国防科工委“十五”规划教材. 信息与通信技术

信息系统与安全对抗理论

王　越　罗森林　著

北京理工大学出版社
北京航空航天大学出版社　西北工业大学出版社
哈尔滨工业大学出版社　哈尔滨工程大学出版社

内容简介

本书全面研究和论述了信息系统与安全对抗的相关理论，主要内容包括：现代系统理论的基本内容；信息及信息系统；信息安全与对抗的系统概述；信息安全与对抗的基本原理；信息安全与对抗的原理与技术性方法；信息安全与对抗的应用实例等。本书可供从事信息安全、信息对抗技术、通信与信息系统等相关方面教学、科研、应用人员阅读和使用，对从事信息安全相关研究的人员具有重要的实用和参考价值。此外，本书也可供其他专业研究人员参考使用，具有重要的理论与实践的指导意义。

图书在版编目(CIP)数据

信息系统与安全对抗理论/王越，罗森林著. —北京：
北京理工大学出版社，2006.1
国防科工委“十五”规划教材. 信息与通信技术
ISBN 7-5640-0472-X

Ⅰ. 信… Ⅱ. ①王…②罗… Ⅲ. 信息系统-安全技术-高等学校-教材 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2005)第 066940 号

信息系统与安全对抗理论

王 越 罗森林 著
责任编辑 董双洪
责任校对 郑兴玉
北京理工大学出版社出版发行
北京市海淀区中关村南大街 5 号(100081)
电话：010－68914775(办公室) 68944990(批销中心) 68911084(读者服务部)
http://www.bitpress.com.cn
E－mail：chiefeditor@bitpress.com.cn
北京圣瑞伦印刷厂印制 各地新华书店经销

开本：787×960 1/16
印张：14.5 字数：290 千字
2006 年 1 月第 1 版 2006 年 1 月第 1 次印刷
印数：3000 册.
ISBN 7-5640-0472-X 定价：25.00 元

国防科工委“十五”规划教材编委会

（按姓氏笔画排序）

目　　录

第 1 章　现代系统理论的基本内容

1.1　引言——通向“系统”的引导

1.1.1　由“运动”说起

“运动”在这里不是指体育领域的运动，即不是指人们所进行的体力、体能测试和训练，而是指广泛意义上物质存在的运动。人们不能追问“运动”为什么产生、产生的终极原因是什么？这是一种客观存在，如同物质之客观存在一样，人们只能在承认运动的客观存在的前提下去认识运动，即不断深入了解“运动”的各种表现形式，它们之间的转化规律以及各种“运动”规律等等。承认物质客观存在就应承认运动客观存在。现代科技发展前沿很大部分是更深入、更广泛地探索研究“运动”，在这里，探索“运动”的重点在于复杂的运动，人们已经按“运动”的各种本质特征分门别类地建立了运动的各种分类学科，如物理运动对应于物理学，就是通过物理量、物理参数和物理基本规律来研究物理运动的，如引力、力、动量、热参数、能量（具有广泛意义，是物质运动的尺度）。物理运动包括宇观、宏观、介观、微观等多种尺度运动。化学运动主要是研究分子、原子、原子间的运动，它必然又关联到电子、原子核间结构布局的相互影响，与物理形成了交叉。实际上人们在分门别类地研究各种“运动”中，逐渐体会到种种运动存在着互相“交叉”融合的现象，如上述物理和化学量子学领域的运动就是一种“交叉”。对交叉作用需要“综合”，它表明人们关注的焦点正逐渐转向综合思维。中国文化的思维特点是重视综合思维，这是传统性的优点，各种复杂运动的研究是人类科学探索研究的永恒主题。研究复杂运动要依靠在分析基础上的综合研究，例如生命运动是多种复杂运动，它是综合性的；生物化学是生物规律在化学领域中的反映，细胞的生长发育，生命的生长发育生存等需要生物科学结合物理领域的研究，如“哥伦比亚号”航天飞机上中国中学生设计的命题，即在太空微重力环境下生物生存的综合问题。宇宙间最复杂的运动可认为是人的生命运动，人的身体组织与器官互相配合以支持人生命延续，也支持其自身生存，人全身数以万万亿计细胞的生存代谢，都与血液和体液系统相联系，进一步联系到人的思维及相关运动，则更是精细、复杂，甚至神奇。人的思维是极复杂的运动，它与其他重要功能相互融合，相互支持，如语言功能就是一种与思维功能密切相关的重要复杂功能，如儿童思维能力虽不完善但都具有基本语言能力。每一个词的发声由发声意识的产生到发声动作的完成，就是一个非常复杂的产生和控制过程，语言与思维密切关联，但发声过程并不由思维意识完全控制，是一种复杂运动。总之，人的存在是由非常

多种类的运动有机组成的。当维持人生命的各种运动一旦停止，则生命将终结；不但如此，而且一种重要运动停止也会牵连整体生命或者致残，如心脏停止运动则将生理死亡，脑运动停止，则是脑死亡，一旦生命运动停止，人的生命就不存在了。紧接着是分解，将复杂的人体最后化成简单元素。由各种客观存在的实际例子，我们可以体会到：世界上除了运动之外没有别的什么东西。这种哲理具有普遍性和深刻性，运动即物质，它是客观存在的。

1.1.2 由运动说到“系统”

上面谈到的各种复杂“运动”，是在人类认识能力不断发展的过程中，必然要研究的对象，解开复杂运动之谜是认识发展中的重要目标。在漫长的认识发展道路上直至 20 世纪中叶以后，人类才领悟到复杂的运动有些共同的规律，是由多种联系相互作用相互影响而形成的有机的、有特点的统一运动体，这种运动体称之为“系统”。形成这个概念是一个重要的突破，因它不同于西方惯常的分析思维，即“还原论”的思维方式，而是承认“综合”的重要性。对复杂运动的认识主要是要掌握其综合性，要在分析的基础上进行综合，认识其整体运动规律。所以我们认为“系统”是在研究复杂运动的过程中所形成的概念，是客观存在于人脑的一种反映，它是真实的，而不是凭空臆造出来的。这个概念一经提出，便引起了很多科学家和技术专家的浓厚兴趣，他们纷纷响应并从各方面进行了研究，试图掌握和应用。这种研究在 20 世纪 40～50 年代至 60 年代形成高潮，在研究系统的普遍运动规律领域形成了系统理论，在实际应用领域形成了系统工程学科。系统工程包括了运筹学等学科分支，在很多领域，特别是用于复杂大型工程项目管理组织中都取得了可喜的成功。如二战中盟国运输船队采取有效的保护措施减小损失，完成重要运输任务；美国宇航局出色完成计划庞大复杂的阿波罗登月等。在我国，古代战国时田忌赛马的策略（孙膑之计）就是早期运筹学思想的出色应用，钱学森先生关于复杂系统理论的研究结果和倡导的方法则是现代的杰出范例。在系统理论方面，作者认为普里高津教授的耗散自组织理论是一个重要突破，在系统理论发展方面具有战略意义和里程碑作用。同时也应看到，系统理论及应用学科的发展尚处在初期阶段，其学科领域体系结构远未达到完备的程度，对其基本规律的认识也还很不充分。系统科学与技术是密切关联到人类对复杂事物的综合认识，并取决于人类掌握的科学技术全领域的水平。人类对复杂性非线性科学、生命科学、思维和认知科学等领域之研究都处于初期阶段，在高潮兴起后，必然会碰到种种严重困难，而跌入低潮。我们应该认识到处于低潮状态并不是消亡，而是处在理性思考和潜心研究阶段，也是进一步发展的前夕。因为系统科学技术是一个人类进化发展中必须解决的重要课题之一，是一种客观要求。本书不可能详细讨论系统科学问题，只能作一简单介绍，利用其为信息安全和对抗问题自顶层往下层进行研究打基础。

1.2　系统的定义及其要点解释

现在对系统的定义有几十种之多，学术界、科技界并没有统一的认识，本书给出一种定义。

1.2.1　系统的定义及要点说明

具有对外部功能，自组织机能，开放耗散结构，并由多元素组成的多层次、多剖面的复杂动态综合整体称为系统。

定义中要点说明如下

· 开放耗散结构："结构"与外部，不断地有物质、能量、信息交换，并能耗散，由不可逆运动过程必然产生的熵使结构能保持有序运动的非隔绝保守结构称为开放耗散结构。

· 信息：事物运动状态的描述与表征。

· 自组织机能：是由内部结构间相互关系，以及内部结构与外部环境所形成的功能关系所组成，由无组织的混乱状态向有序状态演变及保持事物有序运动的机能。

· 序：在总体层次上所存在的运动规律。

· 系统简明含义是指具有以"系统"为特征的运动着的事物，具有内外相互约束、有机结合的功能，是一种客观存在的事物。

综上所述，"系统"是一类客观存在的事物，因其"结构"特性而形成了复杂的多层次和很大数量的相互交织关系（既有与外部的关系形成系统的功能，也有内部结构间的关系），正是这些交织的关系，形成了总体运动规律。随着事物的运动，这些规律也在变化，称为自组织机能。要强调的是，自组织机能并不是只有生命体才具有；生命体当然有自组织功能以维持生命的继续，但非生命体系统，也有自组织特性，它虽不如生命体那样神秘，但也很复杂。以下章节将进行系统运动规律的讨论，并不是专对生命自组织功能的复杂运动规律进行讨论（现在尚未很好认识），而是对普适基础性自组织功能进行讨论。

1.2.2　"关系"的概念

前面提到了"关系"，这是一个重要核心概念，因为它反映了事物间的普遍联系、互相作用、互相影响，还可视为"运动"、运动状态、运动结果的具体表征，还可由关系叠套作用而形成复合关系，如亲戚之亲戚关系、朋友之朋友关系、合并关系、传递关系等等。有的复合关系中前后次序不可变化，并不存在普遍可变换关系次序的情况，例如舅父的儿子为表兄弟，儿子的舅父是舅兄弟而不是表兄弟，这是关系前后次序不能变更之例。

人们通常按一定特征将"关系"分为很多种类，如物理关系、化学关系、数学关系、人际社会

关系(如朋友关系、婚姻关系、血缘关系、法律关系、感情关系等),不同类别关系有不同的定义和特性,现简要分述如下。

一、数学上定义的一些重要关系

设 A 为集合,D 为二元集合[对,错],定义一个 $A\times A$ 表示集合中两个元素按某规则 R 形成的组合,并考察它们到 D 的映射,如果 $a,b\in A$,$aRb\rightarrow$对,则称为 A 的元素间的一个关系,也称 a,b 之间符合关系 $R(aRb)$;$aRb\rightarrow$错,则称 a,b 之间不符合关系 R。

以上是"关系"由映射、概念来定义。数学中已知有非常多的关系,并还在不断寻求新的关系,数学定理在一定意义上就可看做是一种约束条件下的关系,现举几个例子说明。

数学中的等价关系是一个重要基础性"关系":用$\backsim$表示,等价关系的性质有三条,即:

① $a\backsim a$ 自反性;

② $a\backsim b$,则 $b\backsim a$ 对称性;

③ $a\backsim b,b\backsim c$,则 $a\backsim c$ 传递性;

注意:c 为$\vdash a$,$\vdash b$($\vdash a$ 表示非 a),否则将使 $a\backsim a$ 失去独立性。

等价关系的重要性在于作为划分集合的准则,有以下定理:"集合 A 中划分子集必有一等价关系与之对应",这是用自然语言表示的数学定理。证明这条数学定理要用数学方法,首先要转到数学的语言及数学证明的逻辑构架,再用已有的数学知识(定理等)进行证明。

定理:一个集合中,子集合的划分对应一等价关系。

设划分集合依照一准则,符合准则者进入子集合,设准则为$\backsim$,设子集合中元素有 a、b、c 等,则有 $a\backsim a,b\backsim b,c\backsim c$(因为 a、b、c 已进入子集合,故符合准则),其中 a,b,c 都符合$\backsim$,所以 $a\backsim b,b\backsim c,a\backsim c,b\backsim a,c\backsim b,c\backsim a$。

其中$\backsim$具有对称性、传递性、自反性,故$\backsim$为一等价关系。

定理:一等价关系可划分一子集合。

设集合为 A,等价关系为$\backsim$,根据自反性可由 A 中任意挑出满足 $a\backsim a$ 的 a,由 a 按 $a\backsim b$,…挑出 b,c,…即可构成子集。

由于 $a\backsim b,b\backsim a$,先挑出 a 或先挑出 b 无区别,推广至任意挑选无区别。(步骤 2)

由于 $a\backsim b,b\backsim c$,则 $a\backsim c$,说明使用$\backsim$挑选元素无其他限制(如 $a\backsim b,b\backsim c,c\backsim d$,…串行链)。(步骤 3)

由步骤 2 及 3 证明了定理的完备性,即划分子集合用等价关系即可完成,不需要其他条件。

以上两定理的证明没有用其他数学定理加以支持证明,这种证明是最简单的。它表明了集合与等价关系间的关系。

数学中的相似关系:在等价关系中削去传递性,即消去一种约束,形成了较等价关系弱的相似关系,"相似"一般不存在传递性。儿子像父亲,儿子像母亲,但父母不见得相像。数学中

这种种运算也可看做“关系”，而运算更广泛的认识可认为是一种映射，故映射又可看做关系（数学中“关系”定义由映射开始的原因就在于此），“集合”可看做关系的集合。同构类关系是一种复合关系（集合映射和运算的结合）。

设 a,b,c 和 a',b',c' 分别为两个集合 A 及 A' 中的元素，$\cdot$ 和 $\overline{\cdot}$ 分别为两个集合中各自定义的一种运算，Φ 为自集合 A 至集合 A' 的映射，即 $a \xrightarrow{\Phi} a', b \xrightarrow{\Phi} b'$。（$\Phi$ 为一一映射）。如果 $\Phi(a \cdot b)=\Phi(a) \overline{\cdot} \Phi(b)$，则称 A 集合与 A' 集合在映射 Φ 及运算 $\cdot$ 与 $\overline{\cdot}$ 下构成同构关系。同构关系是一个重要关系，在科学技术领域广泛应用，它是“相等”关系的推广，即广义的相等关系（在运算 $\cdot$ 及 $\overline{\cdot}$、映射 Φ 的意义上），也是一种条件严格的关系。此外还有条件较宽松的同态关系等。

二、关系在系统理论中的定义

系统理论中定义的“关系”含义比较广泛，体现事物间广泛复杂的联系。“关系”表征：

- 事物间各种相互作用称为存在某种关系；
- 事物间各种相互作用结果以状态表示（也称存在某种状态关系）；
- 事物间的时空比较状态；
- 事物由某种存在状态在一些作用激发下形成的状态转移。

三、系统理论中涉及的几类重要关系

- 功能关系：专指系统与“环境”发生的主要相互作用，它使系统得以生存，实际上“功能”是由系统内部多种交织“关系”中一组与外部环境发生某种重要关系者，称为功能关系，功能关系的主要内容是“功能”。

- 结构关系：系统内部各部分之间相互作用称为结构关系，其中主要内容构成结构。“结构”按层次组成划分为分系统、子系统、子子系统结构，上一层次的结构关系在下一层次可能成为跨两个子系统之间所形成的功能关系。“功能”和“结构”的划分要依据观察基点而定，这些相互间的关系，形成了系统结构的动态存在，同时也形成了系统层次的“功能”。可以认为系统的“结构”与“功能”，即哲学上称之为事物的内因，它的实质是动态的相互作用及其动态关系可以表征系统的生存。

- 约束关系：“功能”、“结构”的实现和存在是有条件的，实现“功能”、“结构”的前提条件、限制条件，以及所需的支持条件称为约束关系。约束关系根源于人理、物理、事理、生理对事物的约束，最严格和不容逾越的是法律体系所规定的约束界限。深层次的约束关系是以规律的形式出现，也可以是技术状态水平之限制。约束关系的约束作用是体现在对象间的时空运动中，约束作用的表现形式多种多样，例如可以是时间维上的连续作用，也可以是不连续的阶段性作用；又如法律的约束作用也区分为违法和犯法，有着不同程度的惩罚。约束关系具有体系

特征，如构成“约束”的约束，不同层次、不同剖面、不同时间有不同的约束条件，它们的集成构成约束体系。约束关系是关系的一种，是事物互相作用中对某种作用起约束作用的“关系”。

四、“关系”的概念形成及“关系”作为一个概念由其内涵与外延角度划分“关系”间的关系

关系的深化及概念的形成：概念是人对事物深化认识所形成的本质概括，人们往往利用概念和形成概念的思维模式进行新的认识，深化认识各种关系同样得到概念（称为关系概念），利用关系概念研究复杂关系集群组成以及“关系”间关系都很有利，后面将利用概念的内涵与外延研究“关系”间关系。

· 种属关系：一个“关系”的外延被另一个关系的外延全部包括，成为其中一部分，外延大者称为种关系，小者称为属关系，“属关系”内涵多，除“种属关系”所涉内涵外，尚有独立所有者。

· 并列关系：在一个种关系下，平行的两个或多个属关系，其外延互相排斥者（不能兼者）。

· 交叉关系：“关系”的内涵与外延，部分不同，部分相同者。

· 同一关系：两个关系外延完全相同，但内涵不同或不完全相同者（体现事物多剖面特性）。

· 对立关系：是一种特殊形式，即并列关系中其外延相互对立，处在两端位置的属概念。

· 矛盾关系：是一种特殊并列关系及对立关系，两个属关系外延的和等于种关系的外延。

· 由系统之功能关系、结构关系及约束关系的关系概念分析，系统同时可具有以上关系。

五、“关系”的维系间对象的关系

设对象为 X、Y、Z，则产生如下维系关系：

· 相似关系：X 与 Y 相似。

· 时空比较关系：X 比 Y 大，X 比 Y 前、后，X 比 Y 早、晚……以及时空关系组合。

· 占有关系：X 中有 Y，X 控制 Y。

· “是”关系：X 是 Y……

· 继承关系：X 某属性遗传给 Y，Y 继承 X 的某属性。

· 因果关系：X 是因，Y 是果，由 X 产生 Y。

· 矛盾关系：X 与 Y 为矛盾关系。

此外还有成员关系、部分关系、组成关系、类关系等。

六、“关系”的时空展开和“关系”的变换

时间、空间是物质存在的基本形式，事物的存在必然在时间、空间域展开，事物的运动可用一系列关系表示，因此“关系”必定在时空域展开，“关系”的时空展开有多种样式，可单独考虑

在时空域分别展开。全面表示事物运动，则应以“关系”在时空域联合展开较为确切。以连续状态表征运动，则常以$\frac{\partial}{\partial t}$，$\frac{\partial^2}{\partial t^2}$，$\frac{\partial}{\partial x}$，$\frac{\partial^2}{\partial x^2}$，$\nabla$，$\nabla^2$ 等原“关系”在时空动态展开，而在离散状态下则对应以差分方程及离散序列组表示。

在众多关系中，变换关系是一种重要关系，它是将事物性质变换至另外剖面进行表征，如将“性质”看做一种“关系”（即以关系表征性质），则变换关系也是“关系”变换，例如傅里叶变换是将信号在时间域的关系转换至频率域的关系，变换关系的内容还可以是关系集合（不仅是单一关系间变换）间的变换。例如，人工系统设计选择不同方案时，不同方案组成的集合可认为是由“功能”保持不变，“约束”经变换而形成各自不同的集合所组成，因此常概括地说设计实质是利用变换所形成的变换结果。

“关系”是一个重要而灵活的概念，利用各种“关系”研究事物运动、研究系统非常重要。

1.3　系统理论体系初论

1.3.1　哲学——系统理论体系中的基础层次理论

唯物辩证哲学是最基础和普遍的研究事物运动的学问，尤其是矛盾对立统一律，量变质变和否定之否定被认做唯物辩证哲学的核心理论。矛盾对立统一律可看做是辩证哲学公理（以后将加以详细讨论），它支持了唯物哲学的发展（在发展具体内容时往往与相关领域的专门学问相结合，同时体现了辩证哲学的普遍性），以下举两个例子说明唯物辩证哲学的科学性和发展性。

例如，经典的唯物辩证理论中论及时间和空间的概念时指出了它是物质存在的基本形式，这是最基本的和普适性的论述，但并没说明时间和空间之间的关系，在牛顿力学体系中也没有论及，发展到狭义相对论才在惯性系中，科学地并美妙地用数学表达了空间和时间的相关性，这是对经典的唯物辩证理论中时间、空间概念之重要发展和补充。

常用思维模式如图 1.1(a)所示。认为是 A 不是 B，是 B 不是 A（形式逻辑模式）；但辩证思维则认为在一定条件下 A、B 可以互相转化，如图 1.1(b)所示，A 不是 B，但 A 又是 B，辩证思维模式是可普遍应用的。因事物是复杂多层次的、又是动态发展之辩证过程，如 A 代表“对手”，B 代表“朋友”的场合，按绝对化的思维模式，则有，是 A 不是 B，是 B 不是 A，是一种绝对“划分”。即，不是朋友就是对手，不是“对手”就是“朋友”，这种概念实际上常常是行不通的。

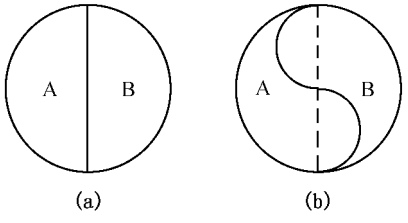


图 1.1　两种不同的思维模式示意图

因为朋友间也有矛盾，对手间也往往有共同点，即如图 1.1(b)所示。

一个重要之例子如中国和美国之间的关系，达不到盟友关系，也不是全面的对手(敌人)关系；有的问题上矛盾严重，但友好合作层面也很多。全世界都关注中美两国关系状态，中美两国利益都需要发展这种非敌非友有合作也有斗争不断发展的关系，如果绝对化思维就会错误地决定中美关系发展的方针。

系统理论的最基本学科特点是研究系统的动态运动，由其矛盾的演化孕育系统的发育萌生、成长直至消亡和新生，所有这一切都可看做是由矛盾运动为根源所发生的运动过程，而矛盾对立统一律是最基本规律。又因系统理论研究的对象是“系统”，具有非常广泛的内涵和非常多的运动类型，需要以唯物辩证哲学作为基础理论加以支持。

1.3.2 耗散自组织系统理论体系及钱学森的开放复杂巨系统理论

耗散自组织理论(dissipative structure－self organization theory)是正在发展的一个学科群。普里高津教授所提出的耗散结构理论作为耗散自组织系统理论的奠基性理论，有着第一原理的意义。耗散结构是构造系统自组织特征的基础条件(必要条件)，自组织特征是事物作为一个活的系统的最基本的特征。在研究发现了系统这两个重要基本特征后才有可能较科学地研究系统演化问题(演化核心机理是新“序”产生及演化过程)，由演化和与“环境”相互关联作用进一步将耗散自组织原理延伸至复杂事物相互关联作用的体系研究中，耗散自组织理论是现代系统理论发展的重要基础之一。

它是系统理论的本体核心，同时作为一个理论体系，也在研究发展之中。这个理论体系的实质用普里高津教授的话来表述，就是研究演化着的世界，即一个进化着的系统。

一、普里高津教授提出的耗散理论及其要点

1. 保守系统与开放系统

系统按其与“环境”的关系可在理论上划分为(与环境不发生关系即与“环境”没有物质、能量、信息交换、交流)保守系统与开放系统两类。保守系统在经历了时间流逝后所处状态必定是平衡态，物理热力学第二定律指出此时保守系统之熵达到最大值(而无熵流产生)，同时保守系统的状态函数在空间是均匀的，在时间上是不变化的，即时空稳定不变。普里高津指出保守系统的宏观序为零，即宏观无序，这种保守系统在研究系统演化中是无意义的，不必多加研究。

开放系统与环境有物质、能量与信息的交流，因为有“交流”，必有“流”(广义之流，而不一定是某种液体流)，有流必有形成“流”的广义推动力，简称“力”(广义)，它实际上是某相关物理量(状态函数)在空间分布的梯度$\frac{\partial T}{\partial r_i}$，$T$ 为某状态函数，r_i 为空间坐标分量。根据“流”与“力”

的关系可有线性关系，即 $J_k=\sum_{i=1}^{n}a_{ki}x_i$，其中 J_k 为第 k 种流，x_i 为 J_k 中的第 i 种推动“力”，这种情况多在系统状态距离平衡态不太“远”的状态发生，即 x_i 数值并不太大（平衡态下 J，x 都为零）。虽然“流”与“力”之间的关系很复杂，但在参考点（现参考值为零）附近用级数展开并取一阶线性近似是可以的。这种状态平时称为非平衡线性状态，物理学家昂色格发现了一个在非平衡线性区的对易定理，即 $a_{ki}=a_{ik}$，即 i 种“力”产生 k 种“流”的效果等同于 k 种“力”产生 i 种“流”的效果。

在非平衡态线性区可能出现这种情况，即系统状态函数的空间分布有差异，但不随时间而变化，这种状态称为非平衡定态。例如一个金属杆一端与沸水接触，一端与流动冷水接触，当时间足够长时杆子上各点温度不相同（但不随时间而变化），按普里高津教授所提出的 $\Delta S=\Delta S_i+\Delta S_e$ 公式分析熵的变化率，$\Delta S=0$。这时各点之温度都不变化，温度梯度也不随时间变化，即 $\dfrac{\mathrm{d}\dfrac{\partial T}{\partial r}}{\mathrm{d}t}=0$，但 $\dfrac{\partial T}{\partial r}\neq 0$，杆子由沸水中稳定吸热而向冷水中散热，有熵的流动，$x_iJ_i\neq 0$，但不随时间变化，此时便会存在 $x_iJ_i=e$（熵产生的时空密度）。事实上，当存在有不可逆的热力学现象时，就必然会有内部熵增加 $\Delta S_i>0$，但由于与外界有能量流进、流出，ΔS_e 是负的，在此熵增加率为零，即熵值不变化，这也验证了普里高津教授所提出的著名的近平衡态，熵的产生率最小定理。

2. 最小熵产生原理

非平衡非线性状态，此时“力”与“流”间呈复杂的非线性关系，也称远离平衡态，普里高津教授认为只有在远离平衡态的开放系统才可能使系统产生新的序，在非平衡线性态熵是不变化，熵的产生率最小，此状态是无法产生新序的。这可以从两个方面来理解：即一个新序的产生要经过混乱无序斗争才可达到有序，无序斗争体现在熵的度量上，先是熵的大量增加，然后是大量减少形成新的序。在非平衡线性定态熵增加率最小，很难“破”，不“破”就很难“立”，故不可能产生新的序。另一方面，在非平衡线性状态，因为线性特性只可能有量的变化，而不可能有质的变化，故不会有序产生。普里高津教授认为只有当系统在开放状态，同时外界驱动能力使系统远离平衡态并达到相关突变的阈值以上，使系统总熵值变化最终小于零（而不是零），才会产生新的序，这种远离平衡态可产生新序的结构，被普里高津称为耗散结构（耗散熵之意）。由于远离平衡态的外界“推动力”只不过是产生新序的条件，新序的实际产生还要依靠系统本身之结构，从这个意义上讲新序的产生是依靠系统的自组织行为，而耗散状态只是最基本的必要条件。

附带指出“耗散结构”的含义，也有学者不仅用在远离平衡态情况而且扩大到非平衡线性态中有序情况，“耗散”是指耗散了熵的增加趋势，故称耗散结构。

3. 两种物理及物理学与进化论的统一

普里高津教授认为：物理学可按其基本定理对时间对称与否的性质，分为“存在”领域与“演化”领域物理两大类。牛顿力学、相对论、电磁理论、量子理论，如在它们的表达式中将 t 换 $-t$，结果不变，时间对称，只能表达存在着的状态，不能表达进化着的事物。进化着的物体，要呈现出“时间对称破缺”，即将 t 换 $-t$，结果绝对不会一样，这是最基本特征。有生命的物体有成长、成熟、衰老、死亡的过程，“时间对称破缺”是其基本特征，这一类演化领域物理则以热力学为代表（“演化”，不等于“进化”）。达尔文的“进化论”是说明和解释地球生物圈生存进化现象的最基本规律，但与热力学第二定律阐述的“熵不断增加”有矛盾——“熵不断增加，生命就很难维持，更谈不上进化。

普里高津教授提出了“耗散结构”概念，即这种结构不是封闭的保守结构，而是“开放”结构，与外界（即外系统）有物质、能量及信息的不断交换，并有一种机制能够不断耗散，内部由于不可逆过程必定产生熵，使结构内部总的熵不会增加（有时反而会减少）。这种重要之机制称之为“耗散”功能，它的重要性在于：它消除了原来物理热力学与进化论间的矛盾，发现了物理学新领域，发展了物理学熵的含义及作用，奠定了从“存在”到“演化”的基础（桥梁），也丰富发展了唯物辩证法（可结合下小节理解）。

