主编 张 曦

非传统安全与现实中国
Non-traditional Security in China

信息安全

Information Security

沈昌祥 左晓栋 著

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

信息安全

Information Security

沈昌祥　左晓栋　著

浙江大学出版社

图书在版编目（CIP）数据

信息安全／沈昌祥，左晓栋著．—杭州：浙江大学出版社，2007.10

（非传统安全与现实中国丛书／张曦，余潇枫主编）

ISBN 978-7-308-05597-0

Ⅰ.信… Ⅱ.①沈…②左…③刘… Ⅲ.信息系统－安全技术 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2007）第 157913 号

信息安全

沈昌祥 左晓栋 著

丛书主持 黄宝忠 陈丽霞
责任编辑 林昌东
封面设计 张志伟
出版发行 浙江大学出版社
（杭州天目山路 148 号 邮政编码 310028）
（网址：http://www.zjupress.com）
（E-mail:zupress@mail.hz.zj.cn）
排　　版 浙江大学出版社电脑排版中心
印　　刷 富阳市育才印刷有限公司
开　　本 787mm×960mm 1/16
印　　张 12.25
字　　数 148 千
版 印 次 2007 年 10 月第 1 版 2007 年 10 月第 1 次印刷
书　　号 ISBN 978-7-308-05597-0
定　　价 20.00 元

总 序

读者手上的这套《非传统安全与现实中国丛书》，不仅仅是中国学界在这一领域推出的第一套丛书，据我所知，它也是亚洲地区头一次以丛书形式出版的非传统安全研究系列，是当今世界不多见的一类成果形式。按照既定的计划，将问世的五本，即《非传统安全与公共危机治理》、《粮食安全》、《信息安全》、《公共卫生安全》、《文化安全》，只是整个丛书的第一辑。如果进展顺利，今后还有更多的成果会与公众见面，涉及范围将逐步扩展到非传统安全研究所有新开拓的分支领域和问题领域，作者队伍不仅可能包括全国各地的专家学者，还将延揽国外在非传统安全研究上有成就的知名人士加盟。潇枫和我本人甚至设想，在各方面的帮助下，并假以时日，以“浙江大学非传统安全与和平发展研究中心”为主要推动单位和研究基地，这套丛书有可能成为中国乃至国际理论界非传统安全研究成果的主要释放窗口，成为衡量全球化时代安全思想充实和发展新阶段、新高度的一个“学术地标”。

非传统安全问题的研究之所以如此“兴师动众”，确实有它的理由：首先，在今天这样一个时代（不论人们用什么词汇或方式概括它），安全问题已越来越多地从传统的军事安全、战场安全及狭义的国家议事的瓶子里“外溢”，蔓延到过去人们无法想像、旧的教科书无法解说、老套办法无法应对的死角与地步；假

使一味听任它的扩张，不顾及、不解决理论（思考）与实践（政策）的脱节，最终各国公众和国际社会可能受到难以想像的厄运惩罚。十年前亚洲金融危机给出的警示之一是：金融领域爆发的强大冲击波，可能造成比一场中等规模的武装冲突更惊人的毁坏。譬如讲，它可以使一个国家的经济倒退一二十年，可以带来社会的严重骚乱和政府的非正常更迭，可以极大地降低公众的自信心和承受度。几年前在中国内地、香港以及新加坡等地刚刚消逝的SARS阴霾，曾经施加我们国家权力中枢所在地前所未有的考验：它不止夺走了数百人的宝贵生命，更以其“查无源、症无药”，以及“来无影、去无踪”的诡异形态，预示着这是一个随时可能再度现身的可怕“妖魔鬼怪”。如果说，学术研究跟不上现实生活的变化，多少还可以理解或辩解；那么，研究工作无视甚至轻视现实生活的挑战，则是不能原谅的。中国是这样大的一个国家，中国在当代的发展又是举世公认的，中国的教学和研究人员当然有义不容辞的义务，直面非传统安全的各种威胁；不这么做，中国算不上是“负责任的大国”，我们的学者也称不上是“有良知的学者”。

其次，非传统安全的研究，属于高难度的系统工程，需要多学科的攻关，更需要广泛的参与和支持。在笔者看来，非传统安全问题的探索不是孤立的工作，也不能与过去的努力截然分割开来，与其说它是对“非传统问题”或“非传统特征”的讨论，不如把它定位为本质上“对安全事务的重新理解和阐释”。这就要求研究者有全新的思考维度，熟练驾驭已有的和正在研制的各种“工具”（既指“传统工具箱”里的各种军事火炮，又指“新式装备库”里的各种软件与技巧），学会应对扑朔迷离、千变万化的对手。举例说，台湾问题既可纳入传统安全的范畴（如何以军事手

