互联网基础研究丛书 | 北京市互联网信息办公室 编

互联网信息安全与监管技术研究

中国社会科学出版社

互联网基础研究丛书

互联网信息安全与监管技术研究

北京市互联网信息办公室　编

中国社会科学出版社

图书在版编目（CIP）数据

互联网信息安全与监管技术研究 / 北京市互联网信息办公室编. —北京：中国社会科学出版社，2014.4

ISBN 978-7-5161-4136-6

Ⅰ. ①互… Ⅱ. ①北… Ⅲ. ①互联网络—信息安全—研究 ②互联网络—监管制度—研究 Ⅳ. ①TP393

中国版本图书馆CIP数据核字（2014）第066713号

出 版 人 赵剑英
策划编辑 李寡寡
责任编辑 王 斌
责任校对 姚 颖
责任印制 王 超

出 版 中国社会科学出版社
社 址 北京鼓楼西大街甲158号（邮编 100720）
网 址 http://www.csspw.cn
中文域名：中国社科网 010—64070619
发 行 部 010—84083685
门 市 部 010—84029450
经 销 新华书店及其他书店

印刷装订 三河市君旺印务有限公司
版 次 2014年4月第1版
印 次 2014年4月第1次印刷

开 本 710×1000 1/16
印 张 23.5
插 页 2
字 数 361千字
定 价 69.00元

凡购买中国社会科学出版社图书，如有质量问题请与本社联系调换
电话：010—64009791

编委会

序

2014年2月27日，中央网络安全和信息化领导小组在北京成立，中国互联网迎来了划时代的转折点。习近平总书记在会上强调指出，要“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”。这不仅确立了我国互联网发展的新的更高目标，还吹响了向网络强国进军的伟大号角。站在时代的交汇点上，面对浩浩荡荡的世界互联网发展大潮，实现建设网络强国的宏伟蓝图，不仅需要宏观上的顶层设计、市场上的开拓进取，更需要理论上的不断求索。

思想是行动的先导，理论是实践的指南，互联网的发展离不开互联网的理论研究。互联网理论研究应坚持战略思维、科学精神和问题导向，整体规划，合力攻关，锐意创新。但纵览我国当前互联网研究，个体研究的多，集体研究的少；技术层面研究的多，理论层面研究的少；微观层面研究的多，宏观层面研究的少。推进互联网科学发展、建设网络强国的战略目标，既需要我们从宏观上科学把握互联网的本质特点、基本规律和发展趋势，科学阐明互联网在人类社会发展进程中的战略地位、重要作用和深刻影响，科学揭示我国互联网所处的时代方位和阶段性特征，科学探索中国特色互联网发展建设管理道路，也需要从中观上深入分析影响和制约我国互联网工作的根本因素和难点问题，深入研究我国互联网的法律法规、产业政策、商业模式、管理机制，还需要从微观上追踪互联网新技术、新应用的前沿，探寻网络传播、产品服务和网民需求的特点，力争在基础研究上取得新突破，在理论创新上取得新进展，并将研究成果转化为指导推动我国互联网治理体系和治理能力现代化的科学理论，转化为适合我国互联

网发展建设管理的科学政策，进而更好地推动我国网络强国建设伟大进程。

北京是中国“网都”，在网络强国建设进程中肩负着重要使命。北京市互联网信息办公室秉持历史责任，发扬首善精神，扛起“整合研究资源、搭建研究平台、研究行业问题、促进行业发展”的大旗。在充分调研论证的基础上，我们围绕互联网立法、赢利模式、信息安全、关键技术等方面的问题，于2013年4月确立了“互联网基础研究”系列课题，并分别组织中国人民大学、工业与信息化部、电信研究院等科研机构专家在相关领域开展深入研究。

在此基础上，我们组织编撰了互联网基础研究丛书：《国内外互联网立法研究》深入探讨了国内外互联网立法的现状，指陈各自的利弊得失；《互联网信息安全与监管技术研究》重在研究我国互联网监管领域的热点难点，并对全球主要国家互联网信息安全战略与监管手段进行了深入分析；《互联网赢利模式研究》通过考察当前互联网的十二种赢利模式，深刻阐述了各种赢利模式的经营理念及具体运作；《互联网接入服务现状及管理对策研究》回顾了全球互联网接入服务发展现状及经验启示，总结了我国互联网接入服务发展现状及存在的问题。四部研究专著均针对各自领域的难点问题，提出了建设性的对策建议。希望通过互联网基础研究丛书的出版，助力科研成果转化，启迪网络强国建设，指引未来发展方向。

