国防科技著作精品译丛
网电空间安全系列

Information Warfare

信息战

【法】 Daniel Ventre 著
胡生亮 贺静波 刘 忠 王旭东 卞小林 李 轲 等译

WILEY
国防工业出版社
National Defense Industry Press

装备科技译著出版基金

信息战

Information Warfare

[法] Daniel Ventre 著

胡生亮 贺静波 刘 忠
王旭东 卞小林 李 轲 等译

國防工業出版社
National Defense Industry Press

著作权合同登记　图字: 军 -2013 -011 号

图书在版编目（CIP）数据

信息战 /（法）文彻（Ventre, D.）著; 胡生亮等译.
— 北京: 国防工业出版社, 2013.5
（国防科技著作精品译丛. 网电空间安全系列）
书名原文: Information Warfare
ISBN 978-7-118-08781-9

Ⅰ. ①信… Ⅱ. ①文… ②胡… Ⅲ. ①信息战—研究
Ⅳ. ①E869

中国版本图书馆 CIP 数据核字（2013）第069051号

信息战
[法] Daniel Ventre 著
胡生亮 贺静波 刘 忠 王旭东 卞小林 李 轲 等译

出版发行　国防工业出版社
地址邮编　北京市海淀区紫竹院南路 23 号　100048
经　　售　新华书店
印　　刷　北京嘉恒彩色印刷有限公司印刷
开　　本　700 × 1000　1/16
印　　张　13 3/4
字　　数　199 千字
版 印 次　2013 年 5 月第 1 版第 1 次印刷
印　　数　1—2500 册
定　　价　76.00 元

(本书如有印装错误，我社负责调换)

国防书店: (010) 88540777　发行邮购: (010) 88540776
发行传真: (010) 88540755　发行业务: (010) 88540717

翻译组名单

(按姓氏笔画排序)

王　涛　　王旭东　　卞小林　　石青环

刘　忠　　李　轲　　李敏勇　　张友兵

金嘉旺　　胡生亮　　贺静波

译者序

由丹尼尔·文特 (Daniel Ventre) 先生所著的《信息战》一书, 于 2007 年在法国面世, 2009 年在美国和英国分别再版, 是目前欧美国家关于 "信息战" 方面一部较新的著作。作者以独特的视角, 描述、分析了美国、印度、日本、俄罗斯、新加坡等不同国家和地区关于 "信息战" 内涵、作用及其在现代战争领域中的地位, 并就信息战所涉及的攻击形式、法律问题等内容提出了自己的见解, 内容全面、系统, 是一部具有显著时代特征的军事读物。

原著作共由 8 个主体章节和 1 个结束语构成, 其中第 2 章对中国的信息战进行了描述, 因部分内容与中国信息战实际不符, 为避免引起读者误解, 通过国防工业出版社与原作者沟通, 以合同形式明确第 2 章内容不予翻译。因此, 本译著自第 2 章开始的章节编排与原著作存在一个数字差 (即本译著的第 2 章对应原著作第 3 章、第 3 章对应原著第 4 章, 依次类推)。需提醒读者注意的是, 为了忠实表达原作者关于信息战的理解和看法, 我们在翻译过程中完整保留了原作中的称谓、举例、假设和观点, 但这并不代表我们支持或认同这些观点!

本译著为国内从事信息战理论研究的学者、信息战部队的指挥技术军官及相关军事理论的爱好者提供了一部了解外军信息战主要内容的读物, 同时也可作为军队院校相关专业的补充教材和部队机关制定相关政策法规的参考读物。

愿通过本著作的翻译出版, 对促进我国信息战相关理论的发展和进

步, 对推动我军信息化建设和普及全民相关军事理论知识能起到一定的促进作用。

感谢国防工业出版社对本译著的顺利出版所提供的大力支持和帮助。

因原著涉及内容较广, 加之译者水平有限, 难免存在偏差, 敬请读者不吝指正。

译 者

2013 年 2 月

缩略语

ACINT	声学情报
AFDD	空军条令文件
AFIWC	空军信息战中心
AFPD	空军政策指令
AIC	反对印度小组
AIIT	军队技术学院 (印度)
APCERT	亚太计算机应急响应小组
ASCON	军队静态通信交换网络 (印度)
BARC	巴巴原子能研究中心 (印度)
BBC	英国广播公司
BFT	蓝军追踪器
BOA	空地作战催化剂
C^2	指挥控制
C^2W	指挥控制战
C^3I	指挥、控制、通信、情报
C^4	指挥、控制、通信、计算机
C^4I	指挥、控制、通信、计算机、情报
C^4I^2	指挥、控制、通信、计算机、情报、信息
C^4I^2SR	指挥、控制、通信、计算机、情报、信息、监视和侦察
C^4ISR	指挥、控制、通信、计算机、情报、监视和侦察
CBINT	生化情报
CERT	计算机应急响应小组
CERT-In	计算机应急响应小组 — 印度
CIA	中央情报局 (美国)
CMO	民间军事行动
CNA	计算机网络攻击
CNCERT/CC	中国计算机网络应急响应小组/协调中心
CND	计算机网络防御
CNE	计算机网络探测
CNO	计算机网络作战
COMINT	通信情报
COMSEC	通信安全
DARPA	国防高等研究计划署 (美国)
DDoS	分布式拒绝服务

