



高等学校信息安全专业规划教材

信息对抗理论与方法

(第二版)

付钰 吴晓平 陈泽茂 王甲生 李洪成 编著



WUHAN UNIVERSITY PRESS

武汉大学出版社

图书在版编目(CIP)数据

信息对抗理论与方法/付钰等编著. —2版. —武汉:武汉大学出版社, 2016.7

高等学校信息安全专业规划教材

ISBN 978-7-307-17927-1

I. 信… II. 付… III. 计算机网络—安全技术—高等学校—教材
IV. TP393.08

中国版本图书馆 CIP 数据核字(2016)第 118861 号

责任编辑:林 莉 责任校对:李孟潇 版式设计:马 佳

出版发行:武汉大学出版社 (430072 武昌 珞珈山)

(电子邮件:cbs22@whu.edu.cn 网址:www.wdp.com.cn)

印刷:湖北恒泰印务有限公司

开本:787×1092 1/16 印张:22 字数:565千字 插页:1

版次:2008年8月第1版 2016年7月第2版

2016年7月第2版第1次印刷

ISBN 978-7-307-17927-1 定价:48.00元

版权所有,不得翻印;凡购买我社的图书,如有等质量问题,请与当地图书销售部门联系调换。



前 言

本书自 2008 年出版以来,世人皆能感受到网络信息空间中所发生的巨大变化。从云计算、物联网、移动互联网到大数据,尤其是在信息安全领域,近年来所出现的重大事件甚至成为了世界各国普通民众关注的热点话题:“伊朗核电站遭受网络攻击”、“美国网络战司令部成立”、美国政府发表的“网络空间国际战略”、“斯诺登事件”的曝光,以及我国成立的网络安全与信息化领导小组等,这一切无不昭示着未来网络安全领域的发展将更具挑战性、基础性和全局性。

信息对抗是指围绕信息的获取、传输、处理、分发和使用等而展开的攻防斗争,其目的是取得信息优势,即通过能力竞争和攻防斗争,使自己在信息利用方面比竞争对手处于占优势的地位,从而为取得竞争的最终胜利奠定基础。随着我国面临的网络空间威胁越来越严峻,国家成立了网络空间安全一级学科,在技术推动和需求牵引的双重作用下,信息对抗已经由单一的作战保障手段发展成为网络空间攻防对抗中至关重要的作战样式。由于目前国内尚没有对网络空间安全内涵与概念的明确界定,本书只是对网络空间安全相关内容进行了适当补充,并对其余章节内容进行了大量更新和扩展,使教材能与信息对抗技术的现状和发展趋势接轨,利于学生将所学知识应用于未来工作中。

本书共分为 10 章。第 1 章介绍了信息对抗的概念、内涵、特性及分类;第 2 章从信息对抗产生的原因、模型和基础设施建设三方面讨论了信息对抗的基础理论;第 3 章论述了电子对抗的基本概念和电子对抗侦察的一般原理;第 4 章阐述了电子对抗进攻和电子对抗防护的相关方法;第 5~7 章介绍了网络对抗相关内容,包括网络对抗模型、网络攻击与防御相关技术;第 8~9 章分别论述了情报战、心理战与军事欺骗的概念与方法;第 10 章介绍了一体化联合信息作战基础理论,并结合教学科研实践论述了美军网络空间安全战略。

本书力求使读者从宏观上对信息对抗有较为全面的了解,在内容取舍、概念表述、习题配用及叙述方式上,注意反映教学特点和要求。本书第 1、2 章由吴晓平编写,第 4 章由李洪成编写,第 5、6、7 章由陈泽茂、王甲生编写,第 3、8、9、10 章由付钰编写,全书由付钰负责统稿。

本书在第二版的编写过程中,得到了海军院校与士兵训练机构重点建设教材与重点建设课程立项资助,还得到了国家社科基金军事学项目(15GJ003-201)、湖北省自然科学基金(2015CFC867)、中国博士后科学基金(2014M552656)、海军工程大学教育科研项目(NUE2014212)等资助。本书在编写过程中,参阅了大量相关书籍、论文、网络文献,在此向相关作者表示感谢!在教材立项和编写过程中,俞艺涵同学对初稿进行了文字查错、图