二、耗散自组织理论的核心观点是构成系统理论本体的核心

耗散自组织理论是一个体系，现仍在发展中。各研究分支所取得的成果不断充实发展了体系内容，其核心概念是：运动生存着的物体必定要“开放”，与外界有物质、能量及信息的交换，在此前提下，由物体内部结构与外部组成复杂的非线性互相作用的关系，形成物体整体运动规律（宏观秩序），并称为自组织行为。由熵角度看即表示为 $\Delta S=\Delta S_1+\Delta S_0$，其中 ΔS 为体系总熵增加值，ΔS_0 为由内部结构与外部环境相互作用（物质和能量的流入流出）所形成的熵流，它为负值，抵消由内部不可逆过程所产生熵的不断增加值 ΔS_1，使得总熵不增加甚至减少，这种机制称为耗散机制。它区别于热力学第二定律。具体自组织机制是复杂的，并互相组合形成了事物的各种复杂运动。从“变化”角度看有“量变”也有“质变”，从动力学角度看是远离平衡状态，并具有非线性的性质才能有产生新序的可能（体现在整体运动规律及控制参数作用上），产生新序后的系统演变成相对稳定的体系结构，与后续量变过程衔接就蕴涵了系统发生“演化”、“进化”的进程。在一定条件下再形成由量变至质变接续第二轮变化并将延续不断地循环。

“系统”是事物运动普遍存在的一种复杂形式，对其研究的系统理论必然涉及“存在”、“演化”问题，即系统的产生、发展、存在以及衰退、消亡等问题，其中主要内容是将系统看成一个整体，并结合与其他系统间相互作用的关系进行研究。当人们对千百万种令人眼花缭乱的系统及其复杂运动进行研究并提炼最普适本质动力学规律时发现，耗散自组织性质是一切运动系统共有的基本规律，因此它被认为是系统核心基础理论。另从讨论“演化”的核心机制而言，耗

散自组织理论还支持了自然辩证法对立统一规律中，事物发展是内因与外因的结合，内因为主的著名论点。

三、耗散自组织理论体系重要分支理论及相关理论

自普里高津教授提出耗散自组织基本概念及论证其普遍存在的基础性和重要性以来，很多对复杂性问题及系统演化问题的研究，直接或间接地发展补充了以耗散自组织概念为基础之各相关剖面的内容，并形成了一个发展中之科学体系，以下的章节中还将重点介绍其中的一些内容。首先介绍自组织动力学，这是因为在建立了耗散理论之后，紧接着便自然而然地需要研究系统在具体环境中如何通过自组织功能形成具体序之机理问题，这就是动力学问题。这方面有较多的研究文章和专著，现着重介绍其中几个重要分支。

1. 布鲁塞尔器

普里高津教授在提出耗散理论之同时也提出了一个三分子反应模型，称为布鲁塞尔器(Blusseletor)，它由下列四个动态关系组成：

$$A \xrightarrow{K_1} X \tag{1}$$

$$B + X \xrightarrow{K_2} Y + D \tag{2}$$

$$2X + Y \xrightarrow{K_3} 3X \tag{3}$$

$$X \xrightarrow{K_4} E \tag{4}$$

其中 A，B 在反应中不断消耗且不断得到外界补充；D、E 为结果，一旦形成则立刻被取走；X、Y 为状态变量，是不断变化的。这个模型用途很广，它表征了自组织特性，其中，式(3)是一个非线性的自催化环节，在模型中起重要作用(其中 Y 起支持催化作用)，箭头→有多种含义，如形成、演化、产生……符号“+”是广义“加”，如支持、加入起反应、补充作用等，例如模型可表示基础知识 A 演化成理论 X，理论 X 在 B 支持补充下演化成理论 Y 及结论 D(D 可看做成果)，将 X 扩充结合 Y 形成更广泛、更完备、更丰富的 X 理论体系，X 理论体系发挥作用得出成果 E。

2. 协同学

下面介绍耗散自组织理论动力学部分的另一重要分支——协同学。

协同学由德国学者哈肯教授所创立，它研究事物由无序变为自组织性有序的规律。哈肯教授发现不同种类的事物其变化往往有相似的现象和规律，进一步研究这些共同规律，形成了较有普遍意义的系统性方法并较深入地说明了自组织机理。协同学研究的范围很广，除了无生命的系统外，还包括有生命系统，如生态系统(生物系统扩大形成的生存循环系统)、社会系统等。系统共性和自组织性是在一定宏观(整体)层次出现的，越往微观层次，差异性越大。在有序情况下还存在着很多方面的无序，系统的多层次多剖面特性是复杂性客观存在在此处的

体现。协同学认为仅限于熵的概念去描述系统是不够详细的，因而进一步利用序参量结合运动状态相互关系进行偏重宏观层次的定量描述，在一定范围内的宏观和微观的结合，研究系统运动（含相变）。通过运动模式及少数序参量来表征运动是一种很好的方法，如表征一个弦的振动，只需用其振动幅度与频率便能很好地概括与表征。如表征一个人的脑思维，决不能用电化学的方法以每个脑神经细胞的活动来表示，而是用思维以及思维模式特点来表征（脑神经细胞的活动作为基础要研究，但不能用于表征一个人的脑思维特性，它距离脑的思维整体层次太“远”了）。因此，可认为协同学基础理论是原有科学方法的提升和集成。

协同学研究运动模式及序参量问题。结合客观存在的随机起伏运动以及系统复杂得多体情况，分层次分剖面利用统计数学及分析数学进行宏观层次的扼要（模型化）的定量分析（没有利用模糊数学），在定量分析中发现各类系统性事物运动都具有自组织特性；对系统的运动可分别就变量间关系建立等同于独立变量个数的微分方程组，并利用变量作用的衰变常数间相对大小（弛豫时间长短）化简系统分析的复杂性，即作用动作快的变量近似看做无滞后地紧跟缓慢变化变量形成“近似绝热过程”概念，在绝热近似的简化基础上能简捷地找出支配变量（对应小阻尼），它支配（役使）大阻尼短寿命的跟随变量，从而形成“役使性”的自组动力学原理。协同学用动力学微分方程式的定态解表征含时解的稳定结果，由“解”的状态还表征了系统稳定性问题，由此进一步与研究稳定性理论分支发生联系。由一定条件下形成的非稳定性突变被看做系统质变，质变往往会使系统产生新的“序”而进入一个新阶段，然后又转成量变新过程，哈肯教授详细分析激光形成过程，证明无生命系统在一定条件下完全可以具有自组织功能，从而使系统产生“序”，同时也进行自组织的有序运动。协同学还研究系统在随机环境中，包括自组织动力学内容的分析方法等，在此不作详细介绍，有兴趣的读者可参阅哈肯教授的协同学专著。下面简单分析绝热役使原理以说明自组织功能的发生往往寓于简单系统中，从而加深自组织功能以及可普遍适用的概念。

由朗之万方程谈起，该方程为：$\dot{q}=-\gamma q+F(t)$，$\gamma>0$，$F(t)$为外力。

设 $F(t)=a\mathrm{e}^{-\delta t}$，$\delta>0$，如不考虑系统过程，可得

$$q(t)=\frac{a}{\gamma-\delta}(\mathrm{e}^{-\delta t}-\mathrm{e}^{-\gamma t})$$

如 $\gamma\gg\delta$，则

$$q(t)=\frac{a}{\gamma}\mathrm{e}^{-\delta t}\equiv\frac{F(t)}{\gamma}$$

表示当系统固有时间常数远小于外力（也可理解为输入的命令）的时间常数时，即 $\tau_1=\frac{1}{\gamma}\ll\frac{1}{\delta}=\tau_2$，这时等价于上面微分方程中的 $\dot{q}=0$。得到，$q(t)=\frac{F(t)}{\gamma}$，其意义即系统立即响应“命令”。

哈肯教授称这种处理方法为“绝热近似”，在简化复杂问题时扮演重要角色，如把“命令”对应“热能”，则意味着“热能”不失散，全部发挥作用，“命令”不走样地被执行。

再进一步由“命令”演化为自组织。设系统方程为

$\dot{q}_1=-kq_1-aq_1q_2$，　$\dot{q}_2=-\lambda_2 q_2-bq_1^2$　　（q_1，q_2 是状态变量，k、λ_2、a、b 是常数）。

当 $\lambda_2 \gg k(\lambda_2>0)$ 时，对应于系统的时间常数为，$\tau_2=\frac{1}{\lambda_2} \ll \tau_1=\frac{1}{k}$，则又可利用“绝热近似”。

令 $\dot{q}_2=0$，则 $q_2 \doteq -\lambda_2^{-1}bq_1^2$，从而 $\dot{q}_1=-kq_1-k_1q_1^3$，　$k_1=-\frac{ab}{\lambda_2}$ 这称为 Pitch－fork 分岔方程，由它解出 q_1，然后得到 q_2，q_1 可看做支配变量或称为序参量，q_2 称为跟随变量，q_2 对应短寿命系统，长寿命系统支配短寿命系统，短寿命系统又反作用于 q_1 形成相互作用。当系统参数给定，以及参数变化时，q_1、q_2 形成一定的运动规律（包括分岔、体现老结构让位新结构、新的序，通过涨落达到新的有序，自组织进化范式等理论）。

对于一般情况而言，系统方程可表达为

$$\begin{aligned}\dot{q}_1 &= -\gamma_1 q_1+g_1(q_1,\cdots,q_n)\\ \dot{q}_2 &= -\gamma_2 q_2+g_2(q_1,\cdots,q_n)\\ &\vdots\\ \dot{q}_n &= -\gamma_n q_n+g_n(q_1,\cdots,q_n)\end{aligned}$$

一般而言，系统方程由两部分组成，一组为负阻尼系数由 $i=1,\cdots,m$ 代表，是系统不稳定的因素；另一组为正阻尼系数从 $i=m+1,\cdots,n$。对于 γ 数值大的微分方程，则可用消去法化微分方程为代数方程，在进行过程中还可将上式近似线性化以求解。在此不详细论证可线性化的条件，如 $g_1,g_2,\cdots,g_n$ 不能线性化，则目前没有很好的解决方法。线性化会带来分析的不准确性，但可以给定性提示方向，找出少数低阻尼慢变化的参量，它起役使作用，其他参量起跟随作用，跟随参量也可反作用于役使参量，这形成子系统间相互关系的自组织功能。少数役使参量称为序参量，这类方程组在实际系统分析中会经常碰到。以上数学表达式简要地说明了“自组织”机理的普遍存在性。

3. 其他工作

在《自组织的宇宙》（美 Jantsch 著）一书中，作者开头便引用了庄子的秋水篇：“故曰，尽师是而非，师治而不乱乎？是未明天地之万物之情者也。”作为辩证思想之基础思维，提出了自组织范式，以阐明包罗万象的进化现象，包括：宏观有序、耗散结构、自组织、通过涨落达到有序（系统进化），大小宇宙的共同进化（实在的对称破缺史），自我超越，走向进化的系统论，进化过程之进化等新理论。

在《自组织的自然观》（曾国屏著）中，作者着重论述自组织演化论，在发展范畴内讨论各剖面的核心因素，同时与辩证法相联系且由更大世界范围的论证研究了自组织理论的深层次作用和意义。

此外，还有一些间接的相关工作，如《正反馈》（郑维敏著）中提出的 反馈理论。反馈是事

物演化的重要模式，在进化过程中，适者生存要靠反馈来实现。人类区别于动物，很大程度上在于有意识的反馈，也就是更聪明、效率更高的反馈，而高效率的反馈必须建立在深刻理解规律和原因的基础上。耗散自组织理论的具体应用，是反馈过程中最基础和最重要的工作，一般情况负反馈多用于稳定发展进化的量变阶段，人们已熟悉并用得较多；在质变过程中旧序的破坏、新序的建立，往往脱不开正反馈，正确理解和利用正反馈，是一种进步，深入研究正反馈也是一项很重要的工作。

突变理论和分岔理论，是研究某些非线性特性的。在一定条件激励下，产生质变，这实际上是一种常见的自然现象，也是在物质进化过程不可少的模式。此外还有混沌、分形的研究，是针对自组织中偶然与必然的结合与互相转换，这种结合与转换是一种深层次之客观存在。对耗散自组织理论所形成的科学体系的广泛内容而言，尚有很多重要工作，在此不能一一罗列。

四、钱学森提出的系统新理论

钱学森教授以系统工程及工程控制论为基础，进一步延拓至系统理论与思维科学的研究，提出有人介入并起重要作用的系统为“开放复杂巨系统”概念，对这类系统提出了“从定性到定量的综合集成”的科学研究方法，是对复杂系统研究的贡献，也是思维科学中处理复杂问题的一种重要方法。钱学森教授提出的新概念、新方法是一个开创，值得继续深入研究和发展。

五、小结

自组织动力学研究系统演化动态过程。除上述内容外，过去较少研究的质变阶段，现有很多学者从事这方面研究并取得了一些成果，如正反馈理论，突变与分岔理论等。研究突变现象与研究系统稳定性问题有密切联系（理论上、概念上一脉相承），这方面研究也补充和支持稳定性问题的研究和发展，但仍有很长的路要走，仍有待根本性的突破。对于“突变”的研究可能会形成一个称为突变理论的专门分支理论。

自组织动力学领域是一个尚不完备的开放式动态学科发展体系，它不可避免地涉及复杂非线性科学，与很多前沿科学分支都有较密切关联，如混沌理论、分形理论、神经网络理论部分。有学者也将其归入自组织动力学领域中。各学科分支相互交织关联是事物广泛交织关联的客观反映，一成不变固定的学科“划分”不科学，也不可能满足人类认识不断发展的需要，以“自组织”作为基本概念与其他学科进行融合发展，从而丰富我们对事物动态发展的认识能力。

1.3.3 耗散自组织理论概念及原理的延伸讨论

研究复杂系统的演化问题是人类多年孜孜探求问题之一，面对复杂问题单纯依靠分析思维还原论方法肯定无法较彻底科学地认识。人类自觉和不自觉地寻求系统总体性地认识复杂

动态演化问题的理论和方法，耗散自组织理论便是这样一种方法，它具有概括性和普适性，且生命力很强，但尚不完备，需要不断检验和补充完善。耗散自组织理论的普适性和基础性，在其发展中必定要结合哲学基本理念共同研究，以下即按此思路对耗散自组织理论内容中的概念和原理进行延伸讨论。

一、耗散自组织理论体系蕴涵相对性和绝对性问题

绝对性和相对性问题是辩证法最重要、普遍、基础的范畴，并有广泛应用。因此，对立统一范畴在耗散自组织理论中应有其具体理解。“绝对性”应理解为生存（运动）系统都遵守耗散自组织规律，规律的基础性、普适性是绝对性的体现。更重要的是其相对性，主要体现有两点：第一，耗散自组织理论仍在发展完备中；第二，理论体现在各类具体系统，都是有具体的多层次先决条件，这些条件是复杂的，也是变化的，并涉及各类科学的较具体规律。自组织耗散理论虽是普适的、重要的，但绝对代替不了各专门领域的规律和知识，只有与之相互结合才能科学地发挥作用。

二、复杂的对称破缺问题——“时间和空间对称破缺”有待深入研究

“对称破缺”是一个复杂的多层次、多类型、值得不断深入研究的问题集合，进化系统的“时间对称破缺”，是以时间剖面的“不可逆”体现了重要、普适的系统运动本质特征。进一步研究各种事物时间与空间的各种结合的对称性关系，是一个复杂问题，如摩擦力（运动物体与其接触物之间的作用）必定与运动方向相反，地心吸引力永远向地心，热流只能由高温热流向低温热流流动才能做功都是体现空间不对称性。有很多事物，在时间上也表现为不对称，对有生命的运动，特别强调在时间过程中具有不可逆转的不对称性很有必要，如细胞的衰老，生命之终结等。总之，时空不对称是物体演化基本特征，值得结合各种系统的演化加以研究。

三、“宏观有序”定律的讨论

该定律说明系统整体层次运动是有规律的，凡总体层次中对系统功能和性质起主要作用的规律，称为“宏观序”。宏观有序并不意味着只有“宏观序”，系统序是系统诸矛盾运动的结果，事物运动必在时空中形成一个序的体系，并具有相对性。下面进行扼要阐述：矛盾主要方面体现主要的序，被统治的矛盾次要方面的逆向序也有表现。每个社会需要正常秩序，如在我国人人尽力劳动，按劳动价值分配。但总有少数人逆而行之形成形形色色犯罪，制造假货，制毒贩毒，贪污受贿，盗窃抢劫，存在各类逆行，虽不是主流，但存在其规律特点，这就是逆向序。进一步细看“运动”内部，也存在“序”的变化差异，前 20 年生产电脑利润很高，现在只能说是微利，工作能力和水平很接近的从事科技的人员专业不同，在不同单位收入差距很大，这属于按劳付酬的大体系内存在不同的规则。还有一部分是按“中性规律”生存，如有人不做坏事，不犯法，不工作劳动，靠父母遗产，兄弟姐妹支援，对社会进步丝毫不起促进作用，但他们合法地生

存着。再看非属于社会生产力领域的家庭主妇集群，她们阶层之序是管理社会细胞——家庭，照顾和教育未成年孩子。有的家庭主妇，文化素养很高，能力很强，家庭管理得井然有序，对小孩的教育做得也很好，就社会整体来说，她们是不可缺少的重要的组成部分，但她们的活动并不算经济领域“序”的组成，这些都表明“系统宏观有序”，对应具体事物的应用具有复杂性。下面将进一步解释：以上是谈论系统运动中，并不单有主要序（序内再包含矛盾主要方面及其对立面），还存在非主要序，这是从主次剖面（角度）来讨论的。现在还要讨论主要序的内部组成，它往往是多层次有机整合，换言之，形成宏观序是由“分序”整合而成，而不是单个序的独立“全程贯彻”，是多个分序有机整合而成，整合模式往往也是分层次的分布式的模式。下面以人的口语为例说明。

口语是人表达思想、感情和目的的一种交流表达方式，组成一段口语是一个非常复杂的问题，详细机理与过程控制远远没有弄清楚。单就一个词或词组的形成就是一个“序”整合之例，发音说话是人类最复杂的神经控制肌肉运动之一，包括了面部、喉、胸腔、腹腔一百余块肌肉的协调运动，这一切都要以非常快的速度完成以匹配说话速度，这么多的控制，绝不是都归结至人脑意识层次（最高层次）来全部毫无遗漏地控制完成，如英语 dilapidated 是由 5 个音节，11 个不同发音，还加入重音控制，每个音都有很多肌肉动作，若都由大脑意识直接调度控制然后组合，那么人说话太累了。实际上每个细微的具体动作绝不是由大脑意识层一一控制，而是由众多的内部模式（预先编制好的存储在脑中的一套动作指令，相当于计算机程序中调子程序）来完成，届时调用各内部模式，否则达不到现在人的说话速度。专家认为那些口吃者的问题就发生在不依靠内部模式，而是下意识地实时倾听自己的发音，进行直接控制，由于大脑反应速度跟不上，使他陷入反馈控制不正常的复杂循环中，从而造成发音不连续，多次中断而又重复一个字音。调用内部模式是非常复杂的过程，细节问题也是一种自组织模式，还远远没有搞清楚。由此我们应理解自组织宏观有序，是一个科学框架性概念（也是一种学说），包括各种极端复杂机理和内容，深入的研究刚刚起步，需要更长更艰难的认识发展过程。对比哲学领域，唯物辩证理论现在虽然建立了科学框架，但仍未被普遍承认，随着人类社会发展、对自然科学规律的不断发现及深入认识，作为科学哲学体系会在发展中被普遍承认。再看自然科学领域激光器的例子，产生的激光束由多个同频、同相的受激粒子同时辐射所致，但细看也不绝对同时、同频、同相（谱非 δ 函数而有离散），说明产生激光的序并不“绝对”。由此推论，根据实际需要在合适的时间空间尺度来分析研究“序”之内涵很重要。

四、“矛盾”概念的进一步讨论

“矛盾”是一个重要概念，各种具体矛盾客观存在于人类社会、自然界及人类与自然界相融合的运动中。在矛盾概念基础上，发现有关矛盾运动规律理论，即唯物辩证理论。它以矛盾的对立统一规律为核心，这一发现可认为是哲学领域的一场革命，在社会科学、自然科学最基础问题的研究中都显示了强大的生命力，像任何“发现”、“革新”一样，被普遍承认都有一个漫长

过程，哲学内容涉及领域非常广泛，更需要广泛地验证。

“矛盾”是用文字表示的概念，与语义学必然有关联。按语义学，矛盾与任何义位一样，是相关语言场中的一员，语义场、义位的内涵与外延同时具有确定性、不确定性和笼统性（并随人类进化而动态变化）。矛盾作为含义非常概括的义位，其相关语义场非常复杂，对此研究是一个哲学有关分支与语义学的交叉问题，在此不多作研究。在系统理论领域的研究工作时时脱离不了矛盾，应着重系统运动的现实矛盾（由现实为背景抽象出的矛盾）进行研究，同时避开单由文字语言上，脱离实际进行讨论。例如张飞和秦琼都是历史人物，如提出“张飞”与“秦琼”间有什么矛盾，这就是一个偏题，因为两者间很少存在重要的相互关系，也没什么意义，如硬要回答，也只能说，两人皆是武将，性格有差异，生存时代不同，环境不同而已。又如问星期一、星期二之间矛盾内容是什么，这个问题比上个问题稍有些意义，但意义也不大。因这两者仅仅是普通名词，只是“星期”这个义位最小语义场中的两个成员，在同一星期中，星期一排在星期二之前。如隔一个星期而言，星期二又在下星期一之前，在固定休息星期六、日的单位，一般来说星期一工作可能更忙些……仅此而已，但如果问，现在中国的信息企业能够成功开发第三代移动通信产品及其服务业务的矛盾主要有哪些？此时所提“矛盾”的意义显著高于前两者，是值得超前分析清楚的重要矛盾，也是复杂矛盾。举这些例子是着重说明：分析矛盾双方往往是不可分离的，一旦强行分离移去一方，矛盾也就不存在了，这说明矛盾统一性对研究分析现实矛盾具有重要性。

1.4　系统理论通常涉及的对立统一范畴

“系统”理论具有诸多对立统一范畴所表述的性质，体现出系统具有多子系统、多层次、多剖面、多过程、多阶段所交织关系的复杂运动特征，以下讨论的几种对立统一范畴，正是从不同侧面表征了系统运动的复杂性。

1.4.1　相对与绝对

这是哲学中争论非常热烈的一对对立统一范畴（在漫长的时间内是按形式逻辑性质争论着，后来人类能够认识到其对立统一的辩证特性是一个很大的进步），它具有宽广的外延和极普遍的内涵，属于哲学总体范畴。它与“有限与无限”、“暂时与永恒”、“整体与局部”、“有条件与无条件”、“连续与间断”等等都有关联，甚至部分有涵盖关系。它还表征着客观事物运动最普遍的基本特征之一。“绝对”表征无条件，无限制，无限范围的整体，无完结的永恒，无依托依靠等等；“相对”则恰表示其反意。但我们更应该认识到这对范畴的重要性、根本性是来源于“相对”和“绝对”的对立统一。“绝对”最主要的表示，也可以说绝对性的“绝对”，是运动的绝对性，和事物对立统一的绝对性。“绝对”中也有其对立统一的“相对”，即无限大范围整体是由

“无限多的个别”所体现和表征，认识也是由对一个个无限多个个体的认识不断累积而成，即整体寓于个体中，绝对寓于相对中，运动是绝对的，客观存在是绝对的，但由具体事物组成又是相对的。用于系统理论的中心课题，即着重“系统”特性的事物运动规律（发生、成长、生存、衰老、死亡），体现绝对的相对概念占有很重要的地位。

1.4.2 相同（相似）与相异

“相同”与“相异”所表达的直观意义是绝对地相对立，但相同与相异总是连在一起出现，表达了重要的对立统一的辩证意义，很多事物都具有形形色色、既相同又相异的特征。很多情况下，“相同”表征“类”或群体特征，而相异则表示个体。如讲同种语言的人的群体，互相都可听懂语言的意思，不同的人所讲语言有区别，所以可用来“识别人”。“相同”在某些意义上意味着“一般”，而“相异”意味着“特殊”。相同与相异的对立统一关系还表现在：事物在普遍层次范围内相同，在细化较具体层次上相异；某些剖面相同，某些剖面同时存在相异，即“空间”不同的范围同时“相同”与“相异”，当然也存在着同空间范围在不同时间的“相同”、“相异”等。还应注意到“相同”含有绝对意义，即“同”是一点无区别之意，实际上事物间很难有绝对意义上无区别的“相同”，只是近似概念，严格说是“相似”（有“同”也有不“同”）。在人工系统的研制中，往往利用事物某些功能相同，但“存在”的约束条件相异，进行按目的性又符合自然决定性的约束的变化来实现人的目的。

1.4.3 必然性与偶然性

“必然”意味着存在规律及规律的作用，而“偶然”意味着无规律性作用，或尚不认识规律。谈论必然和偶然是在一定场合，即一定的空间、时间范围内来看待的，所谓“一定”也不是永远固定，也是随场合而变的。但在论及有关“必然”、“偶然”时，有必要明确时间、空间的界线。事物都在运动变化，没有绝对的必然和偶然，而是必然和偶然辩证地结合，这意味着客观世界的复杂性（无主宰因素或主宰因素的快速变化，也是无规律性的一种复杂体现）。既必然又偶然，必然中存在偶然，偶然中有必然，必然和偶然互相转化。在研究系统时，关键在于寻找其组成及交互式的复杂变化规律，具有必然和偶然相结合的辩证观点观察问题是很必要的。客观事物运动过程中，必然性与偶然性的结合是一种客观存在。人类不断地深化对必然和偶然性的认识，也不断取得成果但“进程”永不终结，尤其在“必然”和“偶然”的结合方面，如概率理论、量子物理、混沌理论的建立都有体现，在经济学、社会学、教育学等包含人的作用的领域，更为复杂也更有待研究。

1.4.4　目的性与自然决定性

人与动物的不同之处在于有意识的目的性(而非生理反应的目的性),及实现目的性的实践能力。目的性意味着未来,是否能实现目的取决于“自然决定性”,所谓自然即客观存在,“决定性”具体化即所有客观事物的存在都有其前提条件,如前提条件得不到满足,则超出了“目的”的约束范围,超出了这范围“目的”是无法实现的。“自然决定性”就是客观条件对新生事物的限制作用,人类新目的的产生来源于人对“需要”的理性物化归纳,由于人认识未来的能力有限,故并不意味着产生的目的一定符合“自然决定性”。如何最大限度巧妙地去“满足”自然决定性,这包含通过“变换”至较宽松的约束条件,以及发展人的能力,从而改变及突破原有“自然决定性”的限制,人类能力所完成的重要未来目标就是一种创造。系统是复杂事物,一个新的人工系统诞生,体现了人完成某种目的与创造的能力,在其实践过程中必然存在严重的目的性与自然决定性相互对立(又统一)的情况,主动理解其中的约束并设法转移“约束”至允许范围内以实现“目的性”是很重要的事。

1.4.5　整体与局部

在系统理论中很重要的一部分内容,是研究整体与局部之间的关系,人工系统的研制其整体的功能是优先考虑的问题,整体功能不等于各局部功能之和,使整体功能大于各局部功能之和是我们追求的非线性跃变关系,应当力求避免其反相关系,但受“自然约束力”的限制,其负面、非加和关系往往客观存在。如多级串联系统的整体能源效率是负面的非“加和”关系(连乘关系),大型多 CPU 计算机效率与 CPU 个数之间也不是加和关系。整体和局部又是相对的,在一定范围内的整体在更大范围内常成为局部,局部也常转变为整体。事物的发展进化,衰退灭亡,都是由局部发生变化进而影响整体,引起全局性变化。整体与局部对立统一的辩证关系是我们感兴趣的热点之一。

1.4.6　复杂与简单

这一对立统一范畴,含义深长。复杂性是世界乃至宇宙存在的表现和根源。人也是复杂性的产物,但又常常避开复杂性去追求简单性,以图顺利解决问题。有的场合人又“追求”复杂性,以体现自己的能力和智慧等。“简单性”是否绝对简单呢?没有绝对简单。简单性和复杂性一样变化多端,并往往与复杂性交织在一起,如有的规律,形式简单,内容却非常复杂。简单中包含了复杂,同时也存在复杂中包含简单的情况。在系统理论中,强调和注意的是复杂与简单对立统一辩证的多方面“转换”。“系统”作为实践的对象,它是复杂的,系统理论是研究“系