《数字化生存》作者尼葛洛庞帝有一句名言：“预测未来的最好办法就是创造未来。”纵观社会发展的每一次进步，人类开创的每一个未来，都离不开对事物规律趋势的精准洞察，对科学真理的执着追求。这既是理论研究的基础，也是实干兴邦的根本，更是贯穿于整个历史的成功真谛。

变化的是环境，不变的是探索。让我们共同思考互联网未来，携手推进互联网建设，共同分享网络强国的荣光。

是为序。

首都互联网协会会长　佟力强

2014年4月9日

目 录

第一章 互联网信息安全与监控需求概述

目前，信息化、网络化已经成为整个世界发展的必然趋势，包括中国在内的所有国家都无法置身于这个潮流之外。互联网时代的到来，网络信息技术的广泛应用，尤其是随着移动互联网的迅猛发展，网络信息安全问题也得到了更为广泛的关注。据统计，在党的十八大报告中有多处明确提及信息、信息化、信息网络、信息技术与信息安全，并且首次明确提出了“健全信息安全保障体系”的目标。毫无疑问，网络空间已经成为继领土、领海、领空之后的“第四空间”，它将直接对现实空间起到制约作用，其战略地位远在领土、领海和领空之上。网络空间作为国家主权延伸的新疆域，成为了整个国家和社会的“中枢神经”，其战略地位日趋重要。2014年2月27日，中央网络安全和信息化领导小组宣告成立，中共中央总书记、国家主席、中央军委主席习近平亲自担任组长，李克强、刘云山任副组长，再次体现了中国最高层全面深化改革、加强顶层设计的意志，显示出在保障网络安全、维护国家利益、推动信息化发展方面的决心。因此，做好互联网信息安全工作已经成为互联网时代最突出、最核心的国家战略问题；了解、认识、维护互联网信息安全，已经成为每个公民的责任和应尽的义务。

在本章我们将结合信息安全的概念、属性、发展历程等，重点分析新时期下的互联网信息安全的需求。

第一节 信息安全概念

一 信息社会需要信息安全

20世纪80年代，世界著名未来学家阿尔文·托夫勒推出了“20世纪最有影响力的杰作之一”的《第三次浪潮》一书。在书中，他将人类发展史划分为第一次浪潮的“农业文明”、第二次浪潮的“工业文明”以及第三次浪潮的“信息社会”，给历史研究与未来思想带来了全新的视角。这一被称为历史上重大变革的信息社会，代表着人类经济社会开始在农业社会、工业社会之后发生巨大变化，信息技术和信息产业在经济和社会发展中的作用日益加强，并逐步开始发挥主导作用。进入21世纪，信息化对信息社会经济社会发展的影响愈加深刻。世界经济发展进程加快，信息化、全球化、多极化发展的大趋势十分明显。信息化被称为推动现代经济增长的发动机和现代社会发展的均衡器。信息化与经济全球化，推动着全球产业分工深化和经济结构调整，改变着世界市场和世界经济竞争格局。

作为20世纪人类最伟大的发明之一，互联网正逐步成为信息时代人类社会发展的战略性基础设施，推动着生产和生活方式的深刻变革，进而不断重塑经济社会的发展模式，成为构建信息社会的重要基石。历经多年发展，中国互联网已成为全球互联网发展的重要组成部分。互联网全面渗透到经济社会的各个领域，成为生产建设、经济贸易、科技创新、公共服务、文化传播、生活娱乐的新型平台和变革力量，推动着中国向信息社会发展。根据中国互联网信息中心（CNNIC）公布的统计数据，截至2013年12月底，中国网民规模达到6.18亿，比2012年底增加5358万，普及率达到53.8%。值得一提的是，截至2013年12月底，中国手机网民规模达5亿，比2012年增加8009万人，网民中使用手机上网的人群占比提升至81.0%。互联网普及率为45.8%，较2012年底提升3.7%。