表校对；在编辑出版过程中，得到了武汉大学出版社林莉等人的大力支持，在此，一并致以谢意！

由于作者水平和经验所限，书中不足或错漏之处在所难免，恳请有关专家和读者批评指正。

作者

2016年4月

于海军工程大学



目 录

第 1 章 信息对抗概述	1
1.1 信息的概念与特性	1
1.1.1 信息的概念	1
1.1.2 信息的特征	4
1.1.3 信息在冲突中的地位	5
1.2 信息对抗内涵与分类	7
1.2.1 信息对抗的概念.....	7
1.2.2 信息对抗的特点.....	9
1.2.3 信息对抗的层次.....	9
1.2.4 信息对抗的分类	10
1.3 信息对抗现状与趋势.....	13
1.3.1 信息对抗的时代特征	13
1.3.2 信息对抗的研究现状	14
1.3.3 信息对抗的发展趋势	16
1.4 本章小结.....	17
习题	17
第 2 章 信息对抗基础理论	18
2.1 信息对抗产生的原因	18
2.1.1 硬件问题	18
2.1.2 软件问题	20
2.1.3 网络缺陷	22
2.1.4 人为破坏	23
2.1.5 电磁频谱的争夺	26
2.2 信息对抗模型	28
2.2.1 信息对抗问题描述	28
2.2.2 信息对抗过程	28
2.2.3 两类攻击手段	30
2.2.4 信息攻击模型	31
2.3 信息对抗基础设施建设.....	33
2.3.1 信息对抗基础设施建设原则	33
2.3.2 信息对抗装备建设	34
2.3.3 信息对抗人才建设	34



2.4 本章小结.....	35
习题	35
第3章 电子对抗侦察	36
3.1 电子对抗概述.....	36
3.1.1 电子对抗的定义	36
3.1.2 电子对抗的分类和作战应用	38
3.1.3 电子对抗的作用对象	41
3.1.4 电子对抗的发展史	47
3.2 电子对抗侦察的特点和分类.....	51
3.2.1 电子对抗侦察的特点	52
3.2.2 电子对抗侦察的分类	52
3.3 电子对抗侦察的实施方法.....	62
3.3.1 电子对抗侦察中的信号侦测	62
3.3.2 电子对抗侦察中对辐射源的侧向	68
3.3.3 电子对抗侦察中对辐射源的定位	70
3.4 电子对抗侦察系统.....	72
3.4.1 电子对抗侦察系统类型	72
3.4.2 电子对抗侦察装备	72
3.5 本章小结.....	74
习题	74
第4章 电子进攻与防护	75
4.1 电子干扰.....	75
4.1.1 电子干扰概述	75
4.1.2 有源干扰	78
4.1.3 无源干扰	79
4.1.4 通信干扰	81
4.1.5 卫星导航干扰	84
4.1.6 光电干扰	88
4.1.7 水声干扰	89
4.1.8 敌我识别干扰	93
4.1.9 无线电引信干扰	94
4.2 隐身技术.....	98
4.2.1 隐身外形技术	98
4.2.2 隐身材料技术	99
4.2.3 红外隐身技术	99
4.2.4 可见光隐身技术.....	102
4.3 电子进攻武器	102
4.3.1 反辐射武器	102