统”的运动规律，作为“规律”，比起名目繁多的现象，本质上简单多了，对系统运动的认识要以掌握规律的方式去对待，这就是复杂向简单的转化，在综合问题的场合，用简单的基本规律综合，去解决复杂问题，基本规律本身就是复杂中的“简单”，也代表了“简单”向“复杂”的转换。

1.4.7 量变与质变

“量变”与“质变”是事物运动的基本特征，系统运动也不例外。在此强调两点，第一，即在系统的生存发展中，存在多层次、多剖面的多个量变到质变的循环过程。第二，掌握量变、质变的条件和规律（尤其是质变条件），利用条件顺应规律促使按人的目的产生新事物，新事物的产生要靠质变（突变）产生，然后以“量变”方式加以稳固发展，这是人类进步过程中实现创新的最基本方法。

1.4.8 连续与间断

连续与间断有多种含义：连续可以意味着客观整体的存在的结束和新个体的代替作用，间断意味着个体的存在；连续可表征量变，间断表示量变的间断，质变的产生。连续间断和间断连续的辩证转换是“运动”的基本规律，人们正确利用“连续”与“间断”体现了人的智慧与能力，也体现了对普遍与特殊的正确处理和对待。在“系统”的分析和实践中，要正确利用“连续”和“间断”概念指导实践，因为事物的运动必然是“连续”与“间断”相结合，没有单独的“间断”，也没有单独的“连续”，在运动过程中“连续”、“间断”顺序交替出现，实际上事物按规律与环境条件在空间（广义）、时间交织中不断以“连续”、“间断”方式进行运动。如在“人口连续增加”的导引下，要粮食连续增产，最简单的方法是不断大规模地开荒造田，扩大农田面积，粮食产量连续上升，但破坏了生态环境的循环链，最终生态环境的连续破坏造成一系列气象、水土保持等方面恶化，粮食产量还是增加不了多少，并不是随土地连续增加产量也连续增加，由此例看到一个复杂运动过程中“连续”和“间断”方式，会在不同层次不同阶段关联地出现。所以正确处理“间断”和“连续”很必要。

运动“方式”是一种现象和形式，也是一种阶段性结果，是受“条件”和规律控制的。所以还要结合规律来对待“连续”和“间断”方式交织的运动。

1.4.9 特殊性与共性（特殊与一般）

特殊性是事物存在的必然形式之一，共性是在一定范围内事物特殊性的抽象与概括，即一个个“特殊性”的重要共同点的抽象和概括。事物都是以个性（特殊性）存在的，没有特殊性就无从谈到共性，共性是较大范围事物存在的特征，它在该范围内具有普遍性与概括性，是建立

于“特殊性”基础上对共同点的概括，二者之间互相否定又相互肯定，这就是两者的对立统一，信息安全与对抗领域讨论中，本范畴是经常要涉及的概念。

上述各小节涉及一些对立统一的概念，这些范畴并不完全，每一对概念侧重某一方面（剖面）表述对立统一关系，所有这些“剖面”并非孤立，而是互相交织关联，这些对立统一范畴也互相交织关联。这些概念在科技研究发展中结合实际，正确灵活地思维和运用是很重要的，可较大程度地增大成功的可能性。

深一层的含义是在运动中上述范畴所描述内容常结合在一起进行动态转换。如“共性”在更大范围内就变为特殊性，当环境条件变化后，之前的“共性”很可能变化成“特殊性”等，这对范畴与“绝对与相对”范畴时也可以联系。

对通信领域的发展而言，无缝隙地通信即任何人、任何时间、任何地点、任何情况下可靠通信，无疑是个方向和目的。对具体发展计划而言应是相对的，即是有条件的，不是无条件的，“条件”考虑不全是不会成功的。

对移动通信而言，其特征是移动状态通信，扩充特征是可用在固定骨干通信网络所不能覆盖处，海洋、极地应该全部包括，但这些地点的用户（在现阶段）相异于业务占主流部分的人口稠密、发达或发展较快地区的用户，铱星的无区别全覆盖是不明智的，把该“特殊”对待的事物没有特殊对待是错误的。如铱星系统，本身虽已经很复杂、很庞大，但与人类社会系统开放复杂程度相比只是一个不算太大的分系统，其发展必须融入人类社会系统的发展而共同发展，其中经济因素占不可忽视的地位，忽视使用成本因素后果严重：铱星计划在复杂技术剖面考虑很周到，得到了先进技术支持且很完备，但违反了一个简单规律“老百姓用不起”。铱星计划在先进技术方案集成方面是一个质变发展，也是一个阶跃发展，但其“目的实现”脱离了现实存在被自然决定性所否决，所以失败是不可避免的，是必然的。

1.5　系统理论暂立的公理体系

以耗散自组织理论为核心的系统理论在近期发展历程中，体现出它强大的生命力，但同时也应理解这样一个现实：即用它较完备地认识具体复杂系统的详细运动演化规律还有很长“征程”，在发展征程中也可以参照发展其他学科的常用方法。即针对问题进行反复思索后建立一些基本概念和一些原理，在此基础上进一步深化及普适化工作，并努力找出基本方程的公理体系，然后在基本方程或公理体系基础上进一步延拓、验证，从而建立该领域的完备理论体系，为人类之认识实践服务。在这里要强调说明的是：所建立公理体系是无法由理论上推演的，只能不断地检验其正确性，检验准则有三条，即：(1)无矛盾性，由公理体系中依不同条公理（或公理的联合）不能推论出不同内容，但具有矛盾性质之定理。(2)公理体系具有独立意义最小数量，即组成公理体系的公理数目在互相独立条件下为最小，公理间不能互相推导出。(3)公理体系具有完备性，即本学科领域所有定理都可以依据公理体系推导得出，一个较大学科领域公理体

系虽不要求推导得出但要经长期检验。形成一个科学公理体系是很艰巨的任务，系统理论有比一门“普通”学科更广的适用范围和更复杂的内容。因此完备建立科学公理体系的艰巨性绝不一般，但为了推进系统理论之发展总要有一个“开始”作为开始。由这个意义思考，在本章中特别重要的限定词是“暂立之”，它可能是真正绝对的暂立，即使这样它的“绝对”暂立出现也能起到“引玉”作用。在结束本段之际，再说明各学科公理间的无矛盾相容要求往往促使“公理”在已有基础上的发展。

牛顿三定律是力学运动学之公理体系，它适用于惯性系统，是绝对时空概念，并包含了相对速度概念。由麦克斯韦方程组（可认为是电磁场领域的公理体系）也涉及光速传播但与参考坐标系运动速度无关的运动速度，这样便产生与牛顿力学之矛盾，经科学家努力，爱因斯坦教授的狭义相对论补充了牛顿定律，也解决了二者之间的矛盾，这有力地说明真理的相对性和“真理”在交叉学科领域之交融、验证和发展。

1.5.1 系统理论公理体系顶层公理——矛盾对立统一律

唯物辩证哲学是在最广泛领域研究事物存在的学问（概括地用英文表示为 what is being），人的意识也是一种“存在”（最高级的存在），逻辑上应该包括在哲学研究问题之内，进而必然会发生意识的存在与其他“存在”之间关系问题这样一个重要哲学命题，这个命题等价于人如何认识客观存在的问题，这是哲学最核心的内涵。经过几千年人类的研究诞生了发展中的唯物辩证哲学，它的科学性集中体现在：量变质变律、否定之否定律、矛盾对立统一律，其中矛盾对立统一律最为基础和核心，它揭示了事物发展的根源和动力，其实质性内容有三部分：

第一，揭示矛盾内部客观存在的同一（统一）和斗争（对立）性，其中统一性表示在矛盾对立面相互依赖、相互依存，矛盾对立面相互贯通（在共同之基础和因素前提下互相包含），直接地说是你中有我、我中有你，对立面间存在内部联系而形成互相转换的趋势，而对立性可理解为互相否定、相互反对、相互限制等。矛盾的对立性有着非常多的表现形式，紧接着要理解到矛盾的对立性在不同事物中有不同的对立斗争形式，而且随着事物运动对立的形式也在变化（时空变化性）。最后关于矛盾对立性和统一性关系问题，这也是“对立统一”的，即这两者属性是对立相反的，又是不可分离的，一方不存在另一方也必不能存在，“统一”是以差别和对立为前提的。同样，两个对立面间如无联系，无法相互否定排斥，也就无法相互对立。因此，“统一”是对立中的统一，“对立”是统一中的对立。

第二，矛盾的统一性和对立性是事物变化发展的动力和根源。统一性使矛盾双方互联为统一体而生存着，它是变化发展的前提，发展是以存在为基础而发生的，因为没有某种存在的运动就谈不上这种运动的发展。事物不可能不变化发展，没有运动便没有事物存在，事物不可能不变化的永存。除上述前提条件外，统一性作为变化发展的根源和动力可从以下三个方面来理解：第一方面，统一又对立的双方都在互相吸取对自己有利的因素，在互相利用、相互促进

中发展(包括存在根本利益冲突的对立双方)。例如,战争双方都是利用对方的失误以谋求自己的胜利。第二方面,双方的变化发展都是朝对立面方向转变,而不是其他什么方向,以上可认为是双方变化的"根源"。第三方面,对立双方都参考利用对方某方面的发展以促进自己的发展(一种脱离不开的"激励"),这是"统一"带给对立双方发展的动力。例如,压迫和反抗是矛盾对立双方,压迫越重,反抗越激烈,反抗越激烈压迫越重。这足以说明以上论点。

矛盾的对立性在事物量变和质变过程中都是事物变化的根本和直接作用。在量变阶段,矛盾的对立斗争使矛盾双方力量彼此消长,由对立面的互相排斥、互相否定产生彼长此消的变化过程;在质变阶段,是对立双方通过对立斗争向各自对立转换借此解决矛盾达到新状态之过程,在其中对立斗争起直接和根本作用。

第三,"矛盾对立统一"的普遍性和特殊性。矛盾普遍存在于客观世界中,并且自始至终存在于事物运动过程中,矛盾的对立统一运动主宰事物运动(即在时间、空间中无处不在以及时刻起作用)称为矛盾的普遍性。同样作为矛盾运动所遵守的矛盾对立统一规律,伴随着矛盾的存在和运动也必具有普遍性。矛盾又具有特殊性,意即在客观世界中有数不清数量的事物在运动着,具体事物的运动对应于不同的矛盾运动,同时多种矛盾还常常交织在一起。在时空域中形成体系性的复杂矛盾运动,这些矛盾运动无论是矛盾组成抑或运动方式都不相同,由此联系到对应的矛盾"统一性"及"对立性",也必具有各自不同的特殊性。将以上内容归纳起来就形成了矛盾对立统一,同时具有普遍性及特殊性的概念。

以上所论述矛盾对立统一律所蕴涵的内容,已充分展示了矛盾对立统一律在唯物辩证哲学中的核心及基础地位,以下将讨论与量变质变律之间的关系。由运动变化性质和变化形式而言,可概括浓缩为"量变"和"质变"两种,量变质变律明确了这种划分,并指明在量变阶段中主要矛盾的主次要矛盾方面并不发生变化而只有矛盾发展程度的变化,因此矛盾性质没有变化,事物性质也不发生根本变化。在质变阶段情况则完全不同,主要矛盾的主次要矛盾方面发生交叉换位,矛盾性质和事物性质也都要发生变化而产生不同性质的"新"事物。量变质变律还指出,"量变"、"质变"互相依存,相互向对方转变。从而形成显变到质变,再到量变,并以此往复循环。同时,在变化过程中所交融(量变过程内包含了一些质变,质变过程中包含了量变以完成质变等内容),量变质变律描述事物运动性质和方式的重要科学规律。换个角度观察,如对矛盾运动性质和方式作为一个事物,则此事物的运动必遵从矛盾对立统一律,进而由对立统一律的内涵对量变质变间关系进行演绎,不难看出量变质变律所述内容可以由矛盾对立统一律的较深层向对立面转换演绎中得出。

现在讨论否定之否定律与矛盾对立统一律之间的关系。否定之否定律是阐述否定行为影响运动的科学规律,富有重要辩证意义——"否定"行为对事物矛盾运动起重要促进作用,讨论否定之否定律与对立统一律之间关系,先由矛盾运动基本概念开始。事物的运动由其内部矛盾所引起并推动,因此事物的运动可由其矛盾运动表征。"否定"是对某种矛盾状态进行反对、排斥、削弱甚至消亡的行动、行为,也可以表示"否定"行为的行动过程。如将对矛盾采用行动

(概括分类的行动)及考虑行动对运动效果的影响,作为一个"事物",运动主要由"否定"和"肯定"两对立面所组成的矛盾运动所决定的,"否定"与"肯定"间蕴涵有多重对立统一的性质,并遵从矛盾对立统一律。进一步讲"否定"一定是否定一些具体的"什么",那么也就是肯定不是哪种具体的"什么",这是特殊的"你中有我"、互相依赖的表现。"否定"是一种"取消"的消极行为,但又是一种重要的"肯定"行为,因为不否定"什么",那"你"永远是"你",不发生变化也永无发展,这是一种"特殊"又具体的转化,实际是"否定"(这种直接的"对立"是发展的根源)与"肯定"对立统一,形成否定—肯定—否定无尽头的循环,推动事物的发展。如果进一步研究对立统一的过程,则会发现"否定之否定"的重要性:其中第一个"否定"如当做开始否定行为,它不能达到完成"否定过程"的肯定,即否定完成"过程"还应继续否定,这是第一个否定的含义。如果将第一个"否定"认做否定过程(质变过程),则完成了质变过程应该转入量变过程(是对质变过程的否定)。所以第二个"否定"是否定质变进入量变之义,但应注意的是此时恢复到"量变"似若回到"原始",实际上是新过程的"起点",并非原来的起点。例如,20 世纪初叶商船或军舰所用的通信与 20 世纪 90 年代 GSM 移动通信系统都是移动通信,但后者绝不同于前者,而是大有发展的移动通信。这就是辩证哲学上所说的"螺旋式上升"。以上论证所得到的结论完全是由矛盾对立统一律蕴涵的内容如对立面的互相贯通、互相转换又互相对立斗争,对立斗争是事物发展的动力和根源,以及"对立统一"具有最大普遍性又处处体现"特殊性"等演绎而得出,这些结论又正是"否定之否定"律的重要内容。按照"公理"和"定理"的概念,可将矛盾对立统一作为公理,"量变质变律"及"否定之否定律"作为由公理推理而得出的定理,是完全合理的。

系统理论主要研究"系统"诞生、生长、发展以及消亡等科学问题。在一般情况下,上述问题都具有非常的复杂性。如果"系统"涉及有人介入,则被称做开放的复杂巨系统。除了复杂性以外,系统理论所涉及的具体系统门类非常广泛,在研究问题时,系统理论必须结合众多学科的内容协同工作,在整合不同特点的内容时非常需要一种普适性很强的基础学科的支持哲学,尤其是唯物辩证哲学,很自然地被认为是系统理论的基础。而矛盾对立统一律作为第一公理是恰当的。

1.5.2 系统理论暂立的二层次公理体系

一、暂立的公理体系

· 任何系统必蕴涵于更大的系统中,为其子系统。而系统本身又包含若干子系统(其间可相互交织),因而系统的组成为多层次交织的结构体系(此处更大系统并不限于几何空间的大,而是广义的,功能结构更复杂、影响关系更普遍等运动、发展进化意义上的更大)。

· 生存着的系统都为非保守的耗散自组织系统(具有时间对称破缺特性),系统与外界环境有物质、能量及信息的交换。

· 系统生存的根本原因是系统的“功能”、“结构”、“环境”及其他系统间众多相互关系的对立统一。

· 生存着的系统(即系统层次)必动态宏观有序,并主要由系统层的序参数(组)所决定,是“功能”与“结构”中“关系”相互作用,也是动态自组织的结果,且在运动过程中不断量变、质变,并通过涨落达到新的有序。

· 系统与环境共同进化,而且进化过程也不断进化,由低级、较简单,往高级、复杂进化,是时间、空间非均匀非线性复杂运动过程,遵守适者生存规律。

· 系统的运动(主要体现在功能和结构)是种物质运动,是有条件的、受约束的,物理、事理、人理及生理为产生“约束”的规律领域,有“得(获得)”必有“付出(代价)”。

二、公理体系的几点简要说明

关于公理 1,涉及系统是否无限可分问题。这是一个物理问题,也是一个哲学问题,现在仍有争论。有的物理学家认为无限可分,有的学者认为(如夸克)封闭划分有极限。在此只认为系统在功能结构组成方面是由多个子系统及其元素交织有机整合而成,而不是物理学上物质分子、原子、原子核那样细分。

系统作为一个事物,其存在发展的“内因”如何具体化的理解,哲学中很少详细分析说明,在系统理论的公理体系中指出,是内部结构和内部与外部的关系体系中的有关重要部分所组成。

公理体系强调指出,“系统”是运动着的事物,是动态变化的事物,而且具有动态的运动规律(序)。它是由有关的“关系”相互作用而产生,相互作用着的“关系”不断运动变化。“变化”在一定条件下会引起系统的序变化,这就是质变,质变的产生是当“条件”具备时,由随机扰动引起的。

过去认为事物的进化符合适者生存的“选择进化论”,事物被动地被环境选择,抑或淘汰,抑或生存进化。现在认为系统与环境互相作用中共同进化,进化的模式和过程也是发展进化的,称为进化过程的进化。

“系统”的生存演变是一种复杂物质运动,需要开放环境支持,人类可按照自己的目的,依靠规律来影响系统的运动(如改变运动状态,额外地保持运动状态等)以获得相关“内容”来达到既定目的,统称为有所“获得”。需要进一步理解得到“获得”是有条件的和需付出代价的(简称“付出”)。代价有各种形式,例如一种“获得”内容包含了两种对立统一“特征”(或效果),得到所需“特征”,必同时承受另一对立“特征”的影响;又如为了获得某“内容”必定要创造获得条件,而这些条件的产生可概括归纳为行动者在时空中生存活动和拥有范围的变化作为代价。如以“自由”作为代价,付出就是以生存和活动范围限制来表征,“获得”和“付出”是一对立统一的范畴,在实际场合,尤其是在复杂运动情况下,“收获”与“付出”往往具有复杂的对立统一辩证关系。如某个事物其某个剖面是以“获得”特征满足目的,但其另外一个剖面会呈现“付出”

代价特征，这种现象即“获得”、“付出”的相对性。又如在某时刻某事物呈现“获得”特征，过一段时间后同样事物变为“付出”特征了，这是一种动态相对性。有的事物在某层次上是以“付出”特征出现的，但这个“付出”是为了高层次“收获”创造条件，也就是以较小“付出”换得较大“收获”的一种变换。以上所述“获得”与“付出”的相对性关系，有别于为了“获得”创造一定条件保证实现“获得”的直接形式的“获得”与“付出”间关系，而是较复杂的辩证“获得”与“付出”的关系。

在实际应用中，系统“获得”与“付出”公理具有非常重要的现实意义。这是因为人们做一些重要事（包括设计实现某新系统）时，总体上总是要权衡达到“目的”的“获得”与为此“付出”代价之间的得失关系。权衡有多种方式，有直接层次的权衡，这是每个人实现“目的”过程中都会做的。重要的是在时间空间中作深层次得失权衡，对未来和隐藏深入的重大得失问题进行权衡，这也是系统理论在应用中所起的一种重要作用。应该着重指出，上述深层次“获得”与“付出”间权衡问题绝不是系统理论单独就能完成的，而是根据被权衡问题所属领域利用系统理论结合该领域专门原理（“理”体系内有关专门规律）来进行的。总结而言，在物理、事物、人理、生理的“四理”约束下系统有获得有付出公理在应用中不能代替各种具体之“理”，它是一条总体性方法，是一种重要的思维方式。

1.6 综合举例——GSM 第二代移动通信系统

在本节中以 GSM 数字移动通信系统为例说明系统理论与实践的结合要点。主要说明：

- “系统”本身的诞生、成长、发展及与环境共同进化。
- “系统”多层次交织的开放动态结构组成。
- “系统”功能及“序”的多层次组成。

1.6.1 GSM 系统的发展与下代移动通信系统

GSM 是继第一代模拟移动通信系统后的第二代数字式移动通信系统，GSM 系统是一个成功的系统，它将移动通信业务大大地推进发展，从而使整个通信业务得以明显发展。由系统理论角度观察，其生存发展的成功是有科学性的，如功能定位准确，系统生存之“序”科学合理等。因此，GSM 系统虽然复杂，但在不长的数年间完全取代了第一代模拟式移动通信系统，使用范围覆盖欧亚两大洲广大地域，GSM 系统虽然发展得很成功，但由其生存周期分析已处在壮年期往老年期转化阶段，新一代移动通信系统正在迅速成长，它逐步代替 GSM 系统的总趋势不可避免。虽然 GSM 系统并不会马上退出社会，就营运而言还会存在相当长时间，并将与新一代系统交融工作，局部还会有所发展（如所用手机不断改型，业务类型增加，基地站系统、管理软件改进等），但新一代移动通信系统诞生和发展的历史趋势不会改变，GSM 作为一个系

统的生长演化过程提供了验证系统理论的一个很好范例，值得分析研究。

1.6.2　GSM 系统组成

如图 1.2 所示为 GSM 系统组成示意图，其众多的分系统、子系统分层次交织组成系统。

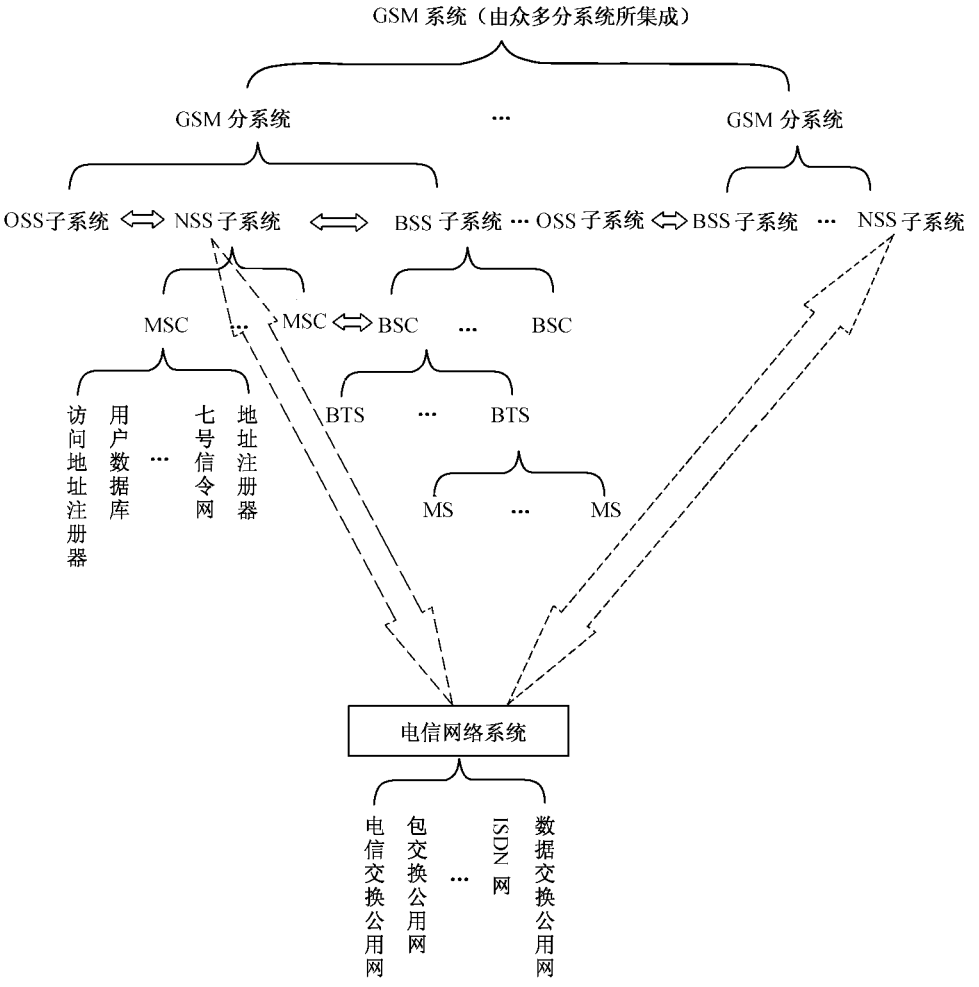


图 1.2　GSM 结构体系及与其他信息网络的连接展开图

其中，双线连接为工作连接示意（非常具体层次的工作连接未在此表示）；单线连接为结构体系组成示意。OSS 为操控子系统；NSS 为网络交换子系统；BSS 为基地子系统；其中 BTS

为基地收发站(子子系统);BSC 为基地收发控制站(子子系统);MS 为手机(它也是一个子子系统,实际上可按工作控制隶属关系将子子系统再细分层次)。图 1.3 是 GSM 分系统结构概略图。

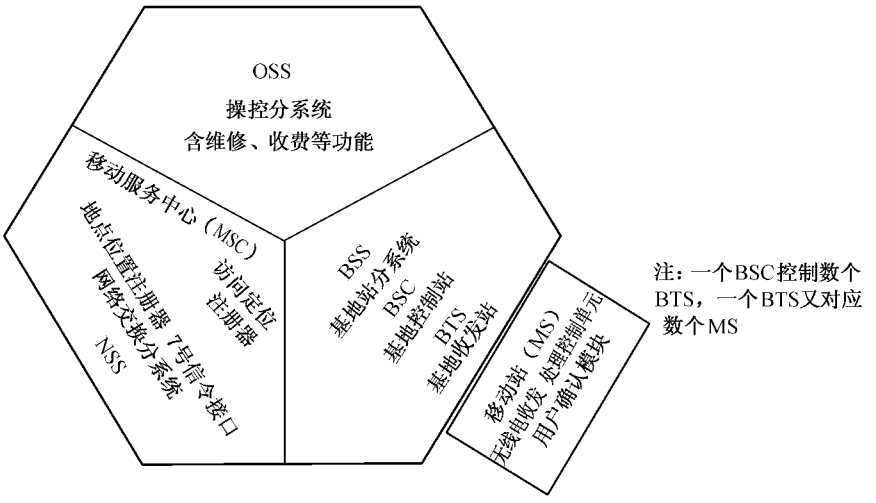


图 1.3 GSM 多层次结构概略图

1.6.3 GSM 系统主要功能

全球移动通信系统(GSM)主要功能(序组成)由以下三个层次组成:

· 第一层:面对用户的通信功能(移动状态)。语音通信服务:GSM 用户间(含漫游状态),GSM 与固定用户(含长途通信);数据服务:与 ISDN 用户连接、与 GSM 用户连接、与分组交换用户连接……;短信息服务:点对点短信息服务、信息广播服务。

· 第二层:保障通信服务的内部系统功能。临时无线电信道的建立和拆除(含利用光纤电信网络要求等待时间短、可靠接入);用户定位管理(含用户确认);用户交接;通信安全性保障;收费管理(用户也需优良合理的收费管理)……

· 第三层:保障上两层功能的系统运行、故障检测功能。GSM 序体系:由系统分系统、子系统、子系统各自在多层次动态组成,在此只介绍总体层次的序。在总体层次序为:时分多址为主,辅以频分支持。蜂窝结构小区,小区交换链接构成移动状态通信;长距通信(尤其是长途漫游)利用电信网以节省资源;开放式体系组成以标准和协议作为开放式体系的组成框架。

1.7　本章小结

本章主要论述了现代系统理论的基本内容，包括："运动"的概念；系统的定义及解释；系统理论体系；系统理论常涉及的对立统一范畴；以及系统暂立的公理体系等；最后以 GSM 第二代移动通信系统为例说明系统理论与实践的结合要点。

习　　题

1. 运动的基本概念是什么？
2. 系统如何定义，其内涵是什么？
3. 现代系统理论的体系如何？
4. 什么是自组耗散结构？突变论的基本概念？
5. 现代系统理论体系常涉及的对立统一范畴主要有哪些？其内涵如何？
6. 现代系统理论体系的顶层公理是什么？有哪些暂立的公理体系？
7. 试针对一实例应用现代系统理论体系的对立统一范畴内容进行分析、讨论。
8. 试用现代系统理论体系暂立的公理体系分析某一信息科技的发展情况。