图 1—1　中国网民与互联网普及率（来源：CNNIC）

图 1—2　2007—2013 年手机网民在网民中占比情况（来源：CNNIC）

另据中国国务院新闻办公室 2010 年 6 月 8 日发表的《中国互联网状况》白皮书披露，从 1994 年到 2010 年的 16 年间，中国信息产业年均增速超过 26.6%，占国内生产总值的比重由不足 1% 增加到 10% 左右。而据工信部数据，2012 年中国电子产品进出口总额达到 11868 亿美元，其中物联网产业市场初具规模，移动数据和互联网业务发展迅猛。网络广告在所有媒体广告中增幅速度最高。预计“十二五”期间，中国互联网服务业收入年均将

增长超过25%，突破6000亿元。

随着互联网技术发展与产业化的推进，“新、旧”主流媒体转向移动化传播，中国主流新闻网站在2012年也加快了改制上市步伐，主流媒体正在由传统媒体转向新兴媒体，由提供内容转向提供产品和服务，以顺应新兴媒体发展的大势，并积极抢占微博、微信等新媒体平台。根据中国互联网信息中心CNNIC的数据，截至2013年12月，中国拥有4.9亿搜索引擎用户，4.53亿网络音乐用户，4.28亿网络视频用户，3.38亿网络游戏用户，2.81亿微博用户，2.78亿社交网络用户，2.59亿电子邮件用户，3.02亿网络购物用户，2.74亿网络文学用户，2.50亿网上银行用户，2.60亿网上支付用户。

从上面的数据可以看出，互联网已经成为最快捷的信息传递通路与公民言论表达的重要阵地，网络文化与商业创新已经成为中国文化产业的重要组成部分。一方面，当前与社会生活联系紧密的应用，如网络媒体、网络通信、移动社交、网络娱乐、电子政务、网络购物、电子支付类应用等不断丰富发展；另一方面，网络应用的专业性大大加强，专业服务与行业应用已经成为互联网应用发展的重要趋势。基于宽带和移动网络与终端的新媒体应用发展很快，如微信推出不到2年注册用户就达3亿。此外，宽带的发展和三网融合的推进极大带动了网络音乐、网络视频、网络游戏等娱乐应用的增长。新兴媒体应用不仅满足信息获取、游戏娱乐、交流沟通、购物消费等方面的需要，也进一步推动新兴媒体成为中国的社会化、信息化平台，并形成了极具中国特色的传播生态。

随着中国进入信息社会时代，我们在分享信息化带来的巨大成果的同时，也在面临着越来越多的信息安全问题，其中网络信息安全问题尤为重要。近年来，中国的网络犯罪呈上升趋势，各种传统犯罪与网络犯罪结合的趋势日益明显，网络诈骗、网络盗窃等侵害他人财产的犯罪增长迅速，制作传播计算机病毒、入侵和攻击计算机与网络的犯罪日趋增多，利用互联网传播淫秽色情及从事赌博等犯罪活动仍然突出。据统计，1998年公安机关办理各类网络犯罪案件142起，2007年增长到2.9万起，2008年为3.5万起，2009年为4.8万起。据不完全统计，2009年中国被境外控制的计算机IP地址达100多万个，被黑客篡改的网站达4.2万个，被“飞客”蠕虫网

络病毒感染的计算机每月达1800万台，约占全球感染主机数量的30%。[①]特别是2013年6月份引爆的“棱镜门事件”，进一步暴露了中国在信息安全方面存在的诸多隐患。事实再次证明，如果不能保障信息安全，将直接影响中国在军事、经济等诸多领域的战略安全。透过“棱镜门事件”，我们需要对国家的信息安全体系建设进行更为冷静的再思考。

那么，什么是信息安全？怎么理解互联网时代的信息安全？接下来我们将进行简单的介绍。

二　信息安全的概念与属性

自从人类诞生以来，信息交流就是人类一种最基本的社会行为，是人类其他社会活动的基础，自然也就出现了对于信息交流的各种质量属性的期望。比如，在面对面的交流中，我们可能会关心对方的话是不是真的，自己的话对方是不是听清楚了，我们之间的谈话是否被人听到了等等。这即是对于信息的完整性和保密性的日常体现。因此，信息安全的需求自古以来就存在，只是进入信息社会以来，政治、经济、军事以及社会生活对于信息安全的需求日益增加，其内涵也在不断深化，外延不断拓展。