4.3.2 定向能武器	104
4.3.3 电磁脉冲武器	109
4.3.4 等离子体武器	110
4.3.5 分布式电子干扰武器	112
4.4 电子防护	113
4.4.1 电子防护的作用领域	113
4.4.2 反电子侦察	114
4.4.3 抗电子干扰	115
4.4.4 抗硬摧毁	116
4.4.5 反隐身	118
4.4.6 电磁加固	120
4.5 本章小结	120
习题	121
第5章 计算机网络对抗	122
5.1 计算机网络对抗概述	122
5.1.1 计算机网络对抗的概念	123
5.1.2 网络对抗的特点	124
5.1.3 网络对抗的关键技术	125
5.1.4 网络对抗的作战方法	126
5.2 网络与信息系统的脆弱性	127
5.2.1 硬件设备的脆弱性	127
5.2.2 操作系统的脆弱性	127
5.2.3 网络协议的脆弱性	129
5.3 网络安全漏洞	138
5.3.1 安全漏洞的概念	138
5.3.2 安全漏洞的发现	139
5.3.3 安全漏洞的分类	139
5.4 网络对抗模型	143
5.4.1 基本的网络对抗模型	143
5.4.2 协同式网络对抗模型	149
5.4.3 网络对抗的博弈模型	157
5.5 网络对抗武器	159
5.5.1 网络对抗典型武器	159
5.5.2 网络对抗武器的发展趋势	160
5.6 本章小结	162
习题	162
第6章 网络攻击技术	163
6.1 目标侦查	163



6.1.1	确定目标	163
6.1.2	网络扫描	164
6.1.3	网络监听	170
6.1.4	社会工程	173
6.2	协议攻击	174
6.2.1	TCP/IP 协议简介	174
6.2.2	链路层协议攻击	177
6.2.3	网络层协议攻击	179
6.2.4	传输层协议攻击	187
6.2.5	应用层协议攻击	189
6.3	缓冲区溢出攻击	190
6.3.1	缓冲区溢出基础	190
6.3.2	缓冲区溢出漏洞的利用	192
6.3.3	ShellCode 的编写	193
6.3.4	缓冲区溢出漏洞的防范措施	197
6.4	拒绝服务攻击	198
6.4.1	DoS 攻击的类型	198
6.4.2	通用攻击手段	199
6.4.3	特定攻击手段	204
6.4.4	分布式拒绝服务攻击	205
6.5	恶意代码	210
6.5.1	计算机病毒	210
6.5.2	网络蠕虫	211
6.5.3	特洛伊木马	212
6.6	APT 攻击	212
6.6.1	APT 攻击技术概述	213
6.6.2	APT 攻击防御方法和手段	216
6.6.3	APT 攻击的纵深防御体系	219
6.7	网络攻击技术的发展趋势	220
6.8	本章小结	223
	习题	223
第 7 章	网络防御技术	224
7.1	信息加密技术	224
7.1.1	加密算法概述	224
7.1.2	公钥基础设施	227
7.1.3	数据库加密	228
7.1.4	虚拟专用网	231
7.2	网络隔离技术	233
7.2.1	防火墙技术	233



7.2.2 物理隔离技术	238
7.3 主动防御技术	240
7.3.1 入侵检测系统	240
7.3.2 蜜罐和蜜网系统	244
7.3.3 安全审计系统	246
7.4 电子取证技术	247
7.4.1 攻击追踪	247
7.4.2 取证的原则与步骤	248
7.4.3 取证工具	249
7.4.4 取证技术的发展	250
7.5 容灾备份技术	251
7.5.1 基本概念	252
7.5.2 容灾系统的级别	253
7.5.3 容灾系统的组成	254
7.5.4 容灾系统的评价指标	255
7.5.5 容灾产品和解决方案	256
7.6 入侵容忍技术	256
7.6.1 基本概念	256
7.6.2 入侵容忍系统构成	257
7.6.3 入侵容忍系统实现方式	258
7.7 网络防御技术的发展趋势	259
7.8 本章小结	259
习题	259
第 8 章 情报战	261
8.1 情报	261
8.1.1 情报的含义与基本属性	261
8.1.2 情报的作用层次分类	262
8.1.3 情报的获取与处理	262
8.1.4 情报在主导作战中的作用	267
8.2 情报战	269
8.2.1 情报战的概念与特点	269
8.2.2 情报战的作用与地位	271
8.2.3 情报战与信息战的关系	272
8.2.4 情报战的发展趋势	273
8.3 本章小结	276
习题	276
第 9 章 心理战与军事欺骗	278
9.1 主观域作战	278