第 2 章　信息及信息系统

2.1　引　　言

本章主要论述信息、信息系统及信息科技相关理论与技术上的问题。

2.2　信　　息

“信息”一词在社会上广为流传，尤其是 20 世纪 80 年代以来，人们讨论的话题，大都离不开信息。但“信息”究竟是什么？却有可“意会”不可“言传”的特点。早在唐朝，有一位名叫李中的诗人写了一首七言绝句诗，诗云“梦断美人沉信息，目穿长路倚楼台”，经考证这是世界上第一例涉及“信息”、出现“信息”一词的历史记载。诗是高度“意境”和多层次想象的“浓缩”，重在“领会”不重“言传”，故诗中对“信息”没有解释说明。遗憾的是，世界上历史和文献也没查见有关“信息”定义解释的详细记载，直到 1948 年美国 Shannon（仙农）教授参考了热力学熵的含义才给出了“信息”的定义和定量描述。

2.2.1　信息的内涵与定义

仙农教授针对通信领域，通过信号传输进而获得信息的过程，提出“信息”是不确定性的消除，借助于物理学“熵”概念定量地表示信息量 $I=-\sum_{i=1}^{n} p_i \lg p_i$，$\sum_{i=1}^{n} p_i = 1$。这是信息科技领域发展的一个里程碑。随着社会的进步，人类与信息领域的关联日益密切，范围不断扩大，已不限于通信领域。“信息”是人类最常用词之一，但对它的定义却极不统一，有多种说法。定量、广义、全面地描述“信息”是不太可能的，是非常难的，对“信息”本质的深入理解和科学定量描述有待长期研究，在此暂时给出一个定性的概括性定义：

“信息是客观事物运动状态的表征和描述”，其中“表征”是客观存在的表征，而“描述”是人为的。

“信息”的重要意义在于它可表征一种“客观存在”，与人的认识实践结合，进而与人类生存发展相结合，信息领域科技的发展体现了客观与人类主观相结合的一个重要方面。

对人而言，“获得信息”最基本的机理是映射（借助数学语言），即由客观存在的事物运动状态，经身体的感知功能及人脑的认识功能进行概括抽象形成“认识”，这就是“获得信息”、加工

“信息”的过程，是一个由“客观存在”到人类主观认识的“映射”。

由于客观事物运动是非常复杂的广义空间（不限于三维）和时间维的动态展开，因此它的“表征”也必定是非常复杂的，体现存在于广义空间维的复杂的多层次、多剖面相互“关系”，及在多阶段、多时段的时间维的交织动态展开，进而指出“信息”，它必定是由反映各层次、各剖面不同时段动态特征的信息片段组成，这是“信息”内部结构最基本的内涵。

2.2.2　信息的表征及其特征

一、信息的表征

“信息”的客观表征非常广泛，源于各种各样运动状态的特征，信息的表征就是各种各样的“特殊性的表现”，也可认为“特征的表现”。

对人而言，可以利用感觉器官和脑功能感知有关自然界的各种信息（通过多种信息荷载的媒体）。此外，人还创造了“符号”来描述、记录、传递、交流、研究和利用“信息”。以上所述概括为人脑主宰的二重“映射”过程，即感知认识信息形成概念和思维，然后再将它们映射为符号（原理上可这样分步骤理解，实际上人脑思维过程中已融入了“符号”，具体细节就是脑的思维过程，现在尚不清楚），很多情况下人又是通过符号认识信息的。

“符号”是内涵非常广泛的一个概念，研究“符号”及其应用已形成专门的“符号学”这门学科，在此简单举例说明：语言、文字、图形、图像，还有音乐、物理、化学、数学等各门学科，除语言文字外还有专门符号，如微分、积分符号发展为算子符号、极限、范数、内积符号等等，物理中量子物理就有独特符号如波矢（态矢）态函数等。推而广之，各种定理可以被认为是有序的符号构成的符号集合，是广义的符号，也是客观规律的“符号”。此外，通常人类的表情、动作（如摇头、摆手、皱眉等）也可认为是一种符号。

二、“信息”的特征和被关注的特征概述

1. “信息”的存在形式特征（直接层次）

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，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，在环境中可区分条件下具有多次复用性。

④ 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，如说话声几个人可同时听到，卫星转播多接收站可以同时接收信号获得信息等等。

⑤ 时间维有限尺度特征：具体事物运动总是在时间、空间维有限度尺度内进行的，因而“信息”必定具有时间维的特征：如发生在何时、持续多长、间隔时间多长、对时间变化率值的大小、相互时序关系等等，这些都是“信息存在形式”内时间维的重要特征，对信息的利用有重要意义。

需着重说明的是，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。事物运行在量子状态的运行能量水平非常微弱，数量级约是 $\varepsilon=h\nu$（ε 为能量，h 为普朗克常数$=6.626\times10^{-34}\text{J}\cdot\text{s}$，$\nu$ 为频率），可以这样理解：即事物的量子化能量值如果低于此值，事物运动状态就无法保持（也可认为是一个低限阈值）。信息系统运行中的能量水平都远远高于此值，例如在微波波段 $\nu=10^{10}/\text{s}$，阈值 $\varepsilon=6.626\times10^{-24}\text{J}$；光波波段 $\nu=10^{14}\sim10^{15}/\text{s}$，阈值 $\varepsilon=6.626\times10^{-19}\text{J}$。现在这两波段信息系统工作最低功率能量约在 $10^{-13}\sim10^{-14}\text{W}$ 及 100 个光子能量水平（信号检测能量阈值），比 ε 值高得多，而信息系统正常工作状态的能量或功率水平更要高得多（如高灵敏信号接收检测设备的正常运行能量水平）。还有些“信息”运行形式是靠外界能量照射形成反射，由反射情况来表示“信息”，这些表征信息的反射能量也远大于 ε 值（如反射光）。这意味着现在这些系统都处在远离量子态的“宏观态”中，才具备上述“信息”特征，如利用量子态荷载“信息”，即信息系统运行在量子态，则它的状态就会“弱不禁风”，碰一下就变。“信息”的上述特征就不再存在，这对“信息安全”领域的信息保密有利，但系统实际运行的同时也有巨大困难。

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“信息”的失真，而“有意”则为人有目的制造失实信息或更改信息内容以达到某种目的。

② 多层次、多剖面区分特性。“信息”属于哪个层次和剖面的，这也是其重要属性。对于复杂运动的多种信息，知其层次和剖面属性对综合、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在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”可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想到企业将推出的新商品，是根据企业所研究课题蕴涵指称对象的多种信息，利用逻辑推理和相关科学技术确定指称对象将投入市场具有强竞争力的新产品，是逻辑推理获得信息附加义的例子。

3. 由获得的一些（剖面）信息进而认识事物的运动过程

事物的运动是“客观存在”并具有数不尽的复杂多样性。“信息”的深层次重要性在于通过“信息”所表征的状态去认识事物运动过程，人们对“信息”关联“过程”的特性主要有两方面，即：

“信息”不遗漏表征运动过程的核心状态，以及“信息”中能蕴涵由“状态”到运动“过程”的要素，由个别状态（信息）认识运动“过程”是由局部推测全局的过程（由未知至有所“知”的过程），但无法要求在“未知”中又事前“确知”（明显的悖理），因此我们关注的是由每条“信息”中所蕴涵了表征运动全局的因素进行“挖掘”以认识全运动过程，由此提出挖掘“信息”内涵的原理框架为四元关系组，即

信息⇒[信息直接关联特征域关系，信息存在广义空间域关系，信息存在时间域关系，信息变化率域关系]⇒一定条件下指称对象的运动过程（片段）

由于运动的复杂多样性，因此上述各域还需要再划分成子域进行研究。

信息的直接关联特征域关系，涉及下列子域：关联对象子域，如事、物、人及联合子域，如人与事、事与物、人与物等；关联行为子域，如动作、意愿、评价、评判等；动状态性质子域，确定性、非确定性（概率性与非概率性不确定性）、确定性与非确定结合性等。

信息存在广义空间域关系，包括三维距离空间子域、“物理”空间子域、“事理”空间子域、“人理”空间子域、“生理”空间子域。各子域仍可再进行多层次子域划分及特征分析，如“物理”（广义的事物存在的理）空间子域中包括数学空间、物理空间、化学空间等各子子域等。

信息存在时间域关系常需分成多种尺度的时间子域：

信息变化率域关系，可进一步划分为以下几个子域，即广义空间多层变化率子域：$\frac{\partial}{\partial x}$，$\frac{\partial}{\partial y},\cdots,\frac{\partial}{\partial\theta},\frac{\partial}{\partial r},\cdots,\frac{\partial^2}{\partial x^2},\frac{\partial^2}{\partial y^2},\cdots,\frac{\partial^3}{\partial x^3},\cdots$；时间域多层变化率子域：$\frac{\partial}{\partial t},\frac{\partial^2}{\partial t^2},\frac{\partial^3}{\partial t^3},\cdots$；时空多层变化子域：$\frac{\partial^2}{\partial x\partial t},\frac{\partial^2}{\partial t\partial x},\cdots$

利用以上所介绍的四元组关系框架对“信息”（含对信息组合）进行分析，并通过类比和联想可以得到“信息”所代表运动过程的一些“预测”。例如，运动过程是否在质变阶段抑或量变过程，是否会有重大新生事物产生，运动过程是否复杂等。

4. “信息”组成的信息集群（信息作品）

一种状态的表征往往需要用多条“信息”来表示，其包括信息量（未考虑其真伪性、重要性、时间特性等等），可用仙农（shannon）教授定义的波特、比特等表示，但这些还只是表征相对简单状态的信息片段，可称为“信息单元”。客观世界中还存在着由信息单元有机组成的信息集

群，它表征更复杂的运动状态和过程，是“信息单元”的自然延伸，但它们还没有专门名称，在此暂用相似于汉语语义学中“言语作品”的“信息作品”来表示，它还能结合逻辑推理判断等，对更复杂的运动进行描述和表征，这对人类社会发展是有意义的。信息作品的表现形式有多种，有文字、图像、多媒体音像等。但信息作品表征较长的过程，信息作品内含的信息单元数量会非常巨大。

2.2.3 人类所感知信息及其媒体

人是通过感知器官，如眼、耳、鼻、舌、手指等感知信息后，传入人脑及中枢神经进行认知的。人总共感知七类信息，传递这七类信息的中介体，称媒体（是一类并不是一种），因其有多种故简称“多媒体”。表 2.1 扼要叙述人感知信息的种类及媒体，以上是对人而言的。在客观世界中传递信息的媒体还有多种，有的超出人的感知范围，要经过“变换”，人才能感知，如电磁波（除可见光段）、超声波等。

表 2.1 人感知信息的种类及媒体

视觉信息	约占全部信息的 70%～75%	主要媒体为文字、图形、图像（可见光反射）
听觉信息	约占全部信息的 10%～15%	主要媒体为 20 Hz～15 kHz 的声波 （视觉、听觉信息占人感知信息的大部分至绝大部分）
触觉信息 味觉信息 嗅觉信息	约占全部信息的 10%～20%	主要依靠手及皮肤感知物理状态所代表的信息，如软硬、冷热、温度等 主要依靠舌及味觉神经系统 主要依靠鼻及嗅觉神经
综合动态信息	尚无详细统计结果，应认识到其重要性	是以上各类信息的有机动态组合，人对分类信息动态感知后，经人脑有机综合形成各分项的所不具有的附加含义，着重于整合性深层次信息
交互式综合信息	尚无详细统计结果，应认识到其重要性	在人们交互活动中，在综合动态信息基础上所获得的更深层次信息。例如在学术会议上的讨论中萌发很多新感知，在研究性讲课中师生都会获得这种信息

人在获得信息后经组织可再转发传递信息（绝大部分亦为视觉、听觉信息，也有综合动态信息及其他种信息），在这过程中往往增加了人的主观“描述”，描述者应力争如实客观进行描

述，接受者应分析后提炼真实有用信息，尽力消除附加不真实部分的影响。

2.2.4　人类传递、利用信息的历程

人类自进化成原始人类时，即具有原始的社会性，表现在组成原始人类社会，最初为集体狩猎而生存。形成社会的基础因素的一是人类互相传递“信息”，协同动作，交流“认识”和“思想”。由动作、表情，结合表达意识意图的声音开始，经过许多万年的人类进化发展，才发展到了语言（有规律固定化的语音序列，然后又经漫长过程形成文字（由结绳记事、画图记事开始），传递交流范围也由近至远，由小到大，可由图 2.1 表示。

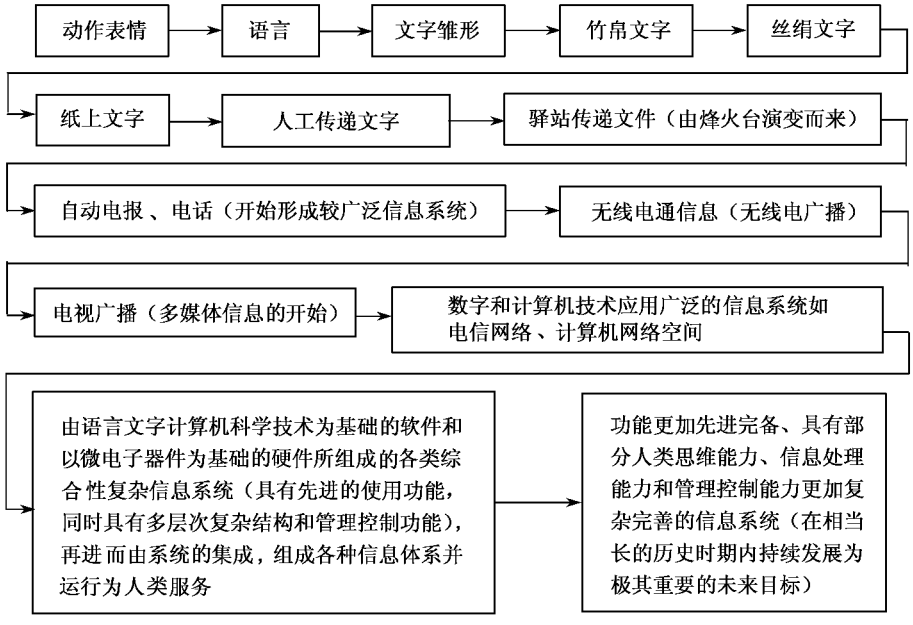


图 2.1　人类不断完善和利用信息的发展过程

对图 2.1 应着重说明三点。第一点，人类进化过程中，直至“现阶段”利用信息的变化过程是先慢后快，而且越来越加速。人类由原始状态到形成语言文字，是以万年计的时段；由文字到电报（19 世纪）是四千至五千年时段，即缩短到“千年”量级；由电报开始到形成使用计算机嵌入的大型信息系统，全过程不过二百年左右，而最近四十年左右发展特别快，现仍在快速发展中。第二点，传递利用信息，由利用简单媒体工具，到利用现代化科学技术进行“信息”变换后再进行管理应用，逐步形成了供人利用的“信息系统”。它是一种高级人工工具，而不是简单工具，这是人类进化的一个重要标志。结合各种系统性复杂工具的发明和利用也只是近百年

才比较明显，尤其是最近的四五十年。第三点，新世纪、新千年信息科技和信息系统的发展特征是信息系统的发展将结合人类正面临的几个根本性问题的较彻底理解和破谜，它们是复杂非线性问题的理解和求解、“生命发生的本质”（由非生命至生命的质变）及生命延续进化的关键细节、人脑认知科学等极具挑战性问题，以上这些问题的“突破”需要一个时期，至少不是二十年至三十年的事。人类在信息科技领域的发展进入了一个新历史时期的前期（至少不能认为是中后期）。叙述至此，我们已经讨论了“信息系统”发展的命题，下面就信息系统作扼要讨论。

2.3 信息系统

2.3.1 信息系统的定义

帮助人们获得信息、存储信息、传输信息、交换信息、处理信息、利用信息和管理信息的系统称为信息系统，是以“信息”为基础服务于人的一种工具。“服务”一词有着越来越广泛和不断扩大的含义，信息系统是有着各种以“信息”为媒介、不同功能和特征，服务于人类的系统的总称。

2.3.2 “信息系统”理论特征

· 现代信息系统内往往叠套多个交织作用的子系统，是系统理论所描述的典型系统。如现代通信系统包括卫星通信系统、公共骨干通信网、移动通信网等组成，卫星通信系统又包括卫星（包括转发器、卫星姿态控制、太阳能电池系统等）、地面中心站系统（包括地面控制分系统、上行信道收发系统等）、小型用户地面站（再分子系统等）。移动通信网系统、公共骨干通信网系统都是由多层子系统组成。

· 每一种信息系统，当其研发完成后仍会不断进行局部改进（量变阶段），当改进已不能适应的情况下，则要发展一种新类型（一种质变）。如此循环一定程度后，会发生更大结构性质变（系统体制变化），如通信系统中交换机变为程控式为体制变化。现在又往“路由式”变化，也是体制变化。这种变化发展“永不停止”，符合系统理论中通过涨落达到新的有序原理。

· 信息系统作为人类社会及为人服务的系统，伴随社会进化而发展，并有明显共同进化作用，且越发展越复杂、高级。

· 每一种信息系统的存在发展都有一定的约束，新发展又会产生新约束，也会产生新矛盾，如性能提高是一种“获得”，得到它必然付出一定的“代价”。

2.3.3　信息系统的功能组成

任何信息系统都是由下列部分交织或有选择交织而组成的。

信息的获取部分(各种传感器等)。任何一种信息系统,其内部都要利用一种或多种媒体荷载信息进行运行,以达到发挥系统作为工具的功能。首先应通过某种媒体,它能敏感获取"信息"并根据需要将其记录下来,这是信息系统重要基本功能部分。应该注意到的是:人类不断地依靠科学和技术改进信息获取部分的性能和创造新类型的信息获取器件,同时信息获取部分科学技术的重要突破会对人类社会的发展带来重大影响。

信息的存储部分(如现用的半导体存储器、光盘等)。"信息"往往存在于有限时间间隔内,为了事后多次利用"信息"需要以多种形式存储"信息",同时要求快速、方便、无失真、大容量、多次复用性为主要性能指标。

信息的传输部分(无线信道、声信道、光缆信道及其变换器,如天线、接发设备等)。这部分以大容量、少损耗、少干扰、稳定性、低价格等为科学研究技术进步的持续目标。

信息的交换部分(如各种交换机、路由器、服务器)。这部分以时延小、易控制、安全性好、大容量、多种信号形式和多种服务模式相兼容为目标。

与信息获取部分一样,这几个部分现在也在不断发展,其中重大的发展对人类的进步影响明显。

信息的变换处理部分(如各种"复接"、信号编解码、调制解调、信号压缩解压、信息检测等,统称信号处理领域)。这部分可被认为是信息科技发展的瓶颈,近年来虽有很大进步,但尚不具备发展所需要的类似人的信息处理能力,实行人与机器的更紧密结合。实现这种结合的科学技术有漫长艰难的发展征程,它是人类努力追求的目标之一。

信息的管理控制部分(如监控、计价、故障检测、故障情况下应急措施、多种信息业务管理等)。这部分功能的完成,除了随信息系统的复杂化而急剧增加变为更加复杂和困难外(如信息系统复杂的拓扑结构是管理监控领域的数学难题),随着信息系统进一步融入社会,其管理控制的学科基础也由于社会科学的进入交融而综合化。其管理控制功能还涉及社科、人文等方面的复杂内容,造成"需要"与"实际水平"之间的差距,矛盾更加明显。例如电子商务系统的管理控制涉及法律,多媒体文艺系统管理涉及伦理道德、法律等领域,总之信息的管理控制部分的发展涉及众多学科,具有重要性、挑战性及紧迫性。

信息应用领域日益广泛,要求服务功能越来越高级、复杂。在很多场合下,由信息系统控制管理部分兼含与应用服务关联功能的工作模式已不能满足应用需要,因此应运产生了专门对应用进行支持功能的专门部分,称为应用支持部分(它与管理控制部分有密切联系)。

各部分都有以下特征:软硬件相结合、离散数字型与连续模拟型相结合、各种功能部分交织、融合、支持,形成主功能部分,如存储部分内含处理部分,管理控制部分内含存储、处理部分

等。以上各部分发展都密切关联科学领域的新发现、技术领域的创新，形成了信息科技与信息系统及社会互相促进发展，“发展”中充满了挑战和机遇。

以下将扼要介绍各部分功能内涵、发展近况及核心内容，同时也提供相关功能为主的信息系统的现有例子。

一、信息获取部分

信息获取部分从功能角度而言是信息系统的基础，如果信息系统缺少了“信息”的获取，就不是一个完备的系统。信息系统主要功能就是利用“信息”，如果系统无“信息”进入，就很难运行。同样对那些主要功能是传输信息的信息系统，如通信系统也少不了“信息”的输入部分，它可以认为是通信系统的信息获取部分。总之，信息获取部分之所以重要，是因为所有信息系统都是以“信息”为人类服务的，获得“信息”是基本条件。人本身就有很好的信息获取能力，但仍嫌不够，故千方百计利用信息系统扩大获得信息的范围，从而产生对信息系统获取和利用信息能力不断发展的需求。

1. “信息获取”基本概念

“信息获取”发展的核心是不断延伸获取信息的时空范围（广义空间），从而扩大信息系统功能或形成新功能，现时人类所能获得的信息仅是物体运动中很少部分的表征，因此发展任务繁重且艰巨。

在信息获取方法的发展进程中，竭力减轻“信息获取”的约束力度是重要研究课题之一。即争取由多种“约束”并存、苛刻的条件要求等，往少数“约束”项目、减轻条件苛刻程度等方向转化。发现一些新的信息获取方法固然重要，但一种新的信息获取方法得以实用，最终取决于在复杂环境下，这种新方法被采用后获得“收益”与付出“代价”间的综合运筹，苛刻的约束条件会使广泛的应用受到很多限制。

“信息获取”最基本原理是“映射”，即借助物质间相互作用关系，将欲知晓的运动状态（信息）映射到另一种人类可认识的物质状态上（包括经过多次转换的间接含义），对应信息领域语言即是通过对荷载“信息”媒体的分析认识，以获得“信息”。形成一种新的信息获取方法，即是寻找一种新的物质间作用关系和可以被人认识的映射关系（并希望它是一一映射以“避免”认识发生错误），其中也包括了寻找新的荷载信息的媒介和通过对媒介的分析认识以获得“信息”。一种新的获取信息方法的出现，其基础在于科学技术的发展。

除了上述基本的信息获取方式以外，还存在一种由所获得“信息”扩充推理而形成附加“信息”的方式（即由对已获得“信息”进行联想、类比以及演绎推理以获得新“信息”）。这种获得信息方式现在主要依靠人根据物理、事理、人理、生理进行思维来完成。人工信息系统这方面的能力还非常弱，无法与人相比。人类不断追求新的信息获取方法来源于社会的进化发展不断需要新的信息系统作为人类的工具。

“信息”获取的简要工作框图如图 2.2 所示。

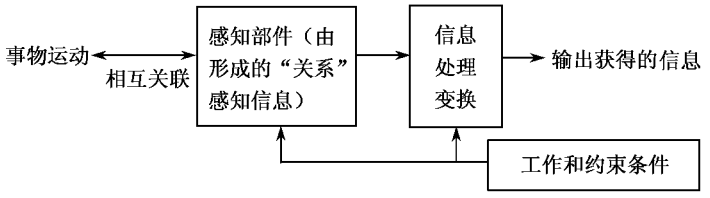


图 2.2　“信息”获取的工作框图

信息处理变换环节包括了广泛内容，如弱信号放大、预处理，也包括其他变换和人的类比联想思维等高级信息处理内容。

“信息获取”概念不仅限于被动式，即对已存在运动状态的感知，还包括依照物理、事理、人理、生理、人工产生各种与欲获得“信息”的荷载体（运动状态）发生关联的“环境”，由环境状态映射获得“信息”。如人工辐射“波”即是人工制造“环境”的一种。

2. “信息获取”基本要求

· “信息获取”的起始阈值尽量低，即敏感信息的起始量值尽量低（灵敏度高）。

· “信息获取”输出输入转换比高（输入输出可能为不同量，恰当选定计量单位，输入输出量间比值尽量高）。

· 输入量敏感分辨能力足够高（包括对输入量敏感及类似输入量的干扰量的高区别能力）。

· 转换比保持线性且误差值小，动态范围足够大或具有对强“输入”自动过载保护，以避免损坏高性能信息获取部件。

· 尽可能地争取工作时只需宽松条件的特性，以避免要求苛刻工作条件限制了重要场合的信息获取工作。宽松工作条件内涵往往还有延伸，即延伸至对抗“工作”及“生存”环境中的干扰。抗损伤能力意指对抗环境中不可避免对信息获取部分的破坏“力”应具有一定程度的耐力。

· “信息获取”部件响应时间足够“短暂”（例如安全保障系统的信息敏感部件响应时间要求可达 μs 甚至 ns 级），另一方面往往要求在长时间工作中误差尽量小，如核潜艇的惯性器件便是突出例子。

· 要求工作可靠，并能够长时间工作以及具有较长的存储寿命。

· 不同“要求”尽量具有性能的独立性，性能指标间往往存在逆向关联性，即调整提高某单项指标要求时，关联到某项指标的负向变动，这样会使应用中选择受多种条件约束的“信息获取”部件变得复杂和困难。

综上所述，明显地得到以下结论：对“信息获取”部分的全面要求，构成了一个事物间相互关联的理想关系框架，其内部充满了对立统一的矛盾，永远不可能完全满足，只有动态发展并

在具体实践中加以辩证选择和动态地“变换”应用各种“信息获取”的方法和方式。

3. 对约束条件的基本认识和对待原则

对上述“信息获取”部分“要求”的限制和极限都可以被认为是“约束”，不断发展就是对“约束”的减弱(形成质变的减弱往往称“突破”)。总体而言，“约束”是永远存在的，任何事物都不可能处在无“约束”的完全自由状态，只不过处在不断地减少某方面“约束”或进行“约束”的“变换”(即转变一种“约束”变为另一种允许条件更为宽松的“约束”)，如耗能条件许可，可利用人工降温或升温以换取工作环境温度的变换以满足实施“信息获取”的工作温度限制。进而应认识到采取各种措施降低约束条件的实施过程也是一种“变换”——施加在“运动”上的一种变换(“运动”只有变换而不可能“产生”和消灭，因运动即是物质)。

4. “信息获取”的重要应用

“信息获取”的应用，经过多年发展历程，已形成嵌入到社会中非常广泛的领域，可以说“无处不在”，凡是有信息系统应用的场合很大部分都会有“信息获取”部分的介入。如科学研究、社会发展、经济发展、国家安全、国际文化交流、国家行政管理等各大领域的信息系统都需要不同形式的“信息获取”部分，现就几个社会普遍关注的前沿领域说明“信息获取”重要应用。

(1) 防灾减灾领域

灾害形成前期“信息获取”，是防止灾害造成巨大损失的关键因素，一些重大灾害的前期“信息获取”存在巨大困难，主要体现在收集不到准确“信息”与不认识灾害形成一一对应信息(不知其映射关系)。例如大地震前有众多“信息”，但不知哪些“信息”是临震信息；又如有些重大传染疾病发生前的“信息”还不掌握，如禽流感、SARS 流行前夕等，要有多个病人传染后才能得知“疾病”可能开始流行；气象灾害如飓风，通过气象卫星观察近年来才有事前预报；一些个人重大疾病前期病因信息也是人类渴望掌握的，如一些癌症病因信息便属于渴望掌握但尚未掌握之列。(当然这些问题发生不单是“信息获取”问题，还涉及总体认识问题。)

(2) 航空航天领域

航行控制方面，航行姿态、加速度、速度传感器(陀螺仪表、光纤陀螺、静电陀螺)、仰角传感器、压力传感器、流速和流量传感器等都是“信息获取”部件或分系统。

飞行员、航天员生命保障系统，如压力传感器、温度传感器、有害射线传感检测器、氧气系统传感器、加速度传感器及反制加速度过大系统等都是以特殊“信息获取”为核心的分系统。

发射返回及起飞降落控制系统是载人飞船中以“信息获取”功能开始结合控制功能所形成的重要分系统。

(3) 医学领域及生物领域(传感器)

相当部分医疗设备是获取人体信息进行诊断的，按其特征有以图像信息方式诊断(如“核磁”、“CT”、“彩超”、“正电子”成像等)。另一类则是获得人体生命表征(物理、化学及生物三个方面参数的信息系统)，如心音、血压等。生命物质从有机体到细胞生命过程中都离不开有关离子，电化学可以测量这些离子状态以表征人体生理状态，从而形成电化学机理的医学信息诊