目前，业界对于信息安全尚无公认和统一的定义。一般而言，信息安全（Information Security）是指网络与信息系统正常运行，防止网络与信息系统中的信息丢失、泄露以及未授权访问、修改或者删除。在很多资料中，信息安全这一概念经常与计算机安全、信息保障等术语被不正确地互相替换使用。毫无疑问，这些领域相互关联，并且拥有一些共同的目标——保护信息的机密性、完整性、可用性，然而，它们之间仍然有一些微妙的区别。比如，信息安全主要涉及数据的机密性、完整性、可用性，而不管数据的存在形式是电子的、印刷的还是其他的形式；计算机安全则主要关注计算机系统的可用性及正确的操作，而并不关心计算机内存储或产生的信息。因此，准确地理解信息安全，就要全面地了解信息安全的几个基本属性。

---

① 国务院新闻办公室：《中国互联网状况》白皮书，2010年。

一般而言，信息安全的属性主要包括信息的保密性、完整性、可用性、可控性与可靠性等五个方面。[①]

保密性：指信息不泄露给非授权的用户、实体或进程，或被其利用的特性。这一点在军用网络系统中体现得最为明显，因此其对于密码、涉密网络与公共网络隔离等有着与传统商用网络更高级的安全要求。

完整性：指信息未经授权不能进行更改的特性。即信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、插入的特性，而破坏信息的完整性往往是对网络信息安全发动攻击的最终目标。

可用性：指信息可被授权用户或者实体访问并按照需求使用的特性。例如，在授权用户或实体需要信息服务时，信息服务应该可以使用，或者是信息系统部分受损或需要降级使用时，仍能为授权用户提供有效服务。比如，通过病毒或者黑客等发起的对于网络或者系统的攻击，即属于针对可用性的攻击。

可控性：指授权机构可以随时控制信息的机密性。比如，美国和一些国家曾经提出的“密钥托管”、“密钥恢复”等，就是实现信息安全可控的例子，其具有防抵赖性、便于政府监听以及可恢复等特性。

可靠性：主要指信息或者系统能够按照用户约定的质量连续为用户服务的特性，包括信息的迅速、及时、准确和连续地转移等。

因此，信息安全也可以说是采用一切方法和手段来保障信息上述五种属性安全。当然，也有不少资料在谈及信息安全时更侧重信息安全的保密性、完整性和可用性，但其也是强调信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。随着信息社会的发展，信息安全的概念也在不断发生变化，了解信息安全的发展历程有助于我们更全面地认识信息安全。

① 沈昌祥，左晓栋：《信息安全》，浙江大学出版社2007年版。

第二节 信息安全的发展历程

一 传统的信息安全

1.通信安全

据说最早的信息安全可以追溯到2000多年前，即公元前50年恺撒大帝发明了恺撒密码，它被用来防止秘密的消息落入错误的人手中时被读取。不过，真正意义上的信息安全是从第二次世界大战开始出现的，这场几乎席卷全球的战争虽然使8000多万人死亡，并给全球经济造成了巨大损失，但也使得信息安全研究取得了许多进展，并逐渐成为一门专业的学科。

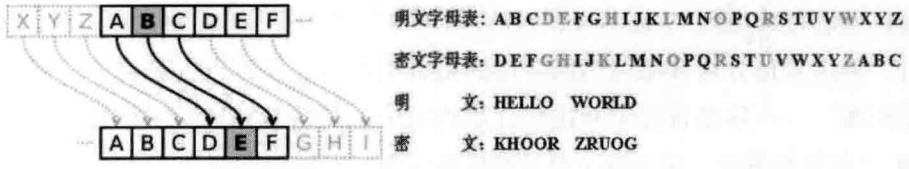

图1—3 恺撒密码示意图（来源：红黑联盟）

有人把这一阶段称为信息安全的通信安全时代，而这一时代的标志就是1949年香农发表的《保密系统的信息理论》。该理论将密码学的研究纳入了科学的轨道，虽然当时其主要关注者集中在军队和政府部门，其主要目的是确保通信内容的保密性，防止非授权人员获取通信信息，同时保证通信的真实性。在通信保密阶段，保密性成了信息安全保护最基本的目标之一，其主要技术手段有信息加密、防侦收、防辐射、物理保密、信息隐藏等。其中，信息加密是指使用密码技术对于信息进行加密处理，即使对手得到加密的信息也会因为没有密钥而无法读取；防侦收是指通过技术手段让对手侦收不到有用的信息；防辐射是防止有用信息通过各种途径辐射出去，主要是做好内部保密机制；物理保密是利用隔离、掩蔽等各种物理方法保护信息不被泄露；信息隐藏是网络环境下把机密信息隐藏在大量信息中不让对