9.2	心理战	280
9.2.1	心理战的概念	280
9.2.2	心理战要素及特点	281
9.2.3	心理战攻击方式	284
9.2.4	心理战作用原理与地位	291
9.2.5	信息化条件下心理战研究的特点与问题	293
9.3	军事欺骗	299
9.3.1	军事欺骗的概念	299
9.3.2	军事欺骗的步骤与方法	301
9.3.3	军事欺骗的作用与地位	302
9.3.4	军事欺骗战例	302
9.4	本章小结	304
	习题	304
第10章	一体化联合信息作战	306
10.1	现代信息作战概论	306
10.1.1	基本原则	306
10.1.2	组织机构	307
10.1.3	计划预案	310
10.1.4	实施指南	312
10.2	进攻性信息作战战法	314
10.2.1	概述	314
10.2.2	目标选择方法	318
10.2.3	情报支援方法	319
10.2.4	行动转换方法	320
10.2.5	协同合作方法	321
10.2.6	作战训练方法	322
10.3	防御性信息作战战法	323
10.3.1	概述	323
10.3.2	信息保护方法	325
10.3.3	情报侦测方法	327
10.3.4	应急反应方法	328
10.3.5	能力恢复方法	328
10.3.6	作战训练方法	329
10.4	美军网络空间安全战略演进及特点	330
10.4.1	美军网络空间安全战略的演进	330
10.4.2	美军网络空间安全战略的特点	333
10.5	本章小结	340
	习题	341
	参考文献	342



第1章 信息对抗概述



美国著名的未来学家托夫勒曾经说过：“谁掌握了信息、控制了网络，谁就拥有了整个世界。”美国前总统克林顿曾说：“今后的时代，控制世界的国家将不是靠军事，而是信息能力走在前面的国家。”美国原陆军参谋长沙利文一语道破：“信息时代的出现，将从根本上改变战争的方式。总之，过去的战争是谁拥有最好的武器，谁就可能在战争中取胜。而今天则是谁掌握了信息控制权，谁就胜利在望。”因此，信息对抗这一领域将一直成为各国学者研究的热门话题。

1.1 信息的概念与特性

信息对抗是围绕信息展开的斗争。理解信息对抗，首先需要把握信息的概念和本质。随着现代通信技术的迅速发展和普及，特别是随着通信与计算机结合而诞生的计算机网络全面进入千家万户，信息的应用与共享日益广泛，且更为深入。人类发展至今，对于信息有着各种各样的理解与定义。

1.1.1 信息的概念

“信息”一词古已有之，在人类社会早期的日常生活中接触到的信息，有如天气预报带来的气候变化信息、新闻报道带来的人类社会生活信息、信件带来的别人内心活动信息，等等。但人们对信息的认识比较广义而模糊，对信息和消息的含义没有明确界定。到了20世纪中叶后，现代信息技术的飞速发展及其对人类社会的深刻影响，迫使人们开始探讨信息的准确含义。

1. 信息的经典定义

1928年，哈特雷(L. VR. Hartley)在《贝尔系统电话》杂志上发表了题为《信息传输》的论文。他在文中将信息理解为选择通信符号的方式，且用“选择的自由度”来计量这种信息的大小。他注意到，任何通信系统的发信端总有一个字母表(或符号表)，发信者发出信息的过程正是按照某种方式从这个符号表中选出一个特定符号序列的过程。假定这个符号表一共有 S 个不同的符号，发送信息选定的符号序列一共包含 N 个符号，那么，这个符号表中无疑有 S^N 种不同符号的选择方式，也可以形成 S^N 个长度为 N 的不同序列。这样，就可以把发信者产生信息的过程看做从 S^N 个不同的序列中选定一个特定序列的过程，或者说是排除其他序列的过程。

然而，用“选择的自由度”来定义信息存在着局限性，主要表现在：一方面，这样定义的信息没有涉及信息的内容和价值，也未考虑到信息的统计性质；另一方面，将信息理解为选择的方式，就必须有一个选择的主体作为限制条件。因此，这样的信息只是一种认识论意义上的信息。

1948年, 香农(C. E. Shannon)在《通信的数学理论》一文中, 在信息的认识方面取得重大突破, 堪称信息论的创始人。香农的贡献主要表现在推导信息测度的数学公式上, 发明了编码的三大定理, 为现代通信技术的发展奠定了理论基础。

