各国之间基本

呈现一种良好合作的态势。

第三节　信息安全的基本特征

进入21世纪，互联网科技高速发展，极大地缩短了国与国之间、区域与区域之间的空间以及心理距离，带来了全世界生产、生活方式翻天覆地的变化。因此，以全球相互依存为特色的多中心点国际体系在信息化社会日益彰显。[1] 这种特色也使人类互惠性不断增强，一个“全球社会”正逐步呈现在大家眼前。

由于全球互联网技术的高速发展，在网络时代下的国家信息安全也出现了许多新的特征。在这个全新的信息社会，网络已经成为支撑社会政治、经济和生活正常运转的基石，接下来我们就来具体看看信息安全的基本特征。

一、信息安全威胁的广泛性

2012年7月19日，中国互联网络信息中心（CNNIC）在京发布了《第30次中国互联网络发展状况统计报告》（以下简称《报告》）。《报告》显示，截至2012年6月底，中国网民数量突破5.38亿，2012年上半年新增网民2450万，互联网普及率达到39.9%。中国目前有网站342万家，域名873万个，截止2012年11月新浪微博注册会员突破4亿。

总结过去五年中国网民增长情况，从2006年互联网普及率升至10.5%开始，网民规模迎来一轮快速增长，平均每年普及率提升约6个百分点，尤其在2008年和2009年，网民年增长量接近9000万。

可以说，社会已经开始进入了全民网络时代，互联网将国家的信息系统连接在一起，网络用户可以在世界上任何一个网络接入点连接互联网，

[1] 刘超：《信息时代国际关系理论探析》，载《欧洲》2001年第6期。

访问其他网络用户。理论上来说攻击者可以在任何一点发动攻击，任何一点也都可能是被攻击的目标。网络把全球无缝地连接在一起，安全威胁的广泛性也使得发动网络攻击的后果往往是双方或多方无一幸免，从而形成全球即时扩散和“蝴蝶效应”，这就使信息安全问题变得更具广泛性。

二、信息安全威胁的灾难性

随着网络的普及和政府上网工程的启动和发展，各级政府部门、军事、能源、金融、交通、通讯等方面都建立了自己的信息网络系统。信息安全问题关系着整个社会的正常运转与稳定，信息技术和网络已经成为整个社会各行业生产、发展的重要基础，一旦这些信息系统遭到破坏，将会对国家安全稳定、企业生产发展、个人工作生活产生极强的破坏性，造成灾难性的后果，危害到国家安全与稳定。

三、信息安全威胁的高智能性

网络技术是科技发展和进步的产物。以往谈论的安全问题，较多地体现为物理手段之间的对抗，通常是指通过武力方式进行的军事斗争。但是随着互联网的普及，通过网络进行的各种斗争更多地表现为信息技术的对抗，对网络和信息的攻击和窃取是通过信息技术手段来实现的，是高智能的对抗，这些年提到的很多的“网络战争”“网络间谍”，就是这种情况。

四、信息安全威胁的隐蔽性和机动性

在网络普及的前提下，网络攻击对攻击者来说具有隐蔽性和机动性的特点，攻击者可以以较低的成本对目标进行网络攻击、信息窃取、终端控制、篡改和破坏信息，因此攻击活动的隐蔽性和活动性很强。他们远离对

方国土疆域，不必冒生命危险，攻击者在暗处，而防守方在明处被动防御，付出巨大的成本。通过网络攻击有时可以达到在常规军事斗争中需要付出诸多生命和大量财物等巨大代价才能达到的战略目标。

五、信息安全威胁来源的多样性和防范对象的不确定性

信息安全威胁来源和安全防范对象的多元性、模糊性，使安全限界的确定变得十分困难，并对信息安全防护工作提出了前所未有的挑战。传统的国家安全中，有能力对国家的军事和政治安全构成威胁的主要是国家的敌对国家和敌对组织，并且一个国家非常清楚地知道谁对其国家安全构成了威胁。如果一个国家受到了攻击，也能很快确定攻击是由谁发动的，进而采取有针对性的措施。但是，在国家生活日益信息化的今天，上述情况发生了极大的变化。在信息社会中，公用和私人网络互联，军用和民用网络互联，各国之间的网络都已联为一体，各类用户数量极大。信息科技的迅速发展和扩散，使得许多非政府组织、跨国公司、与宗教和种族有关的激进组织、恐怖势力、犯罪集团甚至是个人具有了运用高科技的能力。当他们为了达到自己的非法目的或者对一个国家的政策不满时，就可以运用各种信息武器，通过信息网络对国家的信息系统发动攻击。

当攻击发生时，你很难分清楚攻击是来自国内还是国外，是来自国家、组织还是个人，攻击的具体原因是什么。信息安全攻击源的多样性和防范对象的不确定性，使得信息安全攻击更加难以防范。