段遏制台独势力),又可放进非传统安全的领域(怎样面对认同危机、渔业纠纷、合作对付海上犯罪以及妥善处理“三通”问题,等等),这就需要我们的研究群体能够细致探讨传统与非传统安全间的各种定义及其复杂关系。比如它们之间可能的转换及转换的条件,区分属于不同领域发生、不同力量应付、不同思考方式的各种安全难题。从国际关系理论前沿角度观察,后者恰恰反映出国内外分析人士近年来苦苦探索的焦点与难点所在。上面的讨论同时涉及非传统安全研究的另一个重大分歧点,即:这一分支(学科)的边界何在?是否允许把各种有严重瑕疵的“切片”,都放到数量(资源)有限的(非传统安全)“显微镜”下,排队等候各种代价不菲的“药敏试验”?用一个通俗的比喻,能否可以不加区别地将“信息安全”、“能源安全”、“文化安全”、“粮食安全”、“人口安全”等等问题,与“城镇交通安全”、“医院用药安全”、“沙漠化现象”、“城市水资源短缺”、“上访事件与群发性危机”等等现象,全都放进“非传统安全威胁”这个“大篮子”里?什么时候、什么条件下,把哪些问题放进或拿出这个篮子?在最新的国际关系理论里,这类分析被统称为“安全化”研究,包含了对安全概念怎样定义、包括哪些层次和可变性,什么是安全问题、什么不是安全问题,如何将原本非安全的问题安全化、又如何把已经有安全性质的问题非安全化(“去安全化”)等等一系列十分复杂又相当有趣的命题与解释(尽管尚未定型,谈不上十分成熟)。我再次强调,作为新兴大国的研究群体,中国学者有责任、有义务,在这些复杂、高难度但前景无量的分析领域,进行持续有效的努力,争取自己的话语权并作出独特贡献。

本丛书第一批各本的作者,不妨视为非传统安全研究之高山峻岭前比较早的一批“攀岩者”。一方面,我想指出,他们尽到

了自己的努力，尤其是对涉及“公共安全”领域的某些重大非传统安全现象做了独到而有趣的探究，为后来者提供了跟进、批评和超越的文本，毫无疑问这些工作是可喜可贺的；另一方面，我也要特别说明，这一批书的作者都不是军事安全或传统安全研究的“行家里手”，而是造诣精深的科学家、工程院院士、技术专家，是学有专攻的文化学者和伦理哲学家，因此他（她）们很可能在“传统安全分析家”看来是贸然闯入别人领地的“入侵者”，评价上自然会见仁见智，甚至褒贬不一。在我看来，有争论是好事，是学术进步的前提，非传统安全的研究尤其需要学术指导与争辩，因为它本身即是一个未定型的分支领域。实践和时间才是检验作品真伪的最佳标准。

最后，衷心祝贺《非传统安全与现实中国丛书》的出版，也衷心期盼读者对它的认真阅读和批评！

是为序。

王逸舟*

2007年7月1日

---

* 王逸舟，中国社会科学院研究生院教授、博士生导师，中国社会科学院世界经济与政治研究所副所长，《世界经济与政治》杂志主编，浙江大学非传统安全与和平发展研究中心名誉主任。

目　录

第一章　什么是信息安全　001

一　传统的信息安全概念　002
二　信息化发展使信息安全概念不断深化　006
三　新的信息安全观　011
四　国际社会当前对信息安全的共识　019

第二章　信息安全的非传统安全特征　021

一　威胁的多元性　022
二　攻防的非对称性　039
三　影响的广泛性　047
四　后果的严重性　050
五　事件的突发性　057

第三章　中国国家安全面临的主要信息技术安全风险因素　060

一　基础信息网络和重要信息系统安全防护能力不强　061
二　泄密隐患严重　066
三　信息技术自主可控能力不高　075

四　对外风险意识欠缺,防范措施不够　081
五　信息战阴霾密布　091

第四章　中国国家安全面临的主要信息内容安全风险因素　097

一　挑战意识形态建设　097
二　网络政治动员　100
三　造谣煽动以及恶意炒作　106
四　文化入侵与文化颠覆　113

第五章　中国维护国家信息安全的战略对策　118

一　指导思想　118
二　信息安全保障体系建设　122
三　未来展望　138

第六章　发达国家的主要做法　140

一　战略层面高度重视　140
二　美国维护网络空间安全的有关行动　148

第七章　信息安全领域的国际合作　155

一　主要提议　155
二　《网络犯罪公约》:国际合作的突出成果　164
三　共建全球网络安全文化是大势所趋　168

附　录　170

一　从有关电子标签的两次政协提案审视信息时代的国家安全

利益　170
二　从前苏联经济遭“逻辑炸弹”重创反思引进技术的安全风险　173
三　我国信息安全法律法规现状　176

参考文献　183

后　记　184

第一章
什么是信息安全

信息化是当今世界经济和社会发展的大趋势，是推动经济社会变革和进步的重要力量。人类社会已经进入信息时代，正在分享着信息化带来的巨大成果，但同时也面临着越来越多的信息安全问题。特别是，近年来出现了很多影响较大的信息安全事件，引发了人们对信息安全的空前关注。作为重要的非传统安全因素，信息安全已经成为决定信息化成败，关乎政治稳定、经济发展乃至国家安全的重要课题。