香农发现, 通信系统所处理的信息在本质上都是随机的, 可以运用统计方法进行处理。他指出, “一个实际的消息是从可能的消息集合中选择出来的, 而选择消息的发信者又是任意的, 因此, 这种选择就具有随机性”。这是一种大量重复发生的统计现象。

香农对信息的定义同样具有局限性, 主要表现在: 这一概念同样未能包含信息的内容与价值, 只考虑了随机性的不定性, 未能从根本上回答信息是什么的问题。

1948年, 就在香农创建信息论的同时, 维纳(N. Wiener)出版了专著《控制论——动物和机器中的通信与控制问题》, 并且创立了控制论。后来, 人们常常将信息论、控制论以及系统论合称为“三论”, 或统称为“系统科学”或“信息科学”。

维纳从控制论的角度认为, “信息是人们在适应外部世界, 并且使这种适应反作用于外部世界的过程中, 同外部世界进行互相交换的内容的名称”。他还认为, “接收信息和使用信息的过程, 就是适应外部世界环境的偶然性变化的过程, 也是我们在这个环境中有效地生活的过程”。维纳的信息定义包含了信息的内容与价值, 从动态的角度揭示了信息的功能与范围。但是, 人们在与外部世界的相互作用过程中, 同时也存在着物质与能量的交换, 不加区别地将信息与物质、能量混同起来是不确切的, 因而也有局限性。

1975年, 意大利学者朗高(G. Longo)在《信息论: 新的趋势与未决问题》一书的序中指出, 信息是反映事物的形成、关系和差别的东西, 它包含在事物的差异之中, 而不在事物本身。无疑, “有差异就是信息”的观点是正确的, 但“没有差异就没有信息”的说法却不够确切。譬如, 我们碰到两个长得一模一样的人, 他(她)们之间没有什么差异, 但会马上联想到“双胞胎”这样的信息。可见, “信息就是差异”也有其局限性。

据不完全统计, 信息的定义有100多种, 它们从不同侧面、不同层次揭示了信息的特征与性质, 但也都有这样或那样的局限性。信息作为物质世界的三大组成要素之一, 其定义的适用范围是非常宽的。上述几种经典定义也只适合特定范围或层次, 是人们在探索信息的过程中所形成的几种含金量高的认识积淀。

2. 与现代通信有关的信息概念

通信领域对信息的研究有着悠久的历史, 信息科学的出现正是通信理论研究的最重要的成果之一。1988年, 中国学者钟义信在《信息科学原理》一书中, 认为信息是事物运动的状态与方式, 是事物的一种属性。信息不同于消息, 消息只是信息的外壳, 信息则是消息的内核。信息不同于信号, 信号是信息的载体, 信息则是信号所载荷的内容。信息不同于数据, 数据是记录信息的一种形式, 同样的信息也可以用文字或图像来表述。信息不同于情报, 情报通常是指秘密的、专门的、新颖的一类信息; 可以说所有的情报都是信息, 但不能说所有的信息都是情报。信息也不同于知识, 知识是认识主体所表达的信息, 是序化的信息, 并非所有的信息都是知识。他还通过引入约束条件推导了信息的概念体系, 对信息进行了完整而准确的论述。

通过比较, 中国科学院文献情报中心孟广均研究员等在《信息资源管理导论》一书中认为, “作为与物质、能量同一层次的信息的定义, 信息就是事物运动的状态与方式”。这个定义由于具有最大的普遍性, 所以不仅涵盖所有其他的信息定义, 而且通过引入约束条件还能转换为所有其他的信息定义。



3. 信息论中信息的概念

在由通信理论发展而来的狭义信息论中，信息是指消息（物理现象、语音、数据和图像等）包含的内容或含义，信源是指发出消息的人或事物，信宿是指接收消息的人或系统，如图 1-1 所示。