方发觉的一种方法，其与图像叠加、数字水印、潜信道、隐匿协议等理论与技术紧密相关。

总之，这一阶段通信技术还不发达，面对电话、电报、传真等信息交换过程中存在的安全问题，人们强调的主要是信息的保密性，对安全理论和技术的研究也只侧重于密码学，这一阶段的信息安全可以简单称为通信安全，即 COMSEC（Communication Security）。[①]

2. 计算机安全与信息系统安全

20 世纪 60 年代后，半导体和集成电路技术的飞速发展推动了计算机软硬件的发展，计算机和网络技术的应用进入了实用化和规模化阶段，人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标的信息安全阶段，即 INFOSEC（Information Security）。其标志就是 1977 年美国国家标准局公布的《数据加密标准》，以及 1985 年美国国防部公布的《可信计算机系统评估准则》。据考证，“计算机安全”概念是在 1969 年提出的。当时，美国兰德公司在给美国国防部的报告中指出“计算机太脆弱了，有安全问题”——这是首次公开提到计算机安全。在当时和其后的相当一段时间，“计算机安全”的内涵主要是指实体安全，即物理安全。

到了 20 世纪七八十年代，由于各类计算机管理系统开始发展，各种应用开始增多，“计算机安全”开始逐步演化为“计算机信息系统安全”。这时候“安全”的概念已经不仅仅是计算机硬件等实体的安全，也包括软件与信息内容等的安全。20 世纪末以及 21 世纪初，随着通信、计算机硬件和软件以及数据加密领域的巨大发展，小巧、功能强大、价格低廉的计算设备使得对电子数据的加工处理能为小公司和家庭用户所负担和掌握。这些计算机很快被通常称为因特网或者万维网的互联网连接起来，在互联网上快速增长的电子数据处理和电子商务应用，以及不断出现的国际恐怖主义事件，增加了对更好地保护计算机及其存储、加工和传输的信息的需求。这时，继计算机安全、信息系统安全之后，信息保障的概念开始出现。

① 启明星辰：《信息安全发展历程》，2008年。

3. 信息保障

20 世纪 90 年代开始，由于互联网技术的飞速发展，信息无论是对内还是对外都得到极大开放，由此产生的信息安全问题跨越了时间和空间，信息安全的焦点已经不仅仅是传统的保密性、完整性和可用性三个原则，由此衍生出了诸如可控性、抗抵赖性、真实性等其他的原则和目标，信息安全也转化为从整体角度考虑其体系建设的信息保障（Information Assurance）阶段。这时的“信息安全”概念已经不仅仅是安全防范，而是包含了安全保障的含义，即包括监控、保护、应急处理、恢复等系统性的保障。

信息安全保障，在美国称之为信息保障 IA（Information Assurance）。1996 年美国国防部（DoD）在国防部令 S-3600.1 对信息保障下进行了如下定义：保护和防御信息及信息系统，确保其可用性、完整性、保密性、可认证性、不可否认性等特性。这包括在信息系统中融入保护、检测、反应功能，并提供信息系统的恢复功能。近年来，美国围绕信息保障发布了多项法令和技术指南。比如，《信息保障技术框架》（IATF）确立了“纵深防御”的技术思路，并提出其适用于任何机构的任何信息系统或网络；美国 8500.1 号和 8500.2 号国防部令则分别确立了美军信息保障的政策框架和技术实施要求。因此，信息保障从源头上讲是美军针对复杂战场环境提出的概念，它代表了美军对于信息安全发展阶段的最新认识，虽然这一概念也同样适用于民用信息系统，但是仍然具有很强的军事色彩。

二　新时期的信息安全

随着信息化发展，信息安全的内涵不断深化，外延不断拓展。当前，国民经济和社会发展对信息化高度依赖，信息安全已经发展成为涉及国民经济和社会发展各个领域，不仅影响公民个人权益，更关乎国家安全、经济发展、公众利益的重大战略问题。党的十六届四中全会，将信息安全作为国家安全的重要组成部分，明确提出要“增强国家安全意识，完善国家安全战略”，并确保“国家的政治安全、经济安全、文化安全和信息安全”。在这种大背景下，新的信息安全已经从简单的技术问题上升到了国家政治、