那么，什么是信息安全？怎样理解信息安全？这是信息安全理论研究和实践工作中的基本问题。自有人类以来，信息交流便成为一种最基本的人类社会行为，是人类其他社会活动的基础，自然会出现对信息交流的各种质量属性的期望。例如在面对面的交流中，我们就可能关心，对方的话是不是真的，对方的话我是否听清楚了，我们之间的谈话是否被人听到了。因此，对信息安全的需求一直是普遍存在的，在军事斗争中更上升为决定战争成败的重要因素，其根本目的是确保军事指令不被敌人知悉，同时确保没有被改动过，即确保信息的保密性以及完整性。现代信息技术革命以来，政治、经济、军事和社会生活中对信息安全的需求日益增加，信息安全作为有着特定内涵的信息科学门类逐渐得到重视，其内涵不断深化，外延不断

拓展。

传统的信息安全概念

1. 通信保密

几千年的时间里，军事领域对信息安全的需求使古典密码学得以诞生和发展。到了现代，信息安全首先进入了通信保密阶段。其开始时间约为 20 世纪 40 年代，时代标志是 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。在通信保密阶段，信息安全的关注者主要限于军队和政府，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。

所谓保密性，是指信息不被泄露给非授权的用户、实体或过程，或被其利用的特性。普通人通过邮政系统发信件时，为了个人隐私要装上信封。可是到了信息时代，信息在通信线路上传播时，如果没有装“信封”，那么所有的信息都是“明信片”，不再有秘密可言。因此，保密性是首先出现的信息安全需求，直至今天仍然代表着信息安全保护最基本的目标之一。常用的保密技术包括：防侦收（使对手侦收不到有用的信息）、防辐射（防止有用信息以各种途径辐射出去）、信息加密（使用密码技术对信息进行加密处理。即使对手得到了加密后的信息也会因为没有密钥而无法读懂信息）、物理保密（利用各种物理方法，如限制、隔离、掩蔽、控制等措施，保护信息不被泄露）、信息隐形（将信息嵌入其他客体中，隐藏信息的存在）等。

2. 计算机安全和信息系统安全

进入20世纪70年代，通信保密阶段转变到计算机安全阶段，这一时代的标志是1977年美国国家标准局（NBS）公布的《数据加密标准》（DES）和1985年美国国防部（DoD）公布的《可信计算机系统评估准则》（TCSEC），这些标准的提出意味着解决信息系统保密性问题的研究和应用迈上了历史的新台阶。

进入20世纪80年代后，计算机的性能得到了成百上千倍的提高，应用的范围也在不断扩大，计算机已遍及世界各个角落。而且人们正努力利用通信网络把孤立的单机系统连接起来，相互通信和共享资源。但是，随之而来并日益严峻的问题是计算机信息的安全问题。由于计算机信息有共享和易于扩散等特性，它在处理、存储、传输和使用上有着严重的脆弱性，很容易被干扰、滥用、遗漏和丢失，甚至被泄露、窃取、篡改、伪造和破坏。因此人们开始关注计算机系统中的硬件、软件及在处理、存储、传输信息过程中的保密性。主要手段是通过访问控制，防止对计算机中信息的非授权访问，从而保护信息的保密性。但是，随着计算机病毒、计算机软件Bug等问题的不断显现，保密性已经不足以满足人们对计算机安全的需求，完整性和可用性等新的计算机安全需求于是开始走上舞台。

完整性是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。完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不致受到各种原因

的破坏。一份加密的文件，攻击者虽然无法获知其具体内容，但仍可以随意对其信息进行改动，从而使其不能正常解密。例如，电子文件在网络上传输时其本质是二进制比特流，非授权人员可以很容易接触并修改。影响信息完整性的主要因素有：设备故障、误码（传输、处理和存储过程中产生的误码，定时稳定度及精度的降低造成的误码，各种干扰源造成的误码）、人为攻击、计算机病毒等。保护信息完整性的主要方法有：纠错编码方法（最简单和常用的纠错编码方法是奇偶校验法）、密码校验和方法、数字签名、公证（请求管理或中介机构证明信息的真实性）等。

可用性是信息可被授权实体访问并按需求使用的特性。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。可用性与保密性、完整性有明显的区别。即使信息没有遭到泄露，也没有被改动，但如果不能被需要的人所使用，仍然是一种突出的安全问题，分布式拒绝服务攻击（DDoS）便是一例。