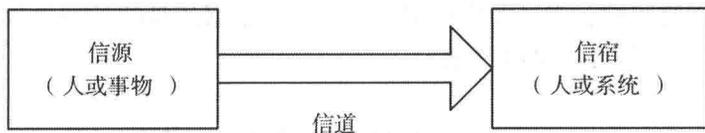


图 1-1 信息系统模型

信息是信源状态及其变化规律的客观反映。它的价值（即信息量）是用其所包含的、信宿此前不知道的内容的多少来度量的。此外，信息量还因人而异，与使用者的知识水平和理解能力有密切关系。消息与信息或信息量之间的关系是复杂的。

可以理解，信息是联系人的主观世界与外部世界（包括客观世界与别人的内心世界）的桥梁，是人们认识世界和改变世界的必然途径。因此，在目前的广义信息论中，信息有客观层次上的本体论定义和主观层次上的认识论定义。

本体论信息的定义是事物（物质和能量等）的状态及状态变化方式的自我显示（或自我表述），如物体的体积、温度、颜色、位置和运动状态等。

认识论信息的定义是主体所感受的或表述的事物的状态及状态的变化，包括状态及其变化的方式、含义和效用。事物状态及其变化的方式称为语法信息，语法信息的含义称为语义信息，语法信息对改变外部世界的效用称为语用信息。因此，认识论信息是包括语法信息、语义信息和语用信息的“全信息”。

图 1-2 是本体论信息到认识论信息，再到改变外部世界的行为的信息过程模型。从中可以看出，认识论信息是经过人或机器处理过的信息，包括知识和决策等。

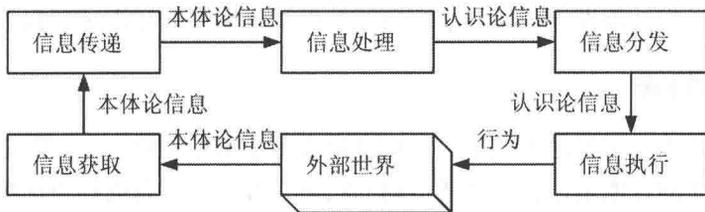


图 1-2 信息过程模型

在给出了信息的定义之后，还有必要说明以下两点来进一步理解它。

一是信息与物质和能量的关系。信息、物质和能量并称为人类社会活动的三大基本要素。从物理上来说，信息既不是物质，也不是能量，而是指物质和能量的状态及其变化的方式。这些状态及其变化方式还是要通过（其他）物质和能量的形式表现出来或被人或系统感知的。因此，物质和能量既是信息的源，也是信息的载体。人或系统通过物质和能量来感知信息。如我们通过光线来感知物体的形状和运动速度，通过声音感知他人的心态等。

二是信息是有主观性的。如果语法信息不能被人所知，我们就无法讨论它。因此，我们所说的信息或语法信息，通常是指可以通过某种手段或途径感知的消息，如能看见的现象、能听到的声音、能测量的数据、能表达或观察的心态等。

4. 信息工程中信息的概念

由于信息论给出的信息定义和度量方法在现实生活中难以掌握和应用，因此在信息工程中，人们常常采用笼统的、广义的信息定义。该定义根据信息的处理过程和可利用的成熟度，将信息分为三个层次，如图 1-3 所示。

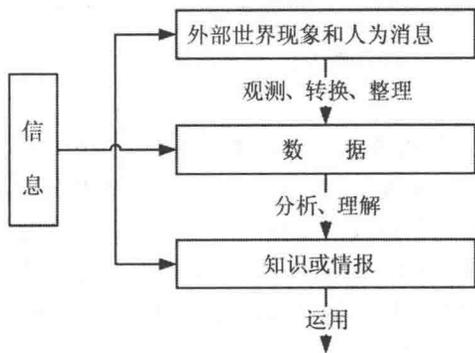


图 1-3 广义信息模型

其中，第一层为外部世界现象（如物体的体积、速度和温度等）及人为消息（如信件、命令和讲话等）。第二层为数据，它是对现象进行观测、变换和整理等得来的结果，包括数字、曲线、图像、电子文档和计算机程序等（这些内容在计算机中都是以数据格式存储、传输和处理的，因此统称为数据）。第三层为知识，它是人或机器对数据进行分析和理解的结果。军事上所用的情报相当于这里的知识。根据该定义，外部世界的现象、信息系统中的数据和人掌握的知识 and 情报，都称为信息。虽然这种定义模糊了信息的形式、内涵和度量方法，但方便了信息概念的使用。实际上，我们通常所说的信息的概念，基本上是与该定义相符合的，即信息是指外部世界现象、系统中的数据和人掌握的知识 and 情报等。