DIA	国防情报局 (美国)
DISA	国防信息系统局 (美国)
DIWA	国防信息战局 (印度)
DoD	国防部 (美国)
DoDAF	国防部体系架构框架
DOE	能源部 (美国)
DoS	拒绝服务
DPRI	国防政策审查倡议 (日本)
DSO	国防科学组织 (新加坡)
DSTA	国防科技署 (新加坡)
EA	电子进攻
EBO	基于效果作战
EDB	新加坡经济发展委员会
EIW	经济信息战
ELINT	电子情报
ELNZ	萨帕塔主义国家解放军
EMP	电磁脉冲
EP	电子防御
ES	电子支援
ETC	电子测试中心 (新加坡)
EW	电子战
FAGCI	政府通信和信息的联邦机构
FAPSI	俄罗斯联邦政府通信情报局
FARC	哥伦比亚革命武装力量
FBI	联邦调查局 (美国)
FIRST	事件响应和安全小组论坛
FIWC	舰队信息战中心
FPDA	火力防御协定
FSB	联邦安全局 (俄罗斯)
GDP	国内生产总值
HKCERT/CC	香港计算机应急响应小组/协调中心
HUMINT	人工情报
IA	信息保障
IAD	信息保障部
IBW	情报资讯战
ICE	集成控制
ICT	信息和通信技术

IDA	资讯发展署 (新加坡)
IED	简易爆炸装置
IFF	敌我识别设备
IIT	印度理工学院
IKC^2	基于知识的指挥与控制
ILS	综合后勤保障
IM	信息管理系统
IMINT	图像情报
INDU	印度国防大学
INFOSEC	信息安全
IO	信息作战
IP	知识产权
IPv6	国际互联网协议第 6 版
ISA	网络内部安全法 (新加坡)
ISC	印度科学大会
ISP	互联网服务供应商
ISR	情报、监视、侦察
ITRC	个人身份失窃资源中心 (美国)
IW-D	防御信息战
IWSC	信息战保障中心
JCS	参谋长联席会议
JDA	日本防卫厅
JEWEL	战争博弈和实验的联合建模与仿真环境实验室 (新加坡)
JPCERT/CC	日本计算机应急响应小组/协调中心
JRA	日本红军
KGB	国家安全委员会 (俄罗斯)
KISA	韩国信息安全局
KrCERT/CC	韩国计算机应急响应小组/协调中心
LIC	低强度冲突
LIWA	陆地信息作战行动
LTTE	泰米尔伊拉猛虎解放组织
MASINT	身份情报
MDA	媒体发展署 (新加坡)
MILDEC	军事欺骗
MIS	结构管理信息系统
TARM	Tupak Amaru 革命运动
MyCERT	马来西亚计算机应急响应小组

NASA	美国国家航空航天局
NATO	北大西洋公约组织 (简称北约)
NCW	网络中心战
NetA	网络攻击
NetD	网络防御
NGA	国家地理空间情报局 (美国)
NIC	国家信息中心 (印度)
NICT	现代信息通信技术
NIH	联邦国家健康协会 (美国)
NISC	国家资讯安全委员会 (新加坡)
NISS	国家战略研究院 (印度)
NIWA	海军信息作战行动
NS	网络支援
NSA	国家安全局 (美国)
NSCC	国家安全协作中心 (新加坡)
NUCINT	核情报
NUS	新加坡国立大学
NGO	非政府组织
NTC	南洋理工大学 (新加坡)
ONI	开放网络机构 (新加坡)
OODA	观测指挥控制环
OPSEC	作战安全
ORNS	国家预备役人员
OSINT	开源情报
P2P	点对点
PAIR	体力行动 — 信息 — 回应
PBA	战场感知
PC	个人计算机
PDA	个人数字助理
PKK	库德斯坦 (库尔德工人党)
PMS	私营军事团体
PSYOPS	心理作战
PSYWAR	心理战
RADINT	雷达情报
RAHS	风险评估及层位扫描 (新加坡)
RAW	印度调查分析局
RBN	俄罗斯网络服务提供商