20 世纪 90 年代后，信息系统安全开始成为信息安全的核心内容。通信和计算机技术相互依存，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，互联网成了寻常百姓可及的家用技术平台，安全的需求不断地向社会的各个领域扩展，人们的关注对象从计算机转向更具本质性的信息本身，继而关注信息系统的安全。人们需要保护信息在存储、处理或传输过程中不被非法访问或更改，确保对合法用户的服务并限制非授权用户的服务，确保信息系统的业务功能能够正常运行。

3. 信息保障

20世纪90年代末，对于信息系统的攻击日趋频繁，安全不再满足于简单的防护，人们期望的是对整个信息和信息系统的保护和防御，包括对信息的保护、检测、反应和恢复能力。同时，安全与应用的结合更加紧密，其相对性、动态性等特性日益引起注意，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机制的强度作为评判指标，而是结合了应用环境和应用需求，强调安全是一种信心的度量，使信息系统的使用者确信其预期的安全目标已获满足。

为此，美国军方率先提出了信息保障（IA）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、鉴别、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。"

信息保障除强调了信息安全的保护能力外，还提出要重视提高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引起破坏后的快速恢复能力。它关注的是信息系统整个生命周期的防御和恢复。

近年来，美军围绕信息保障发布了多项法令和技术指南。《信息保障技术框架》（IATF）确立了"纵深防御"的技术思路，并指出其适用于任何机构的任何信息系统或网络。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。

"信息保障"是信息技术发展到今天，美军为确保复杂战场环境中信息和信息系统的安全而提出的概念，代表了美军对信息安全发展阶段的最新认识。这个概念同时也适用于民用信

息系统。就目前来说，虽然美国的军民信息安全合作很多，但“信息保障”仍具有很强的军事色彩。

此外，近年来许多国家和组织也为信息安全作了不同的定义，这些定义的侧重点虽然各有不同，但就技术性而言，多将信息安全归结为信息和信息系统的保密性、完整性和可用性需求。例如美国在2002年《联邦信息安全管理法案》（FISMA）中提出：“术语‘信息安全’指保护信息和信息系统，防止未经授权的访问、使用、泄露、中断、修改或破坏，以提供：（A）完整性，防止对信息进行不适当的修改或破坏，包括确保信息的不可否认性和真实性；（B）保密性，信息的访问和披露要经过授权，包括保护个人隐私和专属信息的手段；以及（C）可用性，确保可以及时可靠地访问和使用信息。”

二 信息化发展使信息安全概念不断深化

当前，全球信息化正在引发世界的深刻变革，各国高度重视信息化进程中的信息安全问题，普遍将信息安全视为国家安全的基石，从国家安全的高度看待和处理信息安全问题。在信息化的推进过程中，信息安全概念有了更广阔的外延，仅仅从保密性、完整性和可用性等技术角度去认识信息安全已经远远不够了。要理解这种变化，理解信息安全与国家安全的关系，就要首先看到国民经济和社会发展对信息化的重要依赖作用。

1. 大力推进信息化是符合历史潮流的战略选择

信息化是充分利用信息技术，开发利用信息资源，促进信

息交流和知识共享，提高经济增长质量，推动经济社会发展转型的历史进程。

20世纪90年代以来，信息技术不断创新，信息产业持续发展，信息网络广泛普及，信息化成为全球经济社会发展的显著特征，并逐步向一场全方位的社会变革演进。进入21世纪，信息化对经济社会发展的影响更加深刻。广泛应用、高度渗透的信息技术正孕育着新的重大突破；信息资源日益成为重要生产要素、无形资产和社会财富；信息网络更加普及并日趋融合；信息化与经济全球化相互交织，推动着全球产业分工深化和经济结构调整，重塑着全球经济竞争格局；互联网加剧了各种思想文化的相互激荡，成为信息传播和知识扩散的新载体；电子政务在提高行政效率、改善政府效能、扩大民主参与等方面的作用日益显著；信息化使现代战争形态发生重大变化，成为世界新军事变革的核心内容。

信息技术已经成为最活跃的生产力要素，成为影响国家综合实力和国际竞争力的关键因素，各国都在通过积极发展信息技术及其产业，抢占世界经济竞争的制高点。我国的工业化任务还没有完成，现代化水平还不高，更应重视信息化在国民经济和社会发展中的倍增器和催化剂作用，加快信息化发展，坚持以信息化带动工业化，以工业化促进信息化，这是我国加快实现工业化和现代化的必然选择。

2. 信息化对我国产生全方位影响

我国党和政府一直高度重视信息化工作。20世纪90年代，相继启动了以“金关”、“金卡”和“金税”为代表的重大信息化应用工程；1997年，召开了全国信息化工作会议；党