1.1.2 信息的特征

信息来源于物质，而不是物质本身；信息也来源于精神世界，又限于精神的领域。信息归根到底是物质的普遍属性，是物质运动的状态与方式。信息的物质性决定了它的一般属性，它们主要包括普遍性、客观性、无限性、抽象性、不守恒性、复制性、复用性、相对性、共享性、依附性、可传递性、可变换性、可转化性和可伪性等。下面从两个方面分析信息的特征。

1. 信息的存在形式特征

(1) 不守恒性：信息不是物质，也不是能量，而是与能量和物质密切相关的运动状态的表征和描述。由于物质运动不停，变化不断，故信息不守恒。

(2) 复制性：在非量子态作用机理情况下，在环境中可区分条件下具有可复制性（在量子态工作环境，一定条件下是不可精确“克隆”的）。



(3) 复用性：在非量子态作用机理情况下，在环境中可区分条件下具有多次复用性。

(4) 相对性：不同的“主体”（或信宿）由于其理解能力、观察方法和目的不同，从同一事物所获得的信息量各不相同，即信息量有相对性。为了获得更多的信息，“主体”要努力提高观察、理解和采用科学方法的能力。

(5) 共享性：在信息荷载体具有运行能量，且运行能量远大于敏感信息所需低限阈值时，则此信息可多次共享，如话音几个人可同时听到，卫星转播多个接收站可以同时接收信号获得信息等等。

(6) 时效性：信息不脱离信源时，是随信源状态实时变化的；当信息脱离了信源时，它就成了信源状态的记录和历史，因而它的效用可能会逐渐降低，甚至完全失去效用，这就是信息的时效性。信息的时效性要求我们及时地获取和发挥信息的效用，要求我们不断地补充和更新知识。这一性质对信息保密也很重要。

需要说明的是，若信息系统的运行处在量子状态，复制性、复用性和共享性这三种特征的情况就完全不同了。

2. 人所关注的信息利用层次上的特征

信息最基本、最重要的功能是“为人所用”，即以人为主体的利用。从利用层次上讲，信息具有如下特征。

(1) 真实性：产生信息不真实反映对应事物运动状态的意识源可分为“有意”与“无意”两种。“无意”为人或信息系统的“过失”所造成的信息的失真，而“有意”则是人为地制造失实信息或更改信息内容以达到某种目的。

(2) 多层次区分特性：信息属于哪个层次，这也是其重要属性。对于复杂运动的多种信息，知其层次属性对综合、全面掌握运动性质是很重要的。

(3) 信息的选择性：信息是事物运动状态的表征，运动充满各种复杂的相互关系，同时也呈现对象性质，即在具体场合信息内容的“关联”性质对不同主体有不同的关联程度，关联程度不高的信息对主体就不具有重要意义，这种特性称为信息的空间选择性。此外有些信息对于应用主体还有时间选择性，即以某时间节点或时间区域节点为界，对应用主体有重要性，如地震前预报信息便是一例。

(4) 信息的附加义特征：由于信息是事物运动状态的表征，虽可能只是某剖面信息，但也必然蕴涵运动中相互关联的复杂关系。通过信息获得其所蕴涵非直接表达的内容（“附加义”的获得）有重要的应用意义。人获得“附加义”的方式，可分为“联想”方式和逻辑推理方式，“联想”是人的一种思维功能（“由此及彼”的机制甚为复杂），它比利用逻辑推理的作用领域更广泛。例如，根据研究课题性质联系到该研究机构将推出的新产品，是根据研究机构所研究课题蕴涵的多种信息，利用逻辑推理和相关科学技术确定下一阶段将要投入市场的新产品，就是一个逻辑推理获得信息附加义的例子。