RINT	辐射情报
RMA	军事革命
ROI	投资利润率
SAF	新加坡武装力量
SBA/MBA	新加坡广播局/媒体发展局
SCADA	监控和数据系统
SCME	新加坡空军军事实验中心
SIGINT	信号情报
SingCERT	新加坡计算机应急响应小组
SM3	标准 -3 导弹
SMA	新加坡制造商联合会
SPIIRAS	俄罗斯科学院
SPRING	生产力和创新委员会 (新加坡)
SVR	俄罗斯对外情报局
TECHINT	技术情报
TIA	整体情报识别计划 (新加坡)
TLD	顶级域名
TWI	信息战保障办公室
VSNL	印度国营电信公司
WMD	大规模杀伤性武器
3GF	第三代部队

绪论

当产业和社会各界开始规划、创造和梦想着信息技术的发展会给人类带来新生活方式的时候，战略家们却在思考着 21 世纪新的冲突方式：应如何利用信息和信息技术的优势来超越竞争者或敌人。

1991 年的海湾战争给了我们一个早期的明确答案：掌控信息和信息技术是现代冲突取胜的关键。“信息战”作为一个新出现的重要概念，正在全球范围内得到普及，并且逐渐成为不管是军人还是平民的战略家和决策者所关注的对象。

20 世纪 90 年代，一些概念引发了关于信息及其技术的控制、风险和挑战的争论，这些概念包括信息战、网电战、计算机网络攻击、网络恐怖主义或网络中心战。从那时起，世界范围的文献中已经大量充斥书籍、文章、报告、研究、分析及官方或非官方的、严肃，有时甚至牵强的专家评论，反复描述着这些观念和理论。今天，在军事领域，我们更偏好于“信息作战”这一措辞，虽然也越来越多地提到网电战、信息战和网电攻击；然而，基本的概念仍然是广义的“信息战”，它包括在信息领域里实施的广泛行动。

信息技术，表现为 21 世纪国际增长的动力，似乎同样是我们的劲敌，是我们依赖信息系统社会的短板。因为通过掌控信息技术，对手和敌方就能轻易攻击我们。

网电空间攻击普遍存在，可能在类型上变化多端（包括垃圾邮件、钓

鱼、截获、非法访问、数据泄密、地址修改和分布式拒绝服务[①] 攻击), 但都是一种攻击。对于攻击者, 他们一直以来都将计算机黑客作为自己的偶像, 有时一个能够侵入银行或者政府机构的计算机系统, 并且可能有能力对国家网络带来毁灭性破坏的未成年黑客, 会被错误地描绘成一个计算机天才(认为能够利用计算机进行攻击好像需要很大的天分)。但是攻击者并不都是那些为了玩一款新游戏而废寝忘食的未成年人。网络攻击有多种形式及动机, 而且攻击不仅仅只采取计算机黑客攻击这一种形式。

通常, 人们担心网络攻击会破坏公司或国家的经济, 甚至影响全球稳定, 这已经成为那些依赖信息技术国家的噩梦, 世界已进入不安全的信息技术时代。

既然我们现在的生活已经离不开信息和信息技术, 那我们倒不如把信息和信息技术做好, 如果可能, 还可以以此打击敌方。我们应该如何利用信息和信息系统来增强我们的防卫能力? 如何才能掌控敌方? 如何才能击败他们?

信息战一定要回答这些期望。它为那些在军事、技术、经济和数字技术领域较为落后的国家提供了一种与强国进行对抗的手段。然而, 信息技术不是贫穷国家的武器, 这就好比扔向巨人使其致盲的石头, 因为信息战需要我们拥有相关的核心技术手段、经济手段, 特别是战略。

到目前为止,"信息战" 还没有一个约定俗成的定义, 其原因在于它的组成要素。要素之一 "战" 的定义就存在诸多争议, 对于社会学家、人类学家、经济学者、历史学家、政治家和科学家或军队人员而言, "战" 的定义各不相同。而对于 "信息" 这一要素, 不管是数学家、计算机专家、社会学家, 还是新闻工作者、军事人员与经济学者对它的定义正以不同方式逐步接近。

本书主要介绍 "信息战" 这一概念, 但并不能完全解决其定义的问题。本书的目的在于分析信息战是什么及通过介绍它的各个方面和组成 (因为信息战无法仅仅通过遏制计算机网络攻击来减少) 来定义它的发展、挑战及可能采取的策略。同时, 关注 21 世纪初主宰着世界经济、政治、军事平衡的几个大国的信息战现状。

① Denial of Service.

国防科技著作精品译丛．网电空间安全系列

国防工业出版社已出版或即将出版的国防科技著作精品译丛．网电空间安全系列，请关注：

《网络电磁安全科学研究路线图》

《信息战》

《电子战》

《网电空间安全：公共部门的威胁与响应》

《网电战争 —— 安全从业者的技术、战术与工具》

《网电力量和国家安全》

《网电空间态势感知问题与研究》

《网电战基础：在理论和实践中认识网电战基本原则》

《工业网络安全 —— 智能电网，SCADA 和其他工业控制系统等关键基础设施的网络安全》

目录