断设备。利用某些生物活性物具有选择地预测人体内某种生物物质的变化，也是基于生物传感原理而做出的一类信息诊断设备，例如：酶传感器（测量人体血液、尿液某些诊断的成分）。所有医用传感器都面对如下难点，即信杂比值不高；不同个体的数值“离散性”大，即使同一体也会因心理状态而使测得的值离散，而使“判断”困难；还有用于接触人体的测量受保证不伤害健康的强约束。这些医用信息设备的进步发展需要先进信息科技支持。

其他在多个领域，如环境保护，机器人研究设计制造，家用消费，汽车及交通，现代制造业等需要“信息获取”与传感器，畜牧、农业、渔业、园艺、食品等领域也离不开“信息获取”或传感器的应用。社会越发达，利用“信息获取”为人类谋福利的场合就越普遍，需求越旺盛。

5. 现在常用的“信息”特征

① 表征事物存在时间空间域关系的信息。最普通的空间位置关系信息是其中一种，事物特征（广义空间特征）的差别信息也是一种，尤其是微弱差别的信息很重要又很难得到。时间域信息也非常重要，瞬态和微小时间间隔信息在前沿科学技术领域尤其重要。

② 表征事物具体运动状态的信息。常用有运动方向、速度、角速度、（角）加速度、振动（其中含加速度）、流量等。

③ 表征某事物存在状态的信息。如形状（常用圆度、直角度、平滑度），应变状态，颜色及色谱，光谱，温度，硬度……众多信息类别。

④ 通过接收他方信息转为本系统所用（间接获得信息，与信息传输交换有所交融）。

⑤ 按信息获取基础学科领域划分，以物理学原理获取信息，即利用物理原理和方法获得事物运动状态在物理领域的表征，如各种利用波的特征、热力学特征、机械运动、分子运动等方面特征等。物理信息可以是属于宏观层次的，也可以是属于微观层次的信息。

⑥ 由化学原理获取信息。即利用化学原理和方法获得事物运动状态在化学领域的表征，化学学科特征偏重事物分子、原子、离子间相互作用的研究，化学信息多数具有微观性质。

⑦ 生物学原理获取信息，称为生物信息。生物学是个庞大学科领域，其中还再分为众多学科，并发生学科间不断交叉融合，如分子生物、生物化学、生物信息、生理学等。各学科都有一个共同规律，即都需获得研究对象、各种生物运动规律的“信息”进而形成本学科研究发展任务。信息科学技术正和生物学科领域进行交叉融合，形成新的学科内容，这个趋势还将继续下去。现代生物学领域很大部分的提取“信息”是生物化学微观信息，对生物生命活动总体和微观层紧密结合的关键生命信息体系的研究、建立、形成学科尚有待时日。

由基础学科和专门学科交叉融合正在形成一个独立生物信息学科领域。由于该领域研究对象范围十分广泛，内容十分复杂，很多种生物运动规律的认识程度还很初步，使得生物“信息获取”发展的基础性较薄弱，有待于相关生物基础学科交叉融合、互动来形成进一步发展过程。

6. “信息获取”简要小结

人类对争取得到“信息获取”新进展从未停止过，现已在许多领域掌握了多种先进的信息获取手段和方法，但仍嫌不够，在事物按人理、事理、物理、生理支配的广大运动领域内，现在人

类能获得的“信息”只占全部信息的极少部分，尤其是直接依靠人理、事理提取的信息更是稀少，不满足发展需要，还应不断探索和建立新的后继方法和手段。现在一种新的“信息获取”方法和手段的发现和建立，其基础往往需要对一些多学科交融、前沿科学问题的深刻理解和科学、巧妙地运用先进技术。一种新“信息获取”的诞生由共用基础延伸到新获取理论的建立、新技术方法的确定、在实践中验证和改进，是一个艰难的过程，尤其是在一些“极端”条件下的“信息获取”（如非常微弱或非常强的瞬态“信息获取”），其科学技术内涵已绝对不限于传统概念下直接获取的内容，而是包括了信息系统其他功能，如：存储、变换、传输、信息处理等的融入、支持才得以完成。例如医学和生物领域的“信息获取”过程中由于杂波干扰非常严重，必需先进的信号处理措施加以支持。正在不断发展中的“信息获取”科学技术领域带有明显的系统特征，对于获得信息具有重要意义的场合往往以“信息获取”作为主要功能来形成复杂信息系统，如：天文望远镜、声纳、雷达、遥感等大型设备都是依此目的而诞生的。

二、信息存储部分

“信息存储”是信息系统继“信息获取”之后在信息利用过程中不可缺少的重要组成部分，“信息存储”功能相当于人认识过程中的“记忆”功能，人脑如无记忆功能则无法形成“神奇”思维功能，甚至连正常人的最简单功能也不具备。例如不认识自己的亲人，对自己刚说过的话却不知自己说了些什么，与别人交流也是同样情况。总之，在人“思维”的基础上，由“信息存储”逐渐形成人类知识的存储和交流利用，进而形成知识积累和传承。如今信息系统仍处在为人类进步、生活质量不断提高的服务进程中，“信息存储”仍有不可取代的地位。人类不断寻求新的存储方法和方式，同时信息系统与存储部分存在一种日益互动的发展关系。它是一种对立统一的关系（此处所提“信息系统”可以是系统整体，也可以是“系统”的某部分，如新信息获取方式就需要新存储方法和方式）。

1. “信息存储”的基本概念

· “信息存储”的实质内涵是在多维空间与时间中，保存事物运动状态，这种“保存”就是保存荷载、表征运动“信息”的媒体状态，这样就将保存“信息”转变为“媒体”状态与存储物状态的接触、交流、转移与保存。“信息存储”可进一步抽象为首先产生将荷载媒体表征“信息”的物质状态与存储媒体的存储状态发生关系，然后将荷载信息的状态转移映射至对应存储体的某种确定状态（原荷载信息媒体的状态可以“保存”也可不保存）是物质间运动的一种交互关系。从信息存储体角度而言，“存储”过程首先是信息获得，然后是对其保存。

· “存储”的完成既然是一种物质运动状态的转移和保存，那么新的“存储”出现，基础必然在研究物质运动的科学原理和实现该原理的技术方法。因而新存储方式的出现根源在科学发现和技术创新。

· “存储”的基本单元功能是保存信息单元（状态），并不能达到保存“过程”的程度，对信息应用而言仅存储“状态”是远远不够的，更重要的是存储“过程”。“过程”是由数量巨大的“状

态”才能组成的，需要大大地扩充存储容量，这是海量存储出现的原因之一。

· “过程”是快慢参差的连续过程，而“状态”是过程中的“片段”，意即将过程进行“切片”采样得到“状态”。反过来由“片段”组成“过程”，相当于用不连续量形成连续量（过程），就存在“形成”的完备性问题。保证完备性的科学依据是卡捷尼科夫（或奈奎斯特）采样定理，对快速运动过程需要高频率采样，使得需要更多的“状态”表征过程的本质。在计算机中采用二进制数字表征数量，实际上是以更多的“位”数换取可靠、容易地对数量大小的表征，这一切都提高了对存储的要求和难度。

· 事物的运动永无完结，不断地进行量变质变的转化发展，在客观上“信息”也不断产生和变化，伴随人类的发展对“信息”的需求也与时俱进。存储信息是满足人类对“信息”需求的重要内容之一，因而会有不断地要求扩大存储信息类型、提高存储质量、快速方便使用存储信息。在上述要求驱动下“信息存储”的发展会持续不断地进行。

· 随着科技发展、信息系统及社会发展，“信息存储”在学科上已发展成庞大信息学科领域中一个重要分学科领域，它包括了很多交叉分学科，涵盖了广泛的学科范围和众多的学科前沿内容。例如数据库理论与技术、光存储理论与技术、半导体存储理论与技术、材料记忆理论与技术（尤其是功能材料）等。同时多种多样“信息存储”的实现形式，尤其是大型先进的信息存储设施，大多具有完备、复杂的系统特征，它们绝对不是只有单一存储信息功能的简单部件，而是具有多种应用功能存储有大量各种“信息”（包括各种精细信息）、甚至可提供由“信息”组成的运动过程，正在形成以“存储”为核心并系统集成为以“知识”服务人类的信息系统。它需要不断完备系统的自组织机理，软、硬件相结合的构成。系统内部包含有信息处理、交换、传输、管理与控制诸功能，来保证这类系统在以“存储”为核心机理基础上不断完善高级“知识”服务意义上多种功能的实现。例如，公共开放性大型数据库便是不断发展中的知识服务信息系统，它的结构和服务管理都具有复杂的系统特性。

· 除了上述以“存储”为核心机理所形成的信息系统外，“信息存储”作为信息系统的基本功能也大量且不可或缺地嵌入各种类型的信息系统中，以支持它们完成高水平功能。

2. 存储部分主要要求

· 就存储信息本质特征而言，是保证所存储信息的真实性。

· 由于“信息存储”进行过程中对信息存储体而言，“信息”的转移和接收等价于“信息获取”，根据实际情况都有可能需要对“信息获取”的要求，在此不重复列出，可参考前面所列。

· 作为以“信息存储”为核心机理所形成的开放式信息服务系统，系统服务方面有着很多、很高的要求，例如，提供信息的真实性、数据的可靠性、服务使用的方便性和及时性等方面已发展形成了一个随着服务功能的增加而不断增加服务要求的高性能动态指标体系，指标体系内各项要求之间也存有复杂的对立统一矛盾关系，这些进一步形成了“发展”和“需要”间对立统一的矛盾从而促使体系不断发展。

· 系统服务功能不断发展的要求也转化到存储信息系统管理控制功能的不断提高（包括

系统的安全使用性能),再进一步落实到系统的体系结构组成上,由此更进一步扩散到相关科学技术的发展进行支持的基础层次上。

3. "信息存储"分类举例

"信息存储"的方法和方式有着数不清的种类,它是一种物质运动相互作用产生的结果,例如:河流是水流长时间流动的表征,也是"水流"信息的记忆。下面就主要与信息系统有关的人工制造的几种信息存储类型加以讨论介绍。

· 文字是记载人类活动的主要方式之一,它的产生目的就是为了"存储"和传播与"继承"信息和知识。以前荷载文字信息的媒体是皮、丝帛、纸等,现在是磁、电、光效应与文字的结合,将文学所荷载的信息转移到对磁、电、光效应有所响应的媒体中加以存储,而用纸存储文字或图形信息的场合正在减少。

· 作为信息系统中常用存储部分的机理和"结构"发生了很大发展、变化,这种发展趋势仍将持续。如过去计算机的存储部件由磁芯组成,配合使用的"外存"多为磁带与磁带机,而现在已发展为半导体存储器。原来庞大的外置磁带机被内置硬磁盘代替。硬盘容量大大提高,响应速度也有所提高,可携带存储软盘被小型 U 盘取代;大容量易刻录光盘被大量普遍作为固定式和携带式的存储媒介,微观量子效应为基础的各种存储数字化信息的机理和方法正在大力研究。

· 在各种小型信息装备中用数字化半导体存储器取代大量原磁带、消费类摄像功能的数字照相机导体存储部件,对其性能起重要作用,其他如手机、数字摄像机、PDA 等也离不开半导体存储器。

· 研究发展更高密度光存储科学技术以支持更高密度超高容量(如单盘达 10 GB,系统达 20 TB 容量)存储部件和系统的发展和应用,如光致变色存储、多波长多阶存储、高密度磁光存储等。同时在高密度光盘系统集成中,还综合地需要很多其他信息科技的发展支持。例如,数据可靠性分析、容错编码技术、高速数据传输等问题都需要配套研究和发展。

· 以信息存储机能为基础,结合信息系统其他"功能"将信息存储延伸到过程存储、知识存储和利用,从而形成了一大类为人类各种需要服务的存储式信息系统,如各种数据库、信息库、国家信息基础设施等。数字图书馆也可视为一种由信息存储为基础的图书存储和传播服务的信息系统。以下将以数据库为例说明由系统发展角度观察,"信息存储"(含其应用)尚有众多科技问题有待发展解决。数据库是从计算机科学与技术领域中计算机文件系统发展起来的,从它的第一代树状、层次型数据库发展到第二代关系数据库,再到第三代面向对象数据库(关系数据库还在应用中),数据库技术与众多学科如网络技术、通信技术、多媒体技术、并行计算技术等,形成了多种学科交融发展,在此仅就数据库所存储"信息"所关联的时空域特征进行简要讨论,以揭示"信息"存储内含的复杂本质。

· 数据库"时态"性质:"信息"尤其是信息流,本身包括了必然时态信息(Temporal Information),它包括了时刻信息(Instant Information)、时间区间信息(Interval Information)和时

间相互关系信息(Time Relation Information),表示“信息”在时间上的前后、重叠等关系。可以认为,传统关系数据库主要关心空间关系而很少关注“信息”表征中内含的时间关系,时间关系是揭示事物发展运动本质规律的一个重要剖面,不可以不重视。如时刻信息表征发生时刻,时间区间信息可表征“信息”存在的时间间隔长短。同样,数据管理应用方面也非常需要时态信息,现在已建了多种各有特色的数学模型,用来表征信息的时态特征。同时仍有很多实际技术问题有待进一步解决,困难主要表现在数据量大。随着时间的流逝,新的数据源不断进入数据库,当前数据又逐渐变为历史数据。为了保证时态数据库在大数据量下的时空应用效率,必须有高效的主数据存储组织和时态索引结构,在实际应用的时态查询,“选”—“投影”—“连”操作占用了主要资源,即对时态选择、时态投影、时态连接予以优化,成了时态数据库查询优化中特殊的技术焦点和难点,时态数据库的索引中传统的 Hash 和 B 树、B+树需要扩展时态语义才能适应。

· 数据库实时性质:数据库实时性主要表现在关注数据(信息)的实时特征,以及应用过程和管理实时性。实时性包括事物之间在时间坐标上的一致性,以及保持正确的相互关系(包括了数据库内部事物与相关的外部事物)。这是因为客观事物都是在时空中运动,有些过程对时间的流逝非常敏感,需要的是某个时刻或某个时段的信息,时间轴上很小差错也是不允许的。例如航天计划中某些过程的控制,对高速飞行体的探测、导航等。随着科技发展社会进步,这种场合越来越多,越显重要。在实时数据库构成和管理方面比普通数据库要复杂和困难得多。尤其是数据“一致性”内容增加了时域实时性方面的要求,总体而言实时数据库处于正在发展阶段中。

主动数据库,现在使用着的数据库虽然在各种实际中起了很大作用,但它是以被动方式进行服务的,只能根据用户的命令被动地提供服务,即用户给什么命令就提供按命令规定的服务,丝毫没有根据内部或外部环境状态提供灵活服务的能力,在实际情况下无论在应用中或对库的管理中都需要增加一些“主动性能”。例如入库数据太多或库存太少、主动切换检索方法、主动实现状态修改等都需要加入主动服务功能,这些“主动”功能往往与实时性能有较密切关系。联系到软件方面,必须有一种程序设计语言以独立进程方式单独编写一个程序来实现(在一些语言中也有一些初步功能体现,如 Ada 语言中的异常处理即体现一点主动功能,但很不够),在体现“主动性”中,数据库机能的大部分可用事件激发概念来体现(即数据激发的进一步发展,但比数据激发复杂得多),其含义为主动适应功能的发生,是根据某个事件的发生而进行调整和调度。规定“事件”是重要的,尤其是“复杂事件”中相关联事件的“嵌入”和“调度”构成了事件激发中很大的复杂性,显然有很多问题和困难。数据库具有主动性是一个重要发展方向。

移动数据库,当信息系统越多用于服务在“移动”状态,如移动通信、移动办公、移动计算等,移动状态数据库也因此而必然产生和发展。移动数据库不同于分布式数据库的固定分布式拓扑结构,虽然也具有分布性质但拓扑结构是变化着的,这就给移动数据库带来众多复杂

性。如移动用户应用中的沟通联系、调用数据、要求更改数据、输入数据都很有特殊性和复杂性。再深入一步至移动数据库的运动机制和“动态结构”,如保持数据“一致性”和正确性。“复制”机能要求动态布局,“缓存”(Cache)机能也需要如此。如移动状态再要求“时态”、“实时”和“主动”功能,则更加复杂,现在还远远达不到,移动状态下的服务机制是一个重要的研究发展方向。

数据库的模糊性质不能回避,这是因为客观世界事物之间关系绝不都是确定性的,相当大的部分是非确定性的。其中包括概率、模糊以及混沌不确定性等,研究建立模糊数据库的目的是依此帮助人们处理一些客观存在的模糊性质问题。模糊性是事物间一种较深层次的性质,很大一部分模糊信息是隐性的,要由直接获得的“信息”提炼和转化为模糊信息,然后进入模糊数据库。模糊数据库的建立必须完成以下几种工作:

· 建立模糊数据(模糊数、模糊字符串、模糊布尔量、模糊结构量和组元)。

· 建立模糊数据间模糊联系关系(分为不同层次,每个层次都有模糊性;其数据有模糊性、静态模糊性、互相作用的动态模糊性、模糊函数关系)。

· 建立模糊性的约束条件(模糊完整性、一致性、其他约束性等)。

· 建立模糊性操作,模糊性查询语言。

· 建立模糊数据模型,模糊关系模型,面向对象的模糊模型、模糊层次模型、模糊逻辑数据模型等。

· 建立模糊数据语言是由模型往应用层次延伸的重要环节,如语言的模糊模型为模糊程序设计语言、面向对象的模糊数据库语言、模糊关系数据库语言等。

· 建立模糊数据库管理系统(包括系统接口、模糊操作系统、模糊数据库等)。

由以上数据库的发展体现了以“信息存储”作为基本功能,并将存储功能进行扩展形成一类以存储机理为核心配以其他功能而形成的一类重要信息系统,服务人类。这体现了存储信息乃至存储知识作为一类信息系统的主要功能在信息科技领域内由“过去”到“现在”及“未来”持续传承发展的本征重要性。

三、信息传输部分

“信息传输”也是一个信息系统的基本功能,因人类除直接获取信息外,很多“信息”是靠“传输”和“交换”来获得进而利用的,同时为了更好地传输,“信息”形式往往需要经过“变换”,同时不单在传输部分需要,在“其他交换”信息系统中其他部分也很需要“变换”,它起一种很普遍的作用。

1. 基本概念

“信息”总是被某种媒介所荷载(如“信息”对电磁波某种状态参数进行调制,电磁波就是荷载信息的媒介)。而信息传输多数情况下需要将荷载信息媒介状态(有时也包括媒介体本身)加以传输以达到传输信息的目的。信息传输的通道称之为信道,“信道”可由某种物质组成,也可由多种物质集成。

“信息传输”可以是传输信息系统为用户服务的“信息”,也可能传输信息系统运行服务时所需的管理控制所用信息。

信息传输部分是信息系统内部功能不可缺少的重要功能之一,所有信息系统内部结构功能都是为组成信息系统的功能而服务的,故应以局部服从系统总体原则,使信息系统在满足使用条件约束下能充分发挥服务功能(有很多使用条件的约束增加了发挥服务功能的难度)。信息系统内各分系统都要为此努力“贡献”,并不能过分计较为此付出的“代价”。另一方面信息系统对自己的各分系统也应努力支持,体现在内部结构布局所形成内部功能的互相支持,例如移动通信系统的移动使用条件,使得移动通信系统必须采用无线通信,在城市的移动通信传输中必然碰到动态变化的多路径效应,移动通信的传输信息部分“承认”和“容忍”多路径效应带来的各种负面效应并努力减弱负面效应,同时在系统总体结构方面也体现出适应多路径效应下工作的布局,在信号处理部分也采用多种先进原理和处理方法来减轻多路径效应的危害。又如水下通信必须要忍耐利用超长波的困难,尽力采取各种措施来保障通信。

在传输分系统中为了完成所承担的任务,往往需要采用各种方法(包括与其他分系统实行功能合作和取得支持)和增加一些支持性软硬件实体部分,构成一个具有复杂系统性质的广义信息传输分系统来达目的,例如卫星通信系统的卫星转发器应该包括在信息传输分系统中。

就信息传输分系统的传输方案而言,存在着由系统功能决定唯一方案的情况,也有随着科技进步多种传输方案并存的情况。

以传输各种信息进行服务的信息系统统称通信系统,其中包括各类通信系统,它们的核心功能是“信息传输”。因此,此类信息系统的结构是以信息传输为核心理念,配之以其他功能有机形成系统,从而完成信息传输任务。通信系统将不断发展完备并伴随人类而永远存在。

现代信息系统主要是利用不断扩展的频谱包括电磁频谱和其他类频谱如声波、机械运动频谱等作为传输信息的媒介。因此,信息传输分系统中不断对电磁波和声波等的传输特性和传输方法进行研究,现时在主要方向上已取得很大进展,但仍有大量问题需要研究。在传输过程中为了某些原因(功能需要和约束条件原因等)往往需要对信息媒介的某些特征(在不影响“信息本质”的前提下或可以接受的影响程度下)进行“变换”,各种新的变换形式和方法也是重要发展内容之一。“变换”不单用于“传输”领域,在信息系统内部各结构功能的实现中往往同样需要各种“变换”,“变换”可以是事物运动某特征在不同剖面“表征”的变换过程、结果和方法,它同时蕴涵了事物间相互作用关系和规律,“变换”在信息系统的传输分系统中也具有重要意义。

信息传输和变换的发展对信息系统发展有重要促进作用，其发展基础涉及相当广泛的科学和技术学科领域并与相关基础和应用基础的科学研究水平有密切联系。因此，在不断发展信息传输分系统的同时必须注意相关基础和应用基础研究水平以形成成套地持续发展。

在通信系统中“信息传输”与“信息交换”具有各自功能，在信息系统结构组成中往往关联非常紧密并形成互相嵌入，在工作运行时互相匹配。

信道的非理想状态所造成的影响往往体现在整个信息系统功能和结构上从而产生本质性影响。如水声信道所带来的背景干扰、移动通信中的多径干扰等对系统发展影响深远。

2. 信息传输基本要求

信息传输与变换中对“信息”透明度符合要求。

“透明”是指传输和变换过程对“信息”的特征无影响的理想状态。实际上不可能完全透明，如信号传输损耗、传输色散都不可能等于零，只能控制在允许的范围内。

信息传输过程中应采取相应有效方法以补偿传输过程中对“信息”的影响，如及时放大信号补偿衰减，利用反色散特性补偿“色散”等。

传输信道的状态应根据实际需要加以检测以保证信息系统的服务质量和安全服务。

“传输”和“变换”的时间延时应控制在允许范围内，目前信息传输速度的极限在真空中是光速，在实际应用场合中往往比光速低得多。在地球上及低层空间范围内信息传输的延时尚不至普遍发生重要问题，随着人类“进入”深空，信息传输延时问题将日益严重。

信息传输过程中信息安全问题随安全环境变化控制在合理的安全程度上。

信息传输范围很大时，实施信息传输所付出的代价应综合考虑，如光纤是一种高性能有效传输，现实情况下“到楼”比“到户”更现实有效，这就是一个综合考虑结果。

3. 信息传输分系统实例

如下为移动通信系统分布嵌入式传输系统的示例。

· 手机与固定电话通话(如图 2.3)

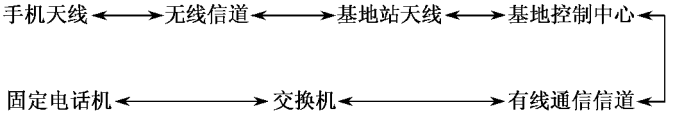


图 2.3　手机与固定电话通话

· 手机与手机在漫游状态通话(如图 2.4)

· 电信网长途电话信息传输分系统示意图(如图 2.5)

现在长途交换机一般还要进行复接编成复接路信号，包括变换信号形成如变换域 DWDN 光通信信号，也涉及传输信号的媒介变化。如对应光信号的传输为光纤线路，在本地交换机间的传输信号传媒多为电话线路，而交换体制是面对连接的，则在一般情况下，不会因信息传输

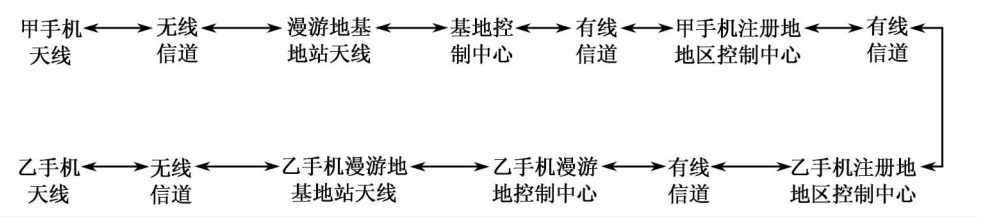


图 2.4　手机与手机在漫游状态通话

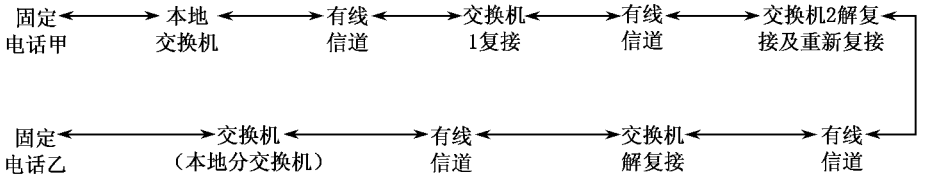


图 2.5　电信网长途电话信息传输分系统

延时不等造成恢复语言信号的严重失真。但在 IP 电话通信场合，便会因信息包(IP)传输中各包延迟不同，而破坏了 IP 对应的原来语言信号间秩序导致通话质量下降。以上说明“传输”部分与其他部分相互渗透制约对完成系统层功能会起相当重要作用，完成一个信息系统的既定功能，需综合运筹决定各部分特性和结构。

四、信息交换部分

1. 基本概念

· “信息交换”也是信息系统应具备的基本功能，它支持信息系统为人类提供传递和交换“信息”的服务。在古时人类也有信息交换和传递，但是以个别专门形式进行的，如派人专送“信息”，烽火台广播发布信息等。随着社会发展，人际交往在时间和空间域中都有很大拓展，如距离增远、交往次数增多、节奏加快等。相应地，要求信息交换在多个用户、分布很广及远距离情况下进行，同时也要求传递和交换更多的信息。由此产生了邮局、电报、电话、电视等多种信息交换方式，现在“多媒体”信息的个人间交换是正在发展中的一种信息传输交换发展模式。

· “信息交换”中单元个数是个重要参数，随着单元个数增加，可能的“交换”组合数快速增加。如二人“交换”只有一种组合即$\frac{2}{2}!$，而 10 人交换则有$\frac{10}{2}!=1\ 814\ 400$ 个可能组合数，“交换”所应具备的组合数随 n(交换单元数)的增加以 $n!$ 方式增加，因此“信息交换”分系统面临第一个困难是解决海量“交换组合”问题。

· 信息交换分系统解决快速交换问题的基本思路是尽可能地利用具有最快传递及交换

速率的荷载信息的媒介体，现在是尽量利用电磁波。关于电磁波的科学技术问题已进行了大量研究，但仍很不够，还需进一步深入研究。

· “信息交换”分系统在整个信息系统内最主要的内部功能（称之为结构功能）是支持和保证信息系统整体功能的实现和完成（局部服从整体原则）。随着信息系统功能增加，服务质量提高，促使交换分系统发展成本身具有复杂系统特性系统（如电信网中程控交换机，卫星通信系统中星座间星际交换系统等）。对其发展应注意使用系统科学的思维方式和方法。

· 大型网络型信息系统的交换分系统，经常需要面对各种异构信息系统和不同服务类型。所需“信息”有不同特征、信息格式，以及执行不同协议情况下进行信息交换。这是一个复杂开放性问题，需不断进行研究，争取以较小代价解决这个问题。

· “信息交换”和其他部分一样，需要众多学科发展所形成的科学和技术支持。科学技术发展水平决定“信息交换”水平，例如：一旦量子信息进入实际应用水平，信息系统的工作原理和条件将有根本性的变化。交换系统也不例外，量子态的不可触及性及非局域性等将给信息传输和交换带来一系列新应用前景和挑战。

2. 基本要求

信息交换分系统的基本要求很大部分类同于信息传输分系统的基本要求，应补充和强调以下几点：

多用户情况下可靠交换问题值得不断研究和发展。交换分系统在一定情况下更是信息系统安全问题策源地，对此应有足够注意（尤其应注意到由“传输”和“交换”可以较有效地扩大对信息系统的各种攻击效果）。

交换分系统结合信息传输作为通信系统核心融入通信系统并构成通信系统框架，类似人体骨架及神经结点两者相结合的地位，因此更应注意此类信息系统中“交换”及“传输”部分的性能水平。此外，也应加紧系统整体及分系统间互相支持，发挥整体优势进行综合运筹考虑。现在应用嵌入式计算机是一关键手段，但嵌入式计算机应用所带来的负面作用也应予以足够重视。