1.1.3 信息在冲突中的地位

信息、物质和能量是人类社会活动的三大要素。信息无处不在，无时不有。它是外部世界规律的反映，也是我们与外部世界联系的桥梁。通过积极地研究、把握和利用信息，我们能够充分地认识和利用外部世界，并更好地改造客观世界。

信息、物质与能量也是冲突或战争的三大要素。就像信息离不开物质和能量一样，冲突也是离不开信息的。这是原始、古老的哲理，而不是信息对抗的新理论。只不过在新的历史

条件下，信息对抗给信息赋予了更加重要的地位和丰富的内涵。只有理解和掌握好信息的本质及其在冲突中的应用方法，我们才能在冲突中取得胜利，尤其是在目前的信息社会中。

1. 原始概念

其实，信息或情报对于冲突的作用是个很原始的常识。例如，有些动物群体进行防御或搏杀时，就有分工负责警戒或观敌了阵的。按信息对抗术语来说，其用意就是及时获取战场的信息，并指挥自己的群体进行有效的攻防。

2. 古老概念

早在公元前 10 世纪，军事家所罗门国王就撰文强调知识（军事情报）、指导（战略和作战计划）和顾问（目标分析员）是战争的制胜法宝。他写道：“聪明的人有较大的权力，有知识的人能增强力量；进行战争需要指导，赢得战争需要许多顾问”。

公元前 6 世纪，孙武在《孙子兵法》中精辟地阐述了信息对战争的作用。他提出的、经常被人们引用的信息观点有如下几条。

(1) “知己知彼，百战不殆”。

(2) “兵法，一曰度，二曰量，三曰数，四曰称，五曰胜”。其原意为，作战决策要采取如下步骤：一是观测田地的多少；二是根据产量和田地的多少计算粮食收成；三是根据粮食的多少和每个人的饭量，计算军队可能供养多少人；四是根据双方兵力的多少，对比双方的势力；最后，才能在前四步的基础上，制定和实施取胜的计划。用信息对抗术语解释其含义，就是只有根据全面及时的作战信息进行仔细的态势评估，制定合适的战略和战术，才能取得战争的胜利。

(3) “见胜不过众人之所知，非善之善者也”。其含义是掌握情报信息和预测未来的能力是鉴别优秀指挥员的标准。

(4) “微乎微乎，至于无形。神乎神乎，至于无声。故能为敌之司命”。其含义是通过欺骗和秘密拒绝等手段控制敌人的信息，可以使敌人产生错误的感知。

(5) “夫用兵之法，全国为上，破国次之……是故百战百胜，非善之善者也；不战而屈人之兵，善之善者也”。其含义是战争的最高形势是用信息影响敌人的感知及意志，而不是使用武力打击方法。

在公元前 6 世纪就应用的这些理论是建立在信息获取、处理和分发基础上的。这些理论至今仍然有效，只是信息的获取、处理和分发手段发生了变化，即电子手段取代了早期的信使和文字通信方法。随着对电子手段的依赖性逐渐增强和信息量的逐渐增加，信息本身已成为战争的有利目标和武器。所以这些变化正在使信息的作用和战争的方法发生剧烈的变革。

3. 现代概念

(1) 战争“迷雾”

拿破仑在《军事格言》中写道：一位将军始终不能确定任何事情，或是清楚地看到自己的敌人，或是有把握地判断他在何方。克劳塞维茨在 1812 年的《战争论》中写道：战争属于捉摸不定的范畴。作为行动依据的诸项因素中，有四分之三笼罩在或多或少的不确定性“迷雾”中。

战争“迷雾”是指由于受情报获取能力、知识水平以及自然和人为随机因素（如因人因时而异的指挥方法）的影响，指挥员总是不能清楚地掌握敌方甚至己方的行动和意图。战争“迷雾”主要是由于情报和知识缺乏造成的，它好像一团云雾模糊了指挥员的视线，使其不能看清战场的全貌，做到“知己知彼，百战不殆”。战争“迷雾”几乎是每个指挥员