不同信息信号特征对应着不同交换要求，这点与“传输”有共性，但重要性更突出，应予以足够注意。

3. 信息交换实例

现代通信网是以电话网络为基础发展而成，按习惯把“电话”以外的信息传输交换服务叫增值服务，现主要有电子邮件、可视电话、电话会议、电视会议、可视图文、视频点播等，各种服务的信息信号有着不同特性，对“交换”也有很大的不同要求。

各种业务结合信号特征对“交换”性能要求往往差异很大。以下简要介绍几种典型交换的要求：

（1）电路交换（语言信号交换）及数据交换要求

· 人与人之间直接语言信号交流，要求一对一交流，一般不应外泄信息。

· 语言信号误码率要求不高于 10^{-3} 便可以。

· 通信持续时间大，平均在 3 min 左右，而且双向对通各占一半左右。

· 电话通信每路速率 0.3～3.4 kb/s 便够了。

· 在通信中依靠人与人的语言交流不需要其他协议。

· 利用计算机或计算机间信息交流进行数据增值业务（信息的信号形式为 0－1 二进制离散数据形式）不外乎人与计算机或计算机与计算机间交流信息，如经加密传输时可防信息外泄。

· 交换信息为数据形式（多为 0－1 二进制），误码率要求高，一般应在 10^{-8} 以上，甚至 10^{-10} 至 10^{-11}，通信持续时间很多为秒级或数秒以内。

· 信息为数据形式的交换中，时间延迟和信息包间次序在信息传送时要求并不太严格，也允许传送完后整理。

（2）电路交换与数据交换类型特点说明

电路交换示意如图 2.6 所示。交换机集群和用户集群组成的通信网络如图 2.7 所示。

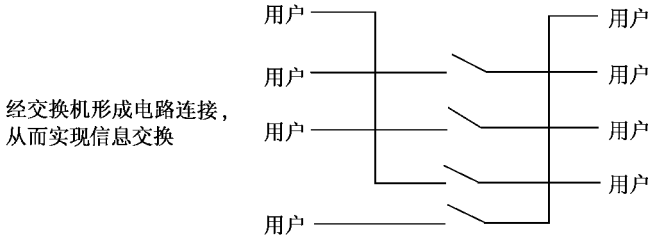


图 2.6　电路交换

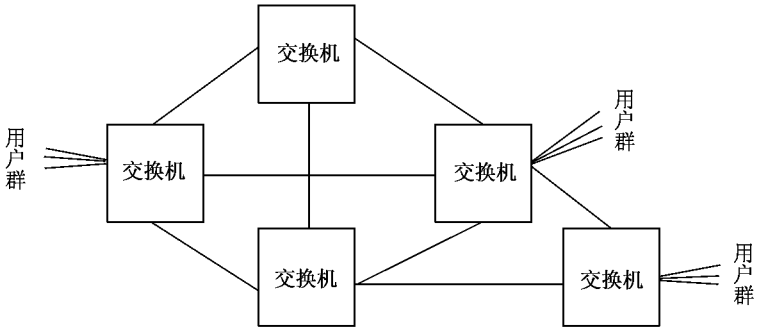


图 2.7　交换机与用户

· 电路交换主要优缺点

优点：信息的传输延时小，一次接续时延固定不变；信息透明传输时交换机不需作存储分析处理；“开销”少，用户信息中不附加很多用于控制的信息；双方的编码方式、信息格式可自主制定，不受网络限制。

缺点：电路进行连接耗时较长，传输短信息时，连接所占时间可能大于信息交换时间；电路资源被通信双方独占，电路利用率低；在通信繁忙时很可能由于电路占用而接不通；双方的信息格式等一旦固定难以适应多种业务间发展不同的协议信息格式等。

· 数据交换

针对电路交换缺点严重影响一些信息服务业务（尤其是计算机充当某些“用户”时）所进行的变革，最初是报文交换方式：其核心概念是交换机内含有存储功能，用户间通信时不需叫通对方，只需叫通交换机将交换信息组成一个“报文”发往交换机并加以“缓存”，而后再叫通对方发送信息。但有以下缺点：即交换延时不固定，可能发生大延时，影响交换及时性，不适宜及时交互通信。报文高速率通信时间较长时，交换机需很大存储容量。

· 分组交换

电路交换不利于实现不同类型数据终端之间的相互通信，而报文交换所引起信息传输延时不固定，有时会很长。减少时延，使之满足利用计算机通信的用户可以及时交互信息（延时比话音延迟要求要低得多）是一种急迫需要，“分组交换”可以较好地解决数据通信中的实时信息交互（利用计算机进行通信），它采用了“报文交换”中“存储转发”方式，但不像报文交换那样以报文为单位交换，而是将报文截成许多较短的规格化的分组（Packet）为单位进行。由于分组长度较短并有统一的格式，所以可在交换机中停留进行排队处理。一旦确定了新路由便很快输出到新的交换机（或终端），这样在交换机中停留时间仅为毫秒级，这样的延时状态能满足绝大多数场合下数据交互式通信的要求。

根据交换机不同的处理方式，分组交换有两种模式，即“数据报”和“虚电路”两种方式，“数据报”方式即是将“分组”当报文处理，每个分组所包含的终点地址信息供交换机为每个“分组”寻找确定路由；可能发生不同路径到达的分组，则由终端进行正确的组排以保证传送的内容不混乱。虚电路方式在开始传输信息时，通过网络建立逻辑上的连接通路，这种通路建立后供用户发送信息用，以分组为单位经由逻辑通路传递。一旦通信完毕则发出拆除逻辑通路的信令并将之拆除。无论哪种形式的分组交换，为了保证数据通信在当时非光纤传输情况下，要得到10^{-9}左右的误码率必须采用各路段按分组进行检验，由路段接收节点（交换机）按分组奇偶校验法，检查是否有误码。如有误则要求发送节点重发而造成延迟，因误码是随机的，故形成了延时随机性。这是一个对于严格要求延时条件下的缺点，但计算机间数据通信是完全允许的。分组交换主要优点除了上述轻负荷传送率情况下延时小、变化不大、误码率低以外，还有向用户提供了不同速度、不同代码、不同同步方式、不同通信控制的数据终端能够相互通信，实现了线路动态统计复用，通信线路（含中继线路和用户环路）的利用率很高，在一条物理线路上可以

同时提供信息以“分组”为单位多条信息通路。

储存和处理不要求交换机具有很大的存储容量，降低了网络设备的费用。但分组交换存在的主要缺点是：由网络附加的传输信息较多，如分组头形成的控制信息，用以建立和拆除数据通路进行差错控制和流量控制信息等。对于长报文，由于拆成“分组”插入的控制信息增加了很多占位，通信效率较低。此外，要求分组交换机具有较高的处理能力，增加了交换机的复杂程度。

· 在光纤传输条件下适应局域网通信为主的快速分组交换——帧中继

分组交换实施背景和保证数据高质量通信的措施。分组交换开始实施时，传输线路（即交换机中继线路）是基于模拟通信为主步进制的电话信道（带宽为 0.3～3.4 kHz），传输带宽一般不大于 9.6 kb/s，误码率为 10^{-3}～10^{-4}，在这种情况下满足数据通信要求必须采取兼顾高效率与低误码率 10^{-9} 的双重措施，主要有：

采用虚拟电路复用方式，可以提高信道利用率，减少网络传输费用。

在网络相邻节点传输通路上执行差错控制协议，具体说便是，发送一组数后等到交换节点返回表示正确收到的返回信号后，再发下一组数据。为了保证传输数据不超过线路的传输容量，要采用流量控制措施，这类同于控差错方法，数据到达后再传送。

用光纤作为局域网传输线路，这时就需考虑到如下特点：

数据传输有高速性，传输速度在 1.544～2.048 Mb/s 之间，光纤传输的误码率很低，约 10^{-9}，甚至可接近 10^{-10}。

传输信息具有突发性，如传输图像和图形时就要求高传输速率。

具有独立端点纠错能力和多协议通信处理能力。

满足上述要求的交换方式称为快速分组交换，即在分组交换基础上改进以满足局域网高速数据传输：

取消了网络节点之间、节点与用户设备间每段传输链路上的数据差错控制，而将差错控制推到终端与终端之间进行，提高了网络响应速度，减少了分组传输的延时。

采用数据“帧”的概念，即为计算机网络分层中的数据链路的概念。将“分组”交换中的“帧”作简化，去掉有关进行链路差错控制帧中的域，则帧中信息字段，不仅可用于分组而且可以存放其他各种控制信息，从而实现不同协议的数据封装和传送。

在帧结构格式中包含的路由选择信息用以指示信息传输的通道。

快速分组交换——帧交换格式可以支持到 34 Mb/s 的传输速率，但是它仍采取建立永久虚电路的方法，同时，由于没有准备适用于不同速率的业务（如低速的音频业务和高速的视频业务），所以目前的快速分组交换——帧中继一般应用于 LAN 之间的互联。

· 异步转移模式（ATM）

ATM 结合了电路交换技术，支持实时业务，和分组交换一样，可以适用各种速率业务，具有较高的复用效率。因此，ATM 适合如 B－ISDN 等下一代通信网交换和复用要求。ATM

的主要特点如下：

采用固定长度(53 个字节)称为信元进行数据交换，在时间上没有固定的复用位置，由于是按需分配带宽，所以取消同步转移模式中帧的概念，与分组交换中分组长度可变不同的是，“信元”长度固定。

ATM 采用面向连接并预约传输资源方式工作，即采用了类同分组交换中的虚电路形式，同时，在呼叫过程中向网络申请传输所需资源，网络根据当时情况决定是否接受，这样就没有传输过程中的流量控制工作，ATM 网络内部取消了链路逐段差错控制的工作，而将这项工作推到网络边缘，由终端进行一定差错控制，以保证数据传输的质量。

ATM 降低了信元头部功能，由于网络中链路段的工作非常有限，所以信元头部变得异常简单，主要是标志虚电路，用以表示分组经过网络中传输的路径，依靠这个标志，可以很容易将不同的虚电路信息复用到一条物理通道上。为了防止分组头部出现差错而导致信元误投浪费网络资源，在信元头部加上了检错和纠错控制。

· 光交换技术——发展中的技术

现在的光网络交换过程中，还做不到全部利用光电子技术进行交换，仍需采用一些电子部件，故缺少不了光电转换部件进行光电转换。由于电子部件的速度不及光电子器件快，因此，进一步提高交换速度的措施是省去光电转换部件，正在发展的光电子技术争取支持全光交换。

五、信息管理控制部分

信息系统的管理控制部分，是信息系统重要组成部分，也是信息系统发展过程中的“瓶颈”之一。它的发展涉及众多学科的支持，是一个交叉融合、复杂发展问题，本小节中作一些基础性介绍。

1. 基本概念

(1) 管理与控制的含义及其区别

“管理”与“控制”的实施都包括主动一方(即管理或控制一方)及被动一方(被管理者或被控制者)，“主动”的含义是其意愿通过一定方式传递至被动方，然后双方按一定的“秩序”共同完成一个运动过程，在“过程”中主动方不断根据运动情况(状态)进行调整以达到“意愿”的实现。“控制”和“管理”的核心内涵，在实施过程有着上述共同点，也有区别，主要区别在于，“控制”要求被控制对象“服从”和遵照“命令”行事，而“管理”则按管理者意图行事的同时，也要注意发挥被管理者主观能动性，所以当管理对象为人时，不要用“控制”一词为宜。

在复杂大型系统中，作为子系统存在的管理控制分系统，常具有完备的复杂系统特征，因此，在研究问题时，应注意应用系统理论中所涉及的系统规律。以使得复杂管理控制系统与功能约束条件之间，形成较高效率和较高和谐程度的相互关系，从而保证高质量地完成管理控制任务。

管理与控制系统中往往涉及人的介入，即人担任管理决策和具体执行管理工作，以及被管

理对象中有人参加。在很多情况下，人既是被管理者又是管理者，在不同管理层次中有不同的身份（这是合情理的）。凡有人介入的系统就大大增加了开放复杂性程度，被称为开放复杂巨系统（钱学森教授提出），它们遵守的机理包括人理、事理、物理及生理四个复杂庞大的“理”领域，更严重的是，四个理领域中大部分内容尚未被人类深入认识，并且“理”本身也在动态变化中。因此，很多管理系统的形成，不得不在各种不确定性、未知性和复杂性所引起的困难中矛盾着前进，而科学地研究人学，并将其基本原理与“以人为本”原则结合，贯彻到有人介入的管理系统中去，是一个漫长具有待发展的过程。

除了上述对“理”认识不足的困难外，还有管理系统所具有的强劲“开放”特征，这个“开放”性不仅是耗散自组织系统原理所指出的，必须不断有物质能量信息输入，并能够通过系统自组织特性耗散内部所产生的熵，使系统得以有序运动意义上的开放性，而还有复杂的管理系统中，事物间的关系引起“关系”套“关系”，很难间断而形成一个封闭的问题范围。关系总是切不断，尤其是当有人或人群介入时，由于人有社会性，因此往往会产生多重牵连。若将复杂的社会关系引入系统，并且全部考虑各种社会关系，则无法解决问题，因此选择重要的问题加以考虑，且采用类同问题的有效解决方法和模式是一种聪明有效的措施。

（2）管理人（对人的管理）的初步讨论

对人的管理，有一条重要原则，即要求被管理的人按一定规则严格准确地完成工作。但当工作环境发生变化超出“常规”时，则需要人能发挥主观能动性完成工作。这种非常发挥与被管理人本身所具有的主动性素质和能力有关，同时也与管理机制有关，对人进行科学管理的一条重要原则是在“以人为本”的原则下，科学地应用对人的激励与约束对立统一规律，即又对立又统一，不断在对立面间科学转换并不断发展延伸。激励和约束的基础因素是人的需要，但要结合实际情况进行实施。下面简要说明人的各种需要：

· 生理需要：这是人生存中最基础的需要（指正常生理需要），如衣食住行方面，如果扩大范围还应包括抚养家庭成员的生理需要。

· 安全需要：这是第二层次需要，包括直接意义上的个人及家庭成员的人身安全需要，还包括了对个人安全享有生理需要意义上的“安全”需要。

· 感情需要：人具有社会性，每个人都生存在社会、人的群体中，因此需要友爱和忠诚对待。同时，也需要群体和社会接纳自己以及自己的融入，这种“接纳”和“融入”在感情上必有所表现，对个人而言是需要这种“感情”的。

· 被他人和社会尊重的需要：一个社会的成员都有自己独立的人格和个人的尊严应该得到承认和尊重。除此之外，随着一个人进入社会的阅历的增加，希望别人和社会对自己的言行更多些尊重（体现在各个方面），这是一种精神上高级的本征需求，这类似于随着子女的成长希望父母对自己更多一些尊重而不希望一切都听从父母指挥一样。

· 自我价值实现的需要：每个人都有着不完全一样的人生价值观，除了极少数人缺乏明确的人生价值观外，所有的人都有实现自己人生价值的需要，其中包括争取和创造条件去实现

的需要，也包括社会或他人对自己的努力成果的承认和肯定，这是一种最高级的需要。

以上五种需求，是人在社会生活中多种需求概括形成的对人的“激励”因素，对人的激励要激励在需求上，而“约束”则不能从根本上限制人的正常需求，两者科学地对立统一才是管理之道。

(3) 信息系统的管理

现代大型信息系统，往往服务功能多，覆盖范围广，系统结构复杂并深深嵌入到社会中，对社会的发展有着重要影响，信息系统中的管理控制分系统对整个系统运行起着关键作用。因此，除了注意管理的共性外，还应注意研究信息系统的特点，它们主要有：

· 信息系统的管理部分(分系统)是以嵌入、交叉融合的方式在结构上与系统结合的，在功能上起着管理控制作用。例如，通信系统管理信令的传输，大部分情况并没有单独的物理信道，而是共用信息传输信道。存储交换设备也有很大部分共用。如“地址”(IP 地址)既可作为信息传输用，也可用做管理甚至收费。管理控制部分也可分布嵌入到信息系统各分子系统中完成相应的管理控制功能，这种情况也很普遍，如手机的 SIM 卡嵌入到手机起管理作用。

· 大型信息系统的管理子系统，在管理功能上具有明显的系统特征。如开放耗散自组织特征，多层次管理控制功能的时空交织动态展开特征等。管理控制系统功能的形成，是将各部分的管理控制自组织功能进行系统集成而产生，整体功能的发展是各子系统功能发展在时空展开的有机形成，如 Internet 中 IP 层协议由 IPV4 发展到 IPV6，会对整个 Intetnet 网的管理起重要发展的作用等。以上实例说明，管理规律具有复杂的系统性质。

· 信息系统的管理分系统，总体上涵盖以下几个不可缺少的内容：服务功能和服务质量管理、服务运行管理(含与其他信息系统协同运行)、系统安全管理、资源调配管理、故障检测及修复管理、费用成本管理、发展策划与管理、管理人员的管理等。以上八项管理内容互相交叉交融，同时每项内容中可划分众多子项。除此以外，每项管理内容必然会与外部社会运行的法律法规、规章制度等有密切关系，形成非常复杂的管理内容。在制定信息系统的管理内容时，则应尽量构成独立可操作运行的完整体系，并力求简明扼要，易于贯彻执行，“间断”地划分出管理界限，使的内外有别、职责分明，这样才能有效进行管理。

· 管理控制系统动态过程的重要依据是“管理信息”，包括被管理对象的状态，外部环境状态等集成管理信息对它进行管理利用。如果没有及时正确地利用管理信息，则信息系统无法得到科学正确的管理。

2. 管理控制功能的七元关系组表征

信息系统管理控制功能的实施，可以看做是一种管理控制动力学过程，而其中的控制功能(一般不包括将人的个性进行控制)，可认为是以控制理论为基础，对控制对象进行控制的过程。根据具体的控制对象，还应将有关控制对象特有的管理控制规律加入到管理控制。例如，费用管理控制应加入财务金融管理控制规则；安全控制应加入信息安全领域所具有的特殊规律，甚至考虑与相关法律有所连接。很多复杂的信息管理分系统，不可避免地属于钱学森先生

所提出的开放复杂巨系统领域，因此，研究信息系统的管理控制分系统，在思路上应该利用定性和定量相结合的系统集成方法。

· 定性和定量分析相结合原则所奠基的七元关系组框架。

用 $R_m^n(P,S,O,I,E,C,t)$ 表示管理控制动态过程的关系组。

其中，m 表示由 m 个动态关系所组成，n 表示第 n 个动态关系，t 表示时间。

$P(S,P,t)$，P 表示管理目的，它是广义的空间和时间函数。

$S(O,P,t)$，S 表示管理主动方与体现为包括 O 的广义空间和时间函数。

$O(S,P,t)$，O 表示被动方与体现为包括 S 的广义空间和时间函数。

$I(S,P,t)$，I 为管理信息。

$E(S,P,t)$，E 为环境项，表示与更高层次系统之间的关系。

$C(S,P,t)$，C 表示对管理系统的约束和对管理关系的约束关系集合。

$R_m^n(P,S,O,I,E,C,t)$，表示由 $R(P,S,O,I,E,C,t)$ 组成的关系集合，其具体形式可以多种多样，如微分方程、代数方程、模糊关系以及几种形式的结合，其动态性质的表现，除了各“元”是时空动态函数外，$R_m^n(P,S,O,I,E,C,t)$ 本身也是在时空中动态变化的一个复杂事件，需利用定性和定量相结合方法，通过建立多层次模型并不断验证修改，才能近似地建立上述 $R_m^n(P,S,O,I,E,C,t)$ 七元关系组。

3. 移动通信系统中管理控制分系统的实例(GSM)

移动通信系统的管理控制系统是移动通信系统中一个重要的分系统，它的工作正常与否决定了移动通信系统能否正常服务。

移动通信管理控制分系统，是一个开放、复杂、多功能、多层次分布嵌入式管理控制系统。其开放性体现在其管理控制功能交融至其他不直接属于本系统的管理控制系统，即有支持其他系统进行管理控制，也有需要其他管理控制系统的支持(论及系统间的“开放性”，即在更高系统层次而言就称之为集成性)；复杂性体现在管理控制工作性质的精细复杂性，同时也体现管理系统结构组成的多层次交叉融合的复杂性；分布嵌入特性表现为某些功能在空间上分布在整个网络空间，时间上嵌入其他功能中，如构成路由链路管理的信令地址嵌入到信息数据流中。移动通信的远距离通信要利用光纤通信，这就形成了两种管理的交融，又互相嵌入，这些都体现了嵌入特性。

(1) 管理功能的介绍

一般分为按日常时间连续管理和定期或事件激发进行管理两类。日常时间连续管理，功能有：日常服务运行管理、日常运行收费管理、运行质量控制管理、管理人员的管理等。定期及按事件发生的重要管理，有网络故障预防及故障消除修复管理、发展策划与管理、资源调配管理等。总之，移动通信管理控制系统由多层次、多种管理功能集合而成，是一种很复杂的管理系统。

(2) 各种通信应用情况下，由通信链路形成管理示意图

· 在同一注册地，同一小区移动用户间通信（如图 2.8）。

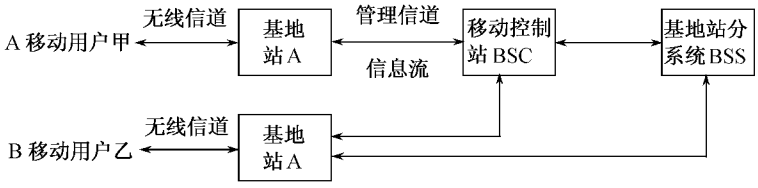


图 2.8　同注册地移动用户间通信

内含用户确认，时隙频率分配，加密算法等形成通信链路，及通信完毕后链路拆除等，如一个用户移动出蜂窝小区，则应加上小区跨接管理。

· 移动用户漫游状态与固定用户长途通信（如图 2.9）。

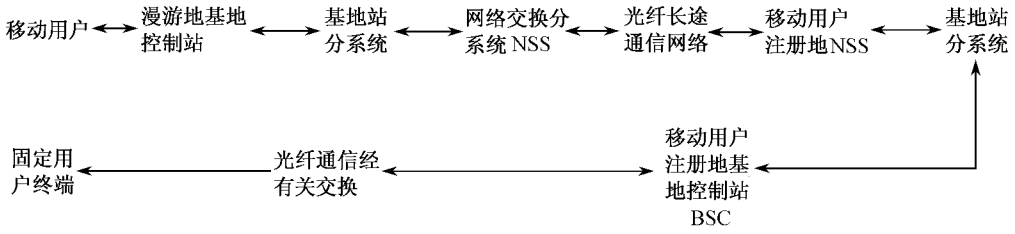


图 2.9　移动用户漫游状态与固定用户长途通信

特点是通信链路中一定要包括移动用户注册地的 BSC，在很多情况下形成反复绕行也在所不惜，因计费管理等管理项目必须在注册地移动站分系统（BSS）上进行，在上述管理流程中每个节点及节点间尚有多层次的管理细节，如移动信道中的时隙频率分布管理，移动网络与光纤通信网络间协议转换连接，光纤通信链路中的复接、分接、交换管理等，管理控制功能的多层次叠套交织才能形成通信链路，完成通信。

上面的示图内包括了建立通信链路和管理信息流通信两部分内容。

· 移动用户漫游状态相互间长途通信（如图 2.10）。

这是一种接入环节比上小节环节更多的链路形成管理。

如果是国际长途通信（现在仍限于两移动用户间使用同一移动通信体制，将来可实现经 BSC 对不同移动通信体制进行转换通信），则在光纤通信网络中增加国际交换节点以保证通信。NSC 按分布式结构考虑，如图 2.10 所示。

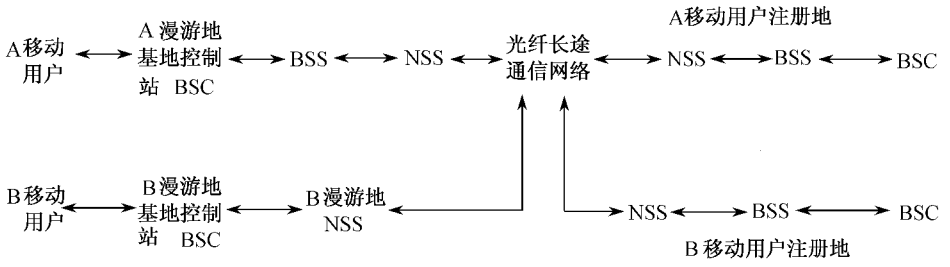


图 2.10　移动用户漫游状态相互间长途通信

六、信息(信号)处理部分

1. 基本叙述

“信息处理”是信息系统的核心功能,因为在实际复杂环境中,只有经过“信息处理”才能提炼出所需的“信息”加以应用,人类利用各种“信息”的最后准备“工序”都离不开人脑的思维。人的思维是最复杂的信息处理,现代人对自己“思维”的科学规律所知尚处于初期阶段,加上下面将要讨论的“信息”和“信号”处理领域中众多需要解决的问题,因此,可以认为信息处理领域对应着一个庞大有待认识的学科前沿领域。人为“万物之灵”,具有很强的信息获取能力和“神奇”的信息思维处理能力。但仍不够,人要不断追求利用信息系统作为工具帮助自己,这样便产生了信息系统的“信息处理”问题。

在讨论问题前,首先需要说明“信息”与“信号”之间内涵的区别。然后讨论作为“信息处理”的一个重要分支领域“信号处理”的发展近况。“信号”是“信息”各种表达形式的总称,即“信号”荷载了“信息”并加以“表达”,还应注意到一种事物的运动(状态)可以有多种“信号”表达(一种运动状态可以经过多种“映射”,从而形成多种不同的“信号”)。例如:一架飞机在天空中飞行,可以用雷达去发现并跟踪记录其飞行轨迹,可用人眼观察其飞行,也可用红外仪测量等,这体现着人需要各种信息系统来帮助自己。因为信息系统不可能在理想纯净“环境”中形成和获得信号。信号总是“伴随”着干扰,或是说信号夹杂在干扰环境中“存在”,因此需要从干扰环境中识别出“信号”及由“信号”中提炼出信息参数(即表征运动状态的参数),这种方法称为信号处理,它是信息处理的前期工作,也是信息系统的主要功能之一。只有经过信号处理才能提炼出信息,后续工作才能延伸完成。信号发展初期来源于实际需要,如雷达应用中,远距离飞机的回波信号淹没在噪声中,如何在噪声背景中检测有无飞机回波,声纳探测、卫星遥感信号也有从噪声和杂波背景中检测某种所需事物的辐射波问题。所以信号处理开始便遇到了从具有随机性质的噪声信号背景中提炼所需信号(本身也具有一定随机性)的问题。化为数学问题便是随机信号的统计检测和参数估计问题。紧接着就要涉及随机信号的特征提取问题,开始阶段对各种随机信号未作深入实际研究,只能由常碰到最简单的随机信号类型入手,这就

是平稳随机过程中高斯分布随机信号。但复杂的实际应用绝不是这样简单，需要修正假定的前提和更细致的参数估计。信息科技在广泛的应用领域中，都离不开非理想环境下提炼信号，因而广泛地需要“信号处理”，这门学科经过几十年的发展逐渐形成了一门独立的新信号处理学科，它现在仍在发展中。

2. 信号处理

上小节叙述了信号处理学科发展的概况，本小节将扼要介绍发展内容。信号处理学科的发展除了理论内容外，还有结合实际应用的问题，所以它的发展有理论和实际结合内容。这主要体现在理论发展的基础上研究新的算法，并根据需要和数字芯片发展情况，研制、设计各种需要的新型信号处理机。信号处理领域与计算机科学技术和微电子集成芯片等有关学科联系紧密，从而形成了信号处理的跨学科特征。例如：由信号处理实践推动 DSP 芯片在信号处理领域的应用研究，就具有明显的跨学科性质。

(1) 信号处理学科发展概况

信号处理学科发展的概况集中体现在如下几点：

· 信号和干扰噪声的概率特征，由高斯型向非高斯型发展，由平稳型向非平稳型过渡。

· 对象系统由限于时不变(或缓变的)线性和因果最小相位系统，向时变、非因果、非最小相位、非线性系统变化。

· 信号处理系统的性能，由概略型向精细个性化方面发展(对具有一定特殊个性对象能精细对待其特征并进行特殊处理)。信号处理的前提条件，由对象严格限定并已知信号处理所需的前提条件向对象较宽松的限定条件过渡，由已知前提条件向未知前提条件(含概略知前提条件)方向过渡，信号处理系统的结构，由简单、单通道向复杂、多通道变化。

· 信号实现方法(算法)和系统构成(软硬件)，与计算机科学技术和微电子集成芯片(DSP、存储、接口芯片、嵌入式系统、SOC 系统)形成互动交融式发展。

(2) 信号处理学科内分领域组成及其发展概况

最开始是基于数学领域中概率及随机变量、随机过程为基点，发展至随机参数估计、假设检验为基础的信号检测，信号检测主要用于从噪声背景中确定(或称检出)信号存在，它属于最简单的一种“信号处理”，但应用中仅是确定信号存在远远不够，还需要对信号本身作进一步处理以获得信号中各类信息。这种处理中很大一部分称为“波形估计”，它包括了信号滤波，波形和各类参数的估计，以及延伸至产生随机信号系统的“辨识”与建模。典型的波形估计分为平滑、预测、滤波以及滤波加预测等几种，波形估计所采用的基本方法是线性最小均方估计，实现这一估计的滤波器是维纳滤波器(针对于时不变信号情况)和卡尔曼滤波器(针对于时变情况)。

在提取信号特征(对应于产生信号事物的信息)中，有一种特征，即随机信号的谱是非常有用的，如它可代表事物运动速度、加速度，部分情况事物所在的方向等，产生了谱分析和现代谱分析分支。现代谱分析提高了谱分析的精确度和分辨率，主要包括 ARMA 谱分析、最大似然

法分析、熵谱估计法和特征分解法四种，各自具有自己的特点。谱分析法只适用于平稳随机过程情况，只在平稳随机过程情况下才有现在定义“谱”的概念。

在波形估计和分析中，常用“滤波器”的方法实现（卡尔曼滤波器用得较多），维纳和卡尔曼滤波器应用前提是，信号和噪声的统计特性先验已知情况下，这两种滤波器才能获得最优“滤波”，如果统计特性并不固定而是有所变化，则要应用自适应滤波方法，通过自动地调整滤波参数获得较好滤波效果，这就发展形成了“自适应滤波”信号处理分支，它主要包括递推最小二乘（RLS）滤波器、最小均方滤波器（LMS）滤波、格型滤波和无限冲激响应（IIR）滤波器以及自适应噪声抵消方法等。

很多情况下，假定系统输入激励信号和加性观测噪声分别属于同一种分布（更确切说，是事实上假定为高斯分布特性），实际中所遇到的时间序列，明显是非高斯概率密度分布的，或多数时间是高斯分布少数时间是非高斯分布的，对于后一种情况出现非高斯分布可视做“异常”（Outlier）。在存在“异常值”的时间序列，如使用一般的最小二乘或最大似然法，将给出极不稳定的处理结果。为了得到数值上稳健的估计结果要采用鲁棒方法，主要包括信息异常值模型的 M 估计、广义 M 估计、RA 估计与 TRA 估计、递推广义 M 估计、鲁棒非参数估计等各种方法。在时间序列不符合高斯分布情况下，信号处理的方法必须由高斯假定下向非高斯型发展，这就形成了非高斯信号处理这一新发展的分支领域，它的主要内容有（主要基础为累积量）基于累积量的 FIR 系统辨识、最小相位 ARMA 系统辨识、基于累积量的阶数确定、非因果系统的辨识、基于累积量的参数自适应滤波、非高斯噪声中非高斯信号检测等等。

在信号分析中现在经常利用各种变换，从信号中抽取有用的信息。在进行分析前总需要有一定的前提条件，主要表现在对要分析信号作一些先验假设，再按假设确定一定的分析方法，以取得好的结果。但当分析信号不符合事前假定条件时，分析的结果会有所差异，性能有所降低，改进这种情况便需要设置新的条件，按新条件寻找新方法。在以前使用变换方法时，都假定信号是平稳序列，傅里叶变换等（一维变换）方法都很有效，但在非平稳或时变信号情况下，要采取时频二维变换才能有效，由此发展起来面向时变信号的时频变换信号处理领域，它主要包括短时傅里叶变换、Gabor 展开、Wigner－Villa 分布及小波变换，现在还有正在研究的分数阶傅里叶变换等，其中小波变换是大量研究的一种新变换方法，包括连续小波变换，离散小波变换的框架理论、正交基小波、多分辨分析小波与 FIR 滤波器组、小波与 IIR 滤波器等内容。

在雷达通信、声纳、地震探测、射电天文探测等领域中，为了改善信息系统的性能，采用了阵列天线进行有方向性的发射和接收，随之而引起在信号处理领域阵列信号处理分支的建立和发展，延续今后一段时间仍将有较快发展，以及对应的实际应用。其分支学科针对的应用领域为信号源定位，即确定阵列信号源的仰角和方位角（近场信号源的距离测定），信源分离即确定各个信号源发射信号波形（由不同到达方向，即使它们在时域和频域是混叠的），信道估计即确定信源与阵列之间的传输信道的参数（多径参数等）。

由信号处理学科的发展状态分析，可以得出以下结论：经过了几十年的发展，信号处理获得了很大的进步，但仍有众多的科学技术问题有待研究解决，所研究问题涉及众多交叉前沿学科内容（含基础学科前沿内容），在理论支持下结合微电子芯片的发展，信号处理的实际应用水平也会继续快速发展。

3. 通信信号处理

无线通信是信息领域重要分支，尤其是数字通信技术和计算机科学技术的诞生与应用，更是极大地推动移动通信科学技术的质变性发展，在具有革命性的发展中，实践和科学理论都需要一门专门的学科，来研究通信领域和移动通信中信号处理问题，例如，在城市环境中进行移动通信时，对多径效应造成的信号衰落处理问题，多用户使用时涉及在时间维、频率维信号形式，以及功率维中如何最大效率分配使用有限资源，同时保证高质量通信等重要实际问题。在这些问题的研究解决中逐渐形成了一门新的通信信号处理学科，它是一门理论结合实际应用的学科，它的发展有力地推动了通信信号处理应用水平的发展。这门学科有以下特点：

· 通信方主要是以合作方式工作，对发射信号在接收端完全重构或恢复（通过接收和信号处理）有非常严格的要求。

· 通信系统的发展越来越要求具有高速率、宽带宽、高质量的传输功能。

· 通信系统越来越要具有非常多的用户在时间、空间域，高速无缝隙通信，并具有高可靠服务功能。

· 通信信道由于通信系统分布所形成的拓扑结构越来越复杂，外加时有变化和电波传播的多径效应，使得移动通信信道尤其是城市中变得非常复杂且多变。

· 通信所能利用的资源有限，并具有很强的应用约束，外加众多用户分享资源等因素，引发在科学技术上迫切需要研究如何解决高效率的分配利用资源并保持高质量通信的问题。

通信信号处理这门学科可认为由两部分组成，即由通信信号和通信信道研究作为本学科的基础理论部分和现代通信信号处理理论与方法的第二部分共同组成。以下扼要介绍各部分核心内容：

首先研究信道问题，无线信道发射端到接收端是无线的，是电波传输媒介的总称。无线信道非常复杂，尤其是高频率段（VHF 以上频段）信道用在城市中移动通信工作，由于众多障碍物及人工建筑物对电磁波漫反射阻挡，使得接收无线电信号受到了多种干扰，可划分为码间、同信道干扰，同时伴随着信号严重的时变性衰落，如无法消除这些干扰和信号衰落，主要影响是无线通信系统（尤其是移动通信系统）无法正常工作。产生接收信号与各种干扰并存是无法避免的一种物理客观存在，其原因是电磁波在传播路径中碰到与其波长相比尺寸大的障碍物形成反射波；遇到比电磁波波长小的障碍物或单位体积内障碍物数量较多时，则形成电磁波的漫射；障碍物边缘不规则则产生绕射。由这几种波的时变复杂叠加的电波传输情况形成多路径信道，它被认为是有限带通信道（这是一个合理和符合绝大多数实际情况的认定），正是由于信道的有限带通特性（非理想），形成了信息调制信号码元的“拖尾”，从而形成码元间干扰。此

外，多用户信号在同一信道内共用，以及蜂窝小区隔区频点重用形成同信道干扰。临近小区所用的不同信道信号形成信道间干扰。由以上简要论述可看出，社会发展孕育出移动通信及其大规模的普及是使信道复杂化的主要原因，针对非理想非平稳信道的客观存在，人们很自然地要研究这种情况下处理利用信号的基本理论，研究不同的调制类型来形成较理想调制信号，以匹配信道特征得到较好的通信质量。由这两个命题形成通信信号处理学科的部分基础性内容，它主要包括通信信号的表示及特征、无线电信道的动态特性与参数、调制技术、最佳接收机、扩频信号、信源编码与信道编码等。通信信号处理第二部分大多是最近发展中的理论和方法，大体内容有信道辨识与均衡，由于信道响应特性是未知的和变化的，针对未知、非理想信道和加性高斯白噪声，讨论消除码间干扰和补偿器（称之为均衡器），包括内容有反卷积和均衡的基本讨论。信道具有码间干扰的最佳接收机、线性均衡器、决策反馈均衡器（原理上不需要使用训练序列进行均衡，实用上是定期发送已知训练序列）、分数间隔均衡器（均衡器抽头间的间隔为码元间隔 T，称波特均衡器，均衡器抽头间间隔为 T 分数倍的均衡器称为分数间隔均衡器），能补偿输入端信号频谱中非混叠产生。固有的信道畸变在信道时变情况下的均衡器要利用自适应补偿方法，它的主要研究结果有 Bussgaug 自适应均衡算法、基于高阶统计量的盲均衡，以及利用接收和发射端循环平稳性的盲信道辨识与均衡（两种方法）、阵列信号处理和自适应阵列处理，其中主要内容有 Bartlett 和 Capon 波束形成器和改进分辨度的 Music 算法等。研究多径对最佳空间滤波的方面有，确定性盲波束形成、盲信号分离、盲信号分离的神经网络算法、最小二乘恒模算法、解析恒模算法、多目标自适应波束形成器、基于子空间的自适应阵列处理等内容。针对多用户运行，在干扰环境中（干扰数字串中）可靠地解调某个特定用户信号的多用户检测方法也是一个重要研究方向，在 CDMA 体制中研究 CDMA 通信中各种特殊环境下的信号处理问题也是新发展的通信信号处理中的一个分支。总之，通信信号处理作为一个新学科，将继续与通信领域进行互动式发展。

4. 信息处理

以上两小节信号处理的基本模型和任务是：在概率不确定测度下，存在随机性噪声干扰及信号具有随机性质情况时，对信号进行处理以提炼其中所含信息（检测信号是否存在，提炼信号中所蕴涵的信息参数）。在多种实际信息处理的场合，并不满足现有信号处理学科所设立的模型框架，问题复杂得多，将涉及更多的科学技术领域（很多问题尚属“未知”领域）。因此，信息处理领域还处在一个初期发展阶段，尚未形成学科基本框架和理论体系，下面只就几个重要研究问题加以介绍。

① 更广泛复杂背景环境下的信息选择问题。不同事物映射形成相似信号，但要求挑选其中一种事物所表征的信息。如两个运动体运动轨迹在荧光屏上点迹相交后，要求继续正确延伸航迹，地物与飞机的电磁回波相似情况下要求挑选飞机回波，这类信息处理解决问题的思路是找出“信息”中存在差异之处加以利用。信息处理中时空二维处理是这种思路的初步发展。

② 在存在虚假信息情况下，对“真信息”进行选择，这是个不能确定一定会有解决方法，而

需要根据实际情况尽量解决的难题。原理上是在时空域中寻找“信息”的“差异”，即使找出了“差异”，是否能进行正确选择是一个延伸的难题。很多情况下只依靠现有“信息”很难对事物进行真伪判断，需延伸至运动过程中进一步加以判断。

③ 按事物某特征或过程特征在海量信息环境中选择相关信息。例如，按某研究课题挑选重要信息，要求快速较准确无遗漏选择，现在还远远无法做到。

④ 对具有模糊不确定性质事物间发生相互关系时对应的信息处理，此种类型的信息处理问题研究开始于模糊信息处理，属于初始发展阶段。

⑤ 对“信息”附加义的处理及对信息作品深层次附加义集群的获取与处理是一个重要问题，“信息”是运动过程中众多状态的一个表征，“状态”与“状态”间相互关联会产生附加义（“状态”是构成“运动”的“元素”）。元素间有机地关联构成整体，由少数“元素”中能得到多少有关整体的“信息”（完全得到是不可能的！）是个不确定而又值得争取的事，人们日常所说“联想起来感觉到什么”其中“什么”便是附加意内容，文字也有附加义，这是因为语言学的“义位”是有附加义的，一个句子也会有附加义，一个语言作品的附加义更多、更深刻。对艺术作品讲究深层次艺术附加义的学派便是印象派艺术家，中国文化特征之一是重视作品的深层次附加义。一个信息作品可以用来表征一个复杂的运动过程。其中所含的附加义集群，内含更多深刻意义，应争取获得并加以利用（情报分析工作的核心便是分析“信息”，得到深层附加义集群以推测事物发展）。总之，附加义是一种客观存在，人们很早便加以利用了，但由理性角度加以研究却是不久的事，利用信息科技领域加以研究才刚刚开始。进一步讲由信息系统来帮助人作附加义的处理当然是一件好事，但这是一件将来之事，取得明显科学技术突破后才能加以应用。

⑥ 在各剖面运动交织组成的复杂运动情况下，必有相应的融合信息存在，依据这个原理人们可从两方面加以利用，一个方面是从得到的交融信号中提炼某剖面信息，从而得到对应运动剖面的状态，通常称这种工作为数据挖掘。另一个方面是根据某种运动特征的应用目的，研究能表征复杂运动有关剖面对应的多种交织融合信息，以便在应用中能根据融合信息较深入地认识复杂运动中所感兴趣运动剖面的状态。一个是分析方法，另一个是综合性方法。

上述信息融合与信息挖掘是（尤其是）复杂事物运动过程中客观存在的性质，对此加以利用是理所当然的事。人类自古代便会进行这样的思维并加以利用，有些已成为人类进化的本能，但并不具有自明科学理性（即不明科学机理）。例如，二岁幼童能从复杂的信息环境中准确地找出妈妈，这是一个信息融合与挖掘结合应用的例子，但幼童并不知道用何种方法识别妈妈，更谈不上在信息系统中人为地、较完备地设置这种机能。现在信息系统中仅限简单的依此概念进行并列地设置数个信息源，以互补性获取信息，深层次的“融合”与“挖掘”还没有做到。

例如，在探测卫星装上多波段、多光谱的探测器，利用多光谱信号进行信息互补或重复性确认。虽然上述工作有时发挥了重要作用，但从掌握科学规律角度大都仍处在初期阶段，还有待长期深入研究和发展。

在重要的运动过程中，某些环节的状态往往起着决定性作用，杰出地利用信息处理手段可

以从掌握“决定性”环节开始，进而掌握重要过程，这种“应用”在具有系统竞争或对抗性的场合能起到决定性的作用，但往往需要靠人发挥高度智慧进行系统策划，单独依靠具体的技术难以取得重大效果。如在 1942 年日本准备对中途岛发动战役攻击前，美方破译日方密码电报后发觉日方意图，但对日方用核心密码加密代号 AF 所代表的攻击地点却无法破译，美方想出用自己低级密码，故意发出假信息“中途岛淡水设备损坏”，诱使日方破译此假信息，看日方反应，再由日方对此假信息反应电报加以验证自己的猜测，历史事实是日方后续电报中称 AF 淡水设备损坏，这就验证了 AF 代表中途岛。这是一个信息处理中的重要环节，这个环节的设置主要是靠“对抗”谋略性智慧。

根据以上论述，可对信息（信号）处理做出以下简要结论：就整体功能角度而言，信息（信号）处理，包括了信号处理（作为基本部分）和信息处理，“信号处理”已形成了一门学科，形成了专门信号处理学科，其框架正向非高斯、非平稳、非线性、精细分析等方向发展，其征程还较漫长。严格意义上讲信息处理学科发展更处初期阶段，很多高级的信息处理人脑子可以完成，但处理的核心机理，人自己还很不清楚。因此利用信息系统完成类似人“思维”模式的“信息处理”以帮助人类利用信息，现在还远远不能做到，有待人类艰苦、长期的努力。

七、应用支持部分

由于各类信息系统嵌入社会，人类活动日益离不开信息系统的服务，“信息系统的应用”形成一个重要的独立领域，在科学技术上对应形成了一个学科交叉的领域。针对解决复杂的应用问题，“需求”必须和科技结合，信息系统广大的应用领域才能不断支持信息系统的应用。久而久之，在信息系统中逐渐形成一个功能组成部分，其功能为“应用支持”，即在本系统中有部分结构起外引内联作用，以使本系统可以扩展应用功能构成新应用系统，在应用所需的支持技术和过程较简单情况下，往往由系统的管理控制部分，在管理系统正常运行中一并蕴涵应用支持功能。例如，全球通移动电话系统，其管理控制非常复杂，构成一个复杂的管理控制分系统，它蕴涵了支持用户应用（用户应用很简单，只需拨号就足够了）；又如计算机应用中，很多编程必须用高级语言，编译程序在计算机领域中称为一种实用软件，性质上属于应用支持功能层次，而操作系统的性质属于管理控制部分。具有特殊性能的新应用场合在信息系统中需有部分结构（软硬件）以支持其特殊应用，往往起到加强嵌入式功能的作用。

1. 基本概念

信息系统应用领域的事物，需要联结信息系统应用支持部分才能充分发挥应用功能，而应用支持部分的本质特征，一方面要尽力支持应用领域发挥预期功能，另外一方面又要根据信息系统的特性，经过应用支持部分的变换匹配，使信息系统“能”且高效率地完成所需应用功能。

应用支持部分完成变换匹配功能的基础是科学技术进步及其巧妙的应用，只有不断应用科技前沿研究的成果，才能使应用支持部分能支持不断发展的应用需求。例如，利用 PC 机形成多媒体音视频应用系统，则应用支持部分必定需要先进的压缩和解压技术，完成视频和音频

信号的压缩和解压，否则 PC 机无法承担处理视、音频的任务，而压缩和解压的新原理、新技术的研究一直持续不断。

应用支持部分的设计核心理念是，屏蔽内部的复杂处理信息过程，增强对用户的透明性，以便用户推广应用。

由于信息科技发展迅速，应用领域服务功能类型急剧增加，形成由基本功能概念上划分的七部分，服务水平和层次越来越高，促使信息系统运行机理的系统性大大加强。在实际系统结构上和业务过程中，七部分互相交融，“你中有我”、“我中有你”，并不能严格、绝对划分为各部分的独立操作，其结构界限往往具有模糊性。应用支持部分往往也需要其他功能部分支持，形成分布有机集成。

2. 应用举例

计算机软件层次可划分为应用软件、实用软件、系统软件、机器指令集，如表 2.2 所示。

表 2.2 计算机软件

应用软件	各应用领域软件，如财务软件、教学软件、销售服务软件、游戏软件、分领域工具软件等，多媒体应用软件大部分是多媒体最终产品
实用软件	一些常用较通用工具软件，如信息采集软件、专用领域编译系统软件、应用变换软件等
系统软件	操作系统，一些通用编译系统软件等
机器指令集	CPU 的机器指令

表 2.2 中，实用软件层次的软件有应用支持功能，应划入应用支持部分（它可常驻计算机内也可临时调入），普遍常用的应用支持软件多已常驻计算机内，有些甚至融入系统软件之中。下面结合多媒体软件进一步说明，多媒体软件按其作用功能分为五个层次（由顶层应用开始）：多媒体应用软件，多媒体编辑创作软件，多媒体数据准备软件，支持多媒体的操作系统，驱动软件。将这些软件对应到信息系统普适的功能进行划分，则应是多媒体操作系统以及多媒体驱动软件属管理控制部分（专门控制管理分支），多媒体编辑创作软件和多媒体数据准备软件属于应用支持部分，各种应用软件属于应用层。下面将各自功能扼要说明如下：

应用软件与应用密不可分，专用软件产品如电子教材、电子书籍、电影、人参与的游戏等。

多媒体编辑创作软件，又称多媒体创作工具，用于组织编排多媒体数据、动画，制作高档特技效果，教育和娱乐节目编辑制作。多媒体数据准备软件用于多种媒体数据采集（含声音、图像以及它们的结合）和预处理，它是编辑软件的前步工作，两者紧密配合与结合以支持应用软件层次工作，多媒体操作系统是在计算机操作系统基础上增加部分针对多媒体数据特征进行多媒体任务的调度，保证音、视频同步以及信息处理实时性等多种基本操作管理。现在微软公司的 Windows 操作系统多兼容了多媒体操作管理，也包含了多媒体功能。驱动软件是直接和

硬件打交道的软件，它完成设备的初始化、打开、关闭和基于硬件的压缩、解压缩，有时随相关硬件一并提供。

2.3.4　信息系统发展的基本情况

一、人类对多媒体信息的感知和理解利用（有待研究的难题）尚处初级阶段

人类感知信息是通过眼、耳、鼻、舌等器官接收多种媒介所载荷的信息，并结合脑的思维认识事物的。总体而言，每个人都“自在”的具有如表 2.1 所列出的七种处理信息能力，但详细的机理却非常复杂，形成了人不认识自己的状态。例如，人的眼球作为一个透镜，所成像应是倒立的，经过视神经的作用，人感知的像却是正向的，其机理并非十分明了，至少绝大多数人本身并不了解，至于“综合动态信息”及“交互综合信息”的认识利用过程就更为复杂，现在所知甚少。在人自己尚不清楚的情况下将无法制造出这方面的高水平信息系统为人服务。因此人企图得到具有类人高级智能的多种媒体信息系统作为工具是人类的“渴望”，但现在却不可“及”，这类信息系统是比单种信息的处理系统更为复杂的信息处理系统。本小节中提出这样一个艰难问题，目的是说明信息科技发展征程是无止境的，人类尚需努力。

二、人对电磁（含光电）媒体利用的历史及发展讨论

对人感知信息而言，是通过感知器官和大脑，对上述七种信息进行感知和认识，这是基本的、不可改变的。人类总是不断通过信息变换和信息系统的帮助，在时间、空间域（广义）上扩大感知和认识信息的范围。为了人能“感知”，最后都变换为上述七类信息供人感知和认识，扩大感知范围的主要手段是利用电磁波为媒介，究其原因与德布洛依教授所提出的物质波粒二重性原理中电磁波是物质存在的基本属性有关。人类也利用声波及其他振动波、引力波（如微重力信息）、扭场等，在不久的将来，量子纠缠态也可能被利用作为表征运动状态。除此的外，以实物信息表征运动状态（如化石、岩芯、冰层、黄土层），还有生物信息也已经引起人类重视。总之，人类会不懈努力去扩大感知和认识信息的时空范围，在本小节中只集中讨论电磁波领域相关问题，见表 2.3。

表 2.3　电磁媒体的发展及用途

波长特征	超长波	广播波段	短波波段	超短波 波段	微波波段	毫米波 波段
主要发展 (20 世纪)	20 世纪 70 年代	20 世纪 20 年代	20 世纪 30 年代	20 世纪 40 年代	20 世纪 40 年代	20 世纪 70 年代 以后～21 世纪
现代用途	深水中通信	通信等	通信广播	通信雷达、遥感等		
波长特征	长波红外波段	短红外线	可见光	紫外线	X 光	γ 射线
主要发展	20 世纪 70 年代以后	20 世纪 60～70 年代	两个多世 纪以来不 断发展	20 世纪 80～90 年代	20 世纪 20～30 年代	20 世纪 80 年代
现代用途	夜视应用等	空间发展 利用等	有各种 新应用	特殊及军 用为主	进行物质 结构研究	宇宙研究、 核研究

人类在电磁领域的普遍应用及重要应用在频率尺度范围已达 10^{15} Hz(时间维尺寸范围约 10^{15} Hz),涉及物理、化学、生物的宏观效应(波)微观及介观效应(粒子、量子效应),总的方向和目标仍是沿着后述的极限目标发展,例如超短波＋微波＋毫米波的卫星通信,是在“任何人”、“任何地”、“任何时”方面改善发展。光通信是偏重“任何人＋任何事”导致的大容量信息快速传输问题,光存储的大容量也是为“任何事”所驱动,移动通信是偏重于任何状态的一种(移动状态)较方便、便宜的通信。现在正发展的 Internet 功能:借助计算机(尤其是小型计算机)以传递信息、利用信息(在处理和利用信息方面仍有瓶颈)。由此可见,人类在信息科技领域已取得(尤其是 20 世纪后半叶)伟大的成就,但对人脑思维规律的认知(宏观、微观方面)认识很初步,提高信息处理能力方面(涉及对任何主题的信息利用)是相对的瓶颈。我相信从 21 世纪开始,人们在生命科学、脑科学(认知思维机理)研究的基础上,将大力研究与人脑能更好协同工作的信息处理系统。

信息科技将伴随着人类进化而发展,如上述已达 10^{15} Hz 左右的尺度范围内应用。宏观上距离现在人类在自然界所掌握的运动尺度 10^{44}(时间维、空间维) 尚有很大的发展空间。就下限而言,它距基于“物质间存在着相互作用”原理(说明很复杂的非线性相互作用并在时间、空间展开)的相互作用能量的最小量化的阈值尚有差距。由以上讨论可得出,人类利用各种荷载信息的媒介,扩大获取信息的活动范围,将持续地动态发展。

三、永存的矛盾和正反向作用

信息科技、信息系统的发展是融入人类进步过程中的一种共同进化,人类社会的进化,是一个开放的复杂巨系统自组织进化体系,其中可再分为多个与开放的复杂巨系统相关联的进

化，如一个地区、一个国家民族的发展进步。一些信息科技问题和信息系统将以“特殊”形式参与具体的发展。本小节中只从总体概念上讨论信息系统的一些永远存在的矛盾和相应的正反向作用。

人类社会的进化的根源在于人类社会内部及与环境对立统一的矛盾运动。信息系统融入社会越紧密，则相互促进发展越明显，矛盾对立统一的斗争也越发激烈。矛盾运动是事物发展的根源，对于信息科技和信息领域而言，社会上各种矛盾在此必将有所反映并形成共同进化。具体的表征可归纳为一些对立统一范畴的具体矛盾，如绝对和相对、整体和局部、质和量、必然和偶然、连续和间断等。例如，现时在我国则更应注意信息领域质的发展（科学新发现，技术的自主创新体现趋近 2.3.5 节所述“极限目标”中作出的贡献）。在 2.3.5 节中，研究信息系统发展的极限目标能发现其中充满了对立统一范畴所描述的对立统一内容是形成“极限”和不断发展的根源。信息系统融入社会进行服务，社会中各种矛盾的融入大大地增加了信息安全问题的严重性和复杂性，在各种技术应用中其内含对立统一的矛盾也往往被激化而产生信息安全问题。例如，复杂的信息系统运行中，必然要预先设置测试的接口（因为系统运行不可能保证绝对正确不出故障），这个接口又可被攻击者用做实施攻击的入口。为公众服务的信息系统必定向公众开放，少数犯罪者便可利用“开放”进行犯罪活动（如利用电子商务盗窃金钱）等。对立的矛盾激化后便会产生对抗的运动方式，其作用效应明显呈相互的正反向特征，也正是正反向效应斗争促使了发展。例如，作战双方处于激烈对抗位置并采取对抗行动，这种情况反映至军事信息系统领域便形成了各国都非常重视的信息安全与对抗问题，虽尽力杜绝发生严重的信息安全事件，虽解决了很多问题，但新的信息安全问题发生的可能性并没有明显下降！本小节中提出了“信息系统永存的矛盾和正反向作用”这样一个基本命题，以后章节中将就信息安全与对抗问题展开讨论，其普遍性结论是：永远普遍存在的对立统一矛盾及正反向作用的斗争是信息科技、信息系统发展的根源。

2.3.5　信息系统发展的极限目标

信息系统发展的极限目标是：任何人在任何地点、任何时间、任何情况下都能安全、方便地获得信息与利用信息（越价廉越好）。值得注意的是，这是个永远不可能完成的极限，只能不断趋近。因为它本身内蕴涵了一些本征性不可消除的矛盾如“任何”等价于“绝对”范畴的实现，那是不可能达到的。信息系统内部存在对立统一的矛盾，正是这些矛盾促使信息系统不断发展，如相对与绝对、个体与整体、自由与约束、有限与无限等在信息系统内不断有所体现。在时间、空间中矛盾斗争不断展开，如功能不断扩大与服务的安全性能问题也同时增加可能性，科技进步同时提升了信息攻击与反攻击的水平，所以信息只有相对的而无绝对的安全。

2.4 信息科技与信息系统的发展是人类永恒的主题之一

2.4.1 理论上的论述

人类进化的最本质因素是“认识”与“实践”能力的不断提高，而认识和实践功能的实施和能力的提高都离不开“信息”作为媒介，包括人认识自己的发展过程也是这样。

基于认识和实践的主要进化方式是，新规律的发现、知识的积累应用、新工具的发明创造、工具的改进等。获得相应信息是以上进化方式的最根本前提，各类信息系统是人类最重要的一类工具。

2.4.2 信息科技与系统具有普适性的“增强剂”和“催化剂”作用

根据上小节所述“信息”是人类提高认识和实践能力这一基本因素，以及信息系统是人类重要的工具这两条基本规律，加上数字化电子科学技术和微电子科技的高度发展，使得很多类信息系统以小体积、轻重量、低电压、低能耗的小型化面貌出现，从而使得这些信息系统方便地与其他系统结合，或者以子系统身份嵌入其他系统起着增强剂的作用。这种以子系统身份嵌入其他系统起增强剂作用的方式，是信息科技和系统中的一种非常广泛、非常重要的工作模式，也是现代信息社会的重要特征之一。这种例子多不胜举，如，民航飞机中的导航系统、盲降系统都是典型的信息系统，它们嵌入民航客机内构成现代先进民航机，具有高度飞行安全和起降安全性能，高质量服务旅客，这大大促进了社会交通发展。高性能的机械加工中心，其中相关信息系统的嵌入是提高加工精度和效率主要措施之一。此外，对小汽车而言，性能越高则嵌入汽车电子信息系统功能越完善，现在这种趋势并无减缓趋势反而有所加强，以下加以较详细叙述。

信息系统广泛为人类服务，按用途划分可分为：

① 科研信息系统（含研究生命科学的各种先进前沿的信息系统）。

② 社会发展信息系统。气象信息系统、防灾信息系统；地震、森林火灾、洪水、流行病检测；医疗急救、环境保护检测、教育用信息系统等。

③ 国家政府安全管理信息系统。国防信息系统；侦察卫星、通讯卫星、雷达声纳；政府办公管理信息；缉私系统；税收、国家行政管理所用信息系统等。

④ 社会公共服务信息系统：通信、计算机网络、广播电视、有线电视系统（兼有国家组织的宣传教育传播功能）、公共信息库等。

⑤ 经济发展及企业营销信息系统。MIS、银行信息系统、股市期货信息系统、电子商务系

统、市场销售服务系统。

⑥ 家庭个人信息系统：消费娱乐、生活及安全信息系统

⑦ 嵌入信息分系统：将信息及控制信息系统作为分系统嵌入其他系统中，以大幅度提高和增强原系统的功能，如民航机的导航、自动驾驶、盲降着陆系统、汽车的燃油喷射控制系统、防撞系统、基于 GPS 道路状态及导航系统等。

还有，具有广泛含义的“其他系统”，包括了非常广泛复杂的社会系统都有信息系统嵌入。例如，文艺系统、经济系统、国防系统等是社会的重要组成部分，也都有信息系统嵌入其中。

其中，①－⑥类信息系统往往是利用共用信息基础设施平台，再在其上搭建专用软硬件设备来完成各种专用功能。

信息系统的服务功能正在发生互相融合，在结构组成上也正共用基础设施，从而形成相互融合的结构又有独立功能的系统。例如，移动通信系统长途业务要利用分布各地的电信网络基础设施，电子商务要利用计算机网络，而计算机网络又离不开电信网络。

总之，现代社会文明的进步发展与信息科技和各类信息系统的发展息息相关。信息科技、信息系统除自主形成产业外（含运行服务业）并广泛融入并带动其他产业发展，从而形成了与经济甚至文化领域发展的互动。

例如，汽车中包括如下的电子、光电子信息系统。

① 电磁兼容软件设计系统，形成电磁兼容性能。

② 车本体的信息及控制系统。如温度控制子系统、压力控制子系统、发动机转速控制系统、车速度加速度（含角度维）控制子系统、流量控制子系统；各种传感器约 30 余种（含光纤传感器）及总线系统等（若不用总线则信号线约 1 000 根）尚不包括辅助控制子系统，如自动锁门、后备箱、空调子系统等。

③ 使用安全系统。倒车雷达，防撞雷达（频率 75 GHz）、ABS 防抱死、安全气囊等。

④ 通信与导航系统（含与各网络的连接）。电子地图、道路状态及电子导航等。

⑤ 环保系统。排放控制子系统、噪声控制子系统。

⑥ 娱乐系统。音频及视频娱乐系统。

⑦ 软硬件支持系统。软件主要集中在信息获取、信息处理、信息利用和形成。控制作用硬件主要有专用 DSP、存储器、编程器件等专用芯片。

⑧ 各种专用器件。专用显示器、专用传感器等。

2.5　信息科技与信息系统发展的多种庞大支持体系

信息系统作为人类重要工具将持续不断地伴随人类的发展进化，它的发展从来都是依靠科学技术的支持，信息系统和信息科技除了互动式相互促进发展外，今日更需多层次庞大的学科群和社会的支持，除此外无法在实际中牵涉到的复杂性问题非线性问题等顶层难题的困扰

中前进。

2.5.1 学科支持体系

① 基础层次：自然哲学、自然语言理解分析学、语言语义学、数学、物理、化学、生物学（有关部分）等。

② 前沿交叉基础层次：信息科学理论、系统科学、控制科学、认知科学等。

③ 专业基础层次：电子学、光电子学、微电子学、计算机科学技术、信息及信号处理科学与技术、生物信息学等。

④ 专业学科层次：多种学科领域，如通信、遥感、微电子设计、电子工艺、光电子器件设计制造等。

2.5.2 各层次发展的社会支持与主要完成单位

① 基础层次：国家基础研究计划、国家专门基金支持下，主要由高校和基础科研机构承担。

② 应用基础层次：10～15 年中长期预先研究；5 年期预先研究，主要由国家相关计划及基金支持，大型企业对 5 年期预先研究支持为辅，主要承担单位同等基础层次。应用研究与发展，企业为主、国家支持为辅，企业研发机构为主承担。

③ 服务应用层次：企业支持、企业研发机构为主（市场应用与支持、保障支持等）。

2.6 几种典型信息系统举例及其要点说明

2.6.1 军用信息系统

信息科技与信息系统在国防军事领域中具有重要的作用和意义。溯源至 2 500 余年前战国时代（孙子兵法）谋攻篇中便指出，“知彼知已，百战不殆”，这是由军事理论、军事哲学领域从根源上说明了战争基本规律并蕴涵了“信息”要素。“知彼”要通过掌握“信息”来达到，只是古代和现代掌握信息的方法、手段和设备有所不同而已，现代信息科学技术支持军队的装备实现了信息化和信息化装备。装备信息化内含利用信息科技及信息分系统嵌入武器装备中以提高其性能，也包括以信息系统（信息化装备）和其他武器综合在一起构成功能更先进、结构更复杂的大型武器系统，也可称装备信息化。信息化装备则指以信息科技为主体所形成的军事信息系统能形成一定战斗力。例如，军用侦察卫星、电子战系统等。军队现代化重要标志之一，是

高度的装备信息化和众多的信息化装备，它们的实质在于获得敌情，然后有效采取措施予以及时有力的对抗和打击。

信息化战争中，信息化装备和装备信息化的程度越高，越应注意信息安全与对抗问题，战争本身就是激烈的对抗，因此“对抗”是战争的本质性质。信息化装备和大量嵌入信息科学技术的装备都必须考虑在对抗环境中发挥作用的问题。比发挥作用更严重的问题，是注意信息系统双刃剑效应中的负面效应，即对方利用各种我方装备中“信息”的特征，造成对我方损害的对抗行动，这是本书所研究讨论的一个主要议题，以后章节中予以讨论。

2.6.2　民用信息系统

1. 家庭用（个人用）信息系统

有娱乐用生活用信息设备向兼有办公性能的信息系统融合趋势。

① 电视终端：接入电视网络（广播与有线电视网）的电视机正由第一代模拟制式向数字式过程转化，其中以数字标准电视（清晰度在 800 行左右）将以比高度清晰制式（HDTV）更快的速度推广，同时以电视机作为终端设备的视频系统将进一步发展。如与新一代 DVD 配合形成“家庭影院”，与广播电视点播网络结合构成个性需求更明朗的视频系统等。

② 计算机与计算机网络（包括其改进型）：形成多种服务（包括生活服务、商务服务、信息服务）的进一步发展，电信网、计算机网络、广播电视网各具别的网络所不具备的优点。基础设施方面，电信网与计算机网络有所共用，但应用服务方面仍分隔明显，如何共用资源开辟更多种服务和提高服务质量仍是一个艰巨任务。

③ 电话与个人移动电话。移动电话业务上升很快，中国移动用户量已占世界第一，主要业务是语言通信，其他为辅，过宽的宽带需求不太旺盛，3G 移动电话主要用途为众多用户保证高服务质量的通话，手机小型美观兼有装饰物功能（尤其年轻女士也会起一定刺激消费的作用）。固定电话用户数随着服务种类的增加仍有增长，但增幅速率会降低。

④ 家用智能综合服务系统，有进一步发展的趋势。用无线微型网络将各家用电子设备连成一个智能型综合服务系统，将是高档住宅内配置的发展方向之一。无线微型网可能是符合 IEEE80211BWLAN 的某种系统，可能是“蓝牙”，也可能是其他系统，现在正在发展中。

中国人口及家庭众多，上述家庭个人用信息系统有广大的潜在市场，同时会形成产量很大的产业，对我国经济发展有重要意义，值得重视。同时，也应看到存在一些问题和发展机遇：

· 最理想状态是三网融合，光纤到建筑物发挥更宽带宽的效果，但短期不太可能普遍实现。

· 中国住宅集中，尤其是新的住宅小区，住户条件较好，可能配置较先进信息系统，另一方面又因用户集中，便于实施宽带到小区或公寓建筑楼相应成本可较大下降。

· 有些线路施工质量控制不严，质量不高，如反射驻波强，接触电阻大，交调串音比较严

重，对较高速率信息业务影响质量，要部分返工，工本花费会有所增加。

· 信息设备的使用尚需进一步降低成本（安装及运行费用），匹配社会发展推广使用。

2. 计算机领域高端核心安全产品系列

自主研发具有知识产权，高可靠性高端安全产品系列，形成产业以确保关键信息设备及构成网络的安全应用（包括安全软件及硬件芯片等）。

3. 发展专用信息设备的关键部件及相应应用软件，可形成各有关应用软件产业和相关的信息产业。

4. 发展三代移动通信有自主知识产权的关键芯片及系统

随着移动通信应用的发展，改进服务功能形成第三代移动通信系统是发展的必然结果。科学地克服困难而发展是一个复杂的系统复杂的系统问题，其中并不单纯是科学技术问题还包括经济商业等交织的复杂问题。

5. 各种其他用途（除计算机外）微电子芯片（含 SOC 等）及各种专用嵌入式系统

如交通卡，各种电器用芯片，汽车电子信息产品等。随着我国进入 WTO，外国企业、大学进入我国经济界各领域，一方面在国内面临外企进入，另外在国际市场出口都有强手的激烈竞争，提高质量，降低成本，改进服务，改善管理都离不开各种信息系统，仅就满足中国企业就有较大需求发展空间。

2.6.3 信息领域高科技企业的一些基本问题讨论

① 信息高科技领域发展奇快，效益不菲，很吸引人。发展奇快说明了一方面近期有需求，仍有很大发展空间；另一方面意味着尚不成熟，处在不稳定阶段，使用性能、规范、标准都存在不确定或快速变化的情况，用户的需求和数量也有随机不稳定性，归结为“市场风险大”的不利因素，从事这方面的企业应有雄厚综合实力，正确选择市场切入点才能立于不败之地。

② 高效益吸引了投资、生产制造、经营、服务等各方面大量参与，一方面形成了强烈的竞争，另外一方面也很容易形成如市场上“供”远大于需，最终导致缩减调整，在经济体系中信息产业过量的发展与增长，会形成泡沫成分，造成各经济成分的比例失调，时间长，便会发生“消肿”“消泡沫”现象，影响经济的正常发展。

③ 对于基础性设施，应提前于现实状态较大程度留有发展余地，如电力、交通、通信骨干设施等。而应用性、消费类产品，却不能超前现实需求太多，尤其消费对象为广大群众时，则应充分考虑其消费需求和消费水平，决不能单由技术先进程度作考虑出发点。例如“铱星”移动通信系统，技术非常先进，但使用者“使用不起”，导致最快最惨的失败。

④ 不要轻信市场宣传者、本领域专家、广告等的片面、极端、过激的宣传，即使是一些著名企业和著名人士的大肆宣传，也不要迷信跟风。绝对化的说法不合实际，要进行科学分析，这种例子太多了。如七八年前，过分宣传很快实现“信息高速公路与多媒体应用 B－ISDN 将取

代一切”，但如今，美国的电话网业务还在一定速度发展（XDSL 等并非 B－ISDN），有线电视网也在发展，规划中的多媒体宽带网虽有发展，但有众多问题有待解决。距离取代电话网，有线电视网还有相当长的历程，关键在于美国老百姓对每户经常保持几兆至几十兆宽带的应用尚无强烈需求。过去宣传 ATM 将取代其他交换体制，3G 移动通信用户的宽带多媒体业务迫在眉睫，基于高速互联网的通信也并非像宣传的那样变为通信业务唯一主流，至于在 2000 年传言 2001 年夏天“蓝牙”技术将席卷全球的事更远非如此，这类例子实在太多了。各种信息系统的确会发展，但它的发展并不能单纯由技术某方面优点或先进性所决定，更主要的是融入人类社会共同发展。

2.7　本章小结

本章主要讨论信息、信息科技、信息系统的基本概念及相关内容，包括：信息的定义、内涵与发展历程。信息系统的特征、功能组成、极限目标以及所需的强大的庞大发展支持体系。最后给出了几种典型信息系统的举例并阐述了高科技企业发展中一些基本问题。

习　　题

1. 信息的定义如何？其内涵是什么？
2. 信息的特征是什么？人类利用信息的发展历程如何？
3. 什么是信息科学？什么是信息技术？
4. 信息系统的基本特征是什么？人类追求的信息系统发展的极限目标是什么？
5. 信息系统发展的支持体系是什么？
6. 为什么说信息科技及信息系统的发展是人类社会永恒的主题之一？
7. 信息系统的普遍作用是什么？
8. 试举例说明某一信息系统的信息采集、传输、处理、交换、存储、控制、管理的过程、作用及其发展过程和支持体系。
9. 试分析和举例说明信息系统的嵌入式特性及其作用？

第 3 章　信息安全与对抗系统概述

3.1　引　　言

由前章内容与社会的现实状态人们普遍承认：信息和众多种类信息系统的运转利用是现时国家社会生存发展不可缺少的因素之一，信息科技与信息系统促进了社会发展，同时社会发展也带动信息领域的发展。社会越现代化，信息科技与信息系统发展利用越充分。我们还应进一步分析理解，信息领域以多种多样的形式深深地融入社会，特别是它的嵌入特性使信息科技和信息系统嵌入社会各部分：信息科技嵌入别的学科领域、融入人们的思维中由“信息”角度思考问题已成为人的一种思维模式，信息系统嵌入其他系统形成更复杂更先进的系统。“信息”融入社会中起“增强剂”作用，社会的发展就是社会的矛盾运动。当信息和信息系统密不可分地融入社会中，社会矛盾结合信息领域内原来的矛盾就会形成新的矛盾运动，这种矛盾运动是复杂矛盾（也可说是矛盾的集合）。多种多样的矛盾，它运动着并与社会共同进步，信息安全问题是其中一种，它本身是一种复杂矛盾，矛盾具有多层次、多剖面交织特性（即可分为多层次、多剖面的多种矛盾又互相关联）；同时又是动态发展变化的，并随不同场合演化为具有不同性质和形式的矛盾，具有复杂时空交织特征。信息安全问题客观上是一个复杂动态运动的矛盾体系，由此很容易得出以下之结论：信息安全问题是社会、信息科技和信息系统在发展中的一个矛盾侧面，它没有“终结”，只有随“发展”而发展，在发展中解决存在的问题，又会发生新的问题（矛盾），再在发展中解决。“信息安全”的发展体现了社会的一种进步，反过来社会进步又会提出很多新问题促使信息科技的进步和信息的安全程度增加，如此互相促进，互相“对立”地不断进行发展。用矛盾、发展的观点看待信息安全问题是我们的基本观点，本章按上述基本观点对信息安全及对抗进行系统概述，共分四节。其中，第二节是“问题”的基本描述，包括信息安全概述（“安全”含义下全部问题）及信息对抗问题的概述（即信息安全问题在对抗剖面（侧面）进行概括讨论）。第三节为信息安全与对抗问题产生的根源（既有安全含义下的根源，也包括产生“对抗”的根源），进行一定程度的溯源性分析以体现问题的复杂矛盾体系。第四节着重于信息安全对抗问题的要点概述，对抗的概要过程，对立双方各阶段行动要点，由发展中增强信息安全之各种措施，第五节专门叙述法律对维护信息安全、防范及惩罚信息犯罪的有关内容。因为“信息安全与对抗”是一个非常广泛复杂之学科领域，在此只能就相关问题进行简单讨论。由于本章所涉及内容非常广泛复杂，不可避免地涉及“法律”，从系统性角度考虑应该包括法律内容，但因本书的主要定位原因，在此只进行框架性概要讨论。

3.2　信息及信息系统安全与对抗问题的基本描述

3.2.1 信息的安全问题

“安全”，是损伤、损害的反义词，“信息”是运动状态的表征与描述，“信息安全”的含义是指“信息”的损伤性变化（即意味着运动状态“表征”的篡改、删除、以假代真等，形成上述结果的方法多种多样，也与多种因素有关），是一件复杂的事。就“信息”的篡改、删除、以假代真而言，也往往与信息表达形式相关。如有关信息内容的重要数字部分用阿拉伯数 10 进制表示，则小数点位置变动影响很大，篡改内容对小数点进行移动可造成重要影响，用中文数字表示数就没有上述问题，但不方便。又如信息作品中加上数字水印，或利用散列函数形成内容摘要都可对内容形成审核等。说明讨论信息或信息作品的安全问题将关联很多内容，很多学科分支，是一个开放性复杂问题。本章并不深入研究“信息”表征及信息作品内容的安全问题，以及相关的详细的科技原理和方法，只侧重于信息安全的基本概念及对抗过程要点的总体性问题进行讨论研究。

3.2.2　信息安全问题的特性归纳

信息安全的特性保持（不被破坏），与信息系统的性能品质、安全水平有密切关系。信息系统的信息安全特性如下：

① 信息的保密性（Confidentiality），即保证信息不能被非授权用户所获得。

② 信息的可获得性（Availability），即保证正当用户及时获得在授权范围内的正当信息。

③ 信息的完整性（Integrity），即保证信息不被非正当篡改、删除及被伪造。

④ 信息的可用性（Usage），指信息的运行利用按规则有序进行，在可用性中还包括一些子性能，都可归纳入可用性范围内，如认证、公证、验证、不可否认性、信任等，它们都是发生在具体场合需要几种子性能交叉集合实现，以确保信息和信息系统的运行安全有序。这种例子很多，举一个例子加以说明：在保密信息交换中必然采用密文通信，需要密钥管理中心进行管理，它不能随意由任何人设立，必须由本身具有公证性的权威机构对密钥管理中心进行授权认证，用户向密钥管理中心申请密码，通过用户身份验证后才得以使用密码，两用户间进行密文通信，互相还应经过身份验证等，这些都是经一定的规范程序实现“可用性”问题。又如数学签名的可用性应体现“不可否认性”。总之，很多可用性的子性能都是在可用性概念下，在实际应用中互相交织使用，以构成一个安全的应用系统。

3.2.3 信息系统的安全问题

信息系统是以“信息”作为系统核心因素运行并形成为人类服务的一类重要工具，“信息”脱离了信息系统就形不成现代化服务功能，信息系统缺少“信息”则系统无从运行也起不到服务人类的作用，“信息”与其运行相关的信息系统是紧密相关互相不可分割的，这种特性体现在信息安全问题上同样紧密关联。与信息系统相关联的信息安全问题主要有三种类型：

第一种类型，“信息”与信息作品内容被篡改、删除、以假代真，虽直接体现在“信息”或信息作品上，但发生过程却体现在信息系统的运行上，离不开作为运行平台的信息系统，这正体现了“信息”与信息系统在信息安全问题上相互关联不可分割。

第二种类型，信息系统发生信息安全问题则意味着系统的有关运行秩序被破坏（在对抗情况下主要是人有意识所为），造成正常功能被破坏而严重影响应用，体现在某时某刻发生对某“信息”的破坏；此外，还会发生其他如“信息”传输不到正确目的地；传输延时过长影响应用。同样，不正常信息的泄露也会严重影响应用。还有一点应该指出，即信息系统发生安全问题（如不及时采取措施纠正）意味着是一类型性问题，如信息延时太长，则所有传输的信息都延时很长；上小节所述的“信息”安全问题，是侧重于具体某“信息”或信息作品被攻击破坏的单件安全问题。

信息系统产生安全问题的具体原因有多种多样，总体上认为信息系统及其应用的发展必含矛盾运动，安全对抗问题是众多矛盾对立的一类表现形式。细分矛盾源种类还有多种，如科学技术对信息系统功能的支持尚不完备，某一种技术措施有其正面效应，同时也可能产生负面效应。例如信息系统虽具有自组织机理，但仍离不开管理人员进行必要的管理，因此设置管理人员对系统进行管理的入口，同样可以被攻击者利用作为攻击信息系统的入口，由于对复杂软件的正确性检验及数学上的 NP 问题而无完备地进行，只得在软件中留有对一旦发现错误进行纠正（打补丁）的接口，这个接口同样可被利用作为对信息系统实行攻击的入口。在 3.3 节将讨论产生信息安全问题各种根源，以及产生安全问题的各种矛盾机理。

第三种类型，安全问题是攻击者直接对信息系统进行软、硬破坏，其使用方法可以不直接属于信息领域，而是其他领域的方法。例如利用反辐射导弹对雷达进行摧毁，通过破坏线缆对通信系统进行破坏，利用核爆炸形成多种破坏信息系统的机理，化学能转换为强电磁能用以破坏各种信息系统等。

3.2.4 信息攻击与对抗

信息安全问题的发生原因，很多与人有关，按人的主观意图分为：过失性，这与人总会有疏漏犯错误有关；另一类是人因某种意图、有计划地采取各种行动，破坏一些信息和信息系统

的运行秩序(以达到某种破坏目的),这种事件称为信息攻击。受到攻击方当然不会束手待毙,总会采取各种措施反抗信息攻击,包括预防、应急措施,力图使攻击难以奏效,减小己方损失,以至惩处攻击方、反攻对方等,这种双方对立行动事件称为信息对抗。信息对抗是一组对立矛盾运动的发展过程,起因复杂。过程是动态、多阶段、多种原理方法措施介入的对立统一的矛盾运动。在信息系统应用一方而言它不是件好事,但从理性意义上应该理解为,它是不可避免的事件。它是一种矛盾运动,在人类社会发展过程中不可能没有矛盾。再由辩证角度观察一件坏事有促进发展的重要作用,应该以"发展是硬道理"理念积极对待不可避免的事。信息对抗过程非常复杂,在此用一个时空六元关系组概括表示:

$$\text{对抗过程} \longleftrightarrow R^n[G,P,O,E,M,t]$$

其中 n 表示对抗回合数,P 为参数域(提示双方对抗的重要参数),G 为目的域,O 为对象域,E 为约束域,M 为方法域,t 为时间,R^n 为表示六元间复杂的相互关系,"关系"是运算和映射组合的另一种直观称呼,关系中还包括了诸元的相互变化率:$\frac{\partial O}{\partial P}$,$\frac{\partial^2 O}{\partial P^2}$,$\frac{\partial^3 M}{\partial t \partial O \partial E}$等表示连续多重变化,不连续变化常用、序列、差分方程等表示。详细、全面地定量描述一个复杂对抗过程非常困难,虽然在自然科学和数学中人们已发现很多重要关系,在泛函分析中,集合间或元素间的广义距离关系构成距离空间,大小量度关系构成赋范空间,集合间某些运算关系(具备某些约束)构成内积空间,内积关系可能同时满足赋范和距离关系等。代数中有同构同态关系,物理中一系列重要关系等。但就对抗领域的六元相互复杂关系而言,由于其广泛性和复杂性的"关系",还难于直接用上(包括具体化条件不确定,时变因素等),主要还是靠发挥人的智慧随机应变,定性与定量相结合,决定 $R^n[G,P,O,E,M,t]$。

3.3　信息安全问题产生的根源

信息安全问题的产生根源是一个复杂综合性问题,以下就一些主要根源分别进行分析。根据哲学定律,事物内及关联中必然有各种矛盾普遍存在(对立统一的差异对立、对抗等),并在各种矛盾抽象为一种对立统一的范畴来表征具体的矛盾,在信息领域的安全问题上同样遵守此定律,存在着众多安全剖面的矛盾,是产生安全问题的根源。

人们对信息系统的发展设定为人类服务功能越全面、越方便越好,如何在任何时间、任何地点方便地获得和利用信息,这隐含了要更多地"自由",更多的"普遍性",更多"普遍性的自由"。"自由"与"约束"、"普遍"与"特殊"是对立统一的范畴,信息安全是在普遍性的自由的整体要求下实现具体"约束"和"特殊性",这样肯定会出现矛盾,发生"安全问题",这是一种矛盾体现。

又如高性能的芯片多要工作在高工作频率上,但高工作频率在相对短尺寸上的辐射效应不能忽略,对于信息隐藏而言这是一对矛盾,是由物理规律所决定的性能与信息隐藏之间的矛

盾(也是“发展”所引起的矛盾)。

3.3.1 信息安全问题根源在于矛盾运动

辩证哲学认为,对立统一规律认定事物的存在是体现在不停的运动之中,运动发展即是矛盾的对立统一的运动,没有矛盾就没有发展。如计算机网络,应用的主体是大量的个人计算机,对于个人计算机的发挥应用功能,互联网是一个很大的发展。但个人计算机设计和发展的前期却是完全个人应用,并没有考虑网上工作所应具备的安全控制功能,加上在互联网络应用初期应用人数远不如现在多,安全问题也远不如现在这样严重,故其传输层协议中安全因素考虑不足,如 IPV4 协议就是这种情况,再如电子商务中的安全问题随着其应用发展日益占据重要地位,反映在信息系统中矛盾日益突出,要求保证安全的防范措施必须快速发展。由哲学总体上讨论,发展的矛盾是永远存在的,否则便没有“发展”了,信息安全对抗问题的产生和日趋重要是信息系统日益融入社会促进社会发展中所产生的一种必然矛盾,对此应有理性认识和积极态度来对待。人们努力做的仅是按发展规律预测未来,尽力做些支持发展的事情,力争使发展较为顺利。

后三小节叙述引发信息安全问题的几类具体矛盾,在具体领域内讨论矛盾运动产生信息安全问题的根源。

3.3.2 国家间利益斗争反映在信息安全领域

诞生在中国古代战国时代的孙子兵法,早在二千多年前便精辟指出“知彼知已,百战不殆”,“知彼”是第一位的,靠什么“知彼”,依靠获得的各种信息进行综合分析是关键因素。现代信息科技,以及多种国防信息系统,在现代战争中起着重要作用,各国都非常重视,甚至提升至尽力争夺“制信息权”的高度上。战争领域“对抗”是个本征属性(矛盾斗争的激烈形式),“对抗”在作为战争服务的信息系统中必然有强烈反映,这是国防信息系统安全问题产生的根源表现在以信息攻击、反信息攻击、反反信息攻击……对立的对抗过程,它永无完结地持续着,这是国防信息安全领域生存发展的规律。

3.3.3 科技发展不完备形式的信息安全问题

人对科学技术的掌握是一个持续的过程,世界不断运动变化,人类不断认识,这个过程不会完结。总体而言,人类的认识永远落后于客观运动的存在。现实情况是,对于科学规律而言,人只掌握了其中较少部分,对复杂非线性问题、非平稳性问题、生命问题、认知思维问题等所知很少。但是,信息领域很大一部分较深入的科学问题都涉及上述领域,可是由于人类尚未

掌握这些问题的科学规律，所以技术上必然有被动无奈之处。例如，大型软件的正确性问题就无法验证，因为在数学上尚未解决验证方法问题，会存在很多错误和缺陷，大型软件的安全缺陷俗称“漏洞(Bug)”。同样，复杂网络可抽象为复杂的拓扑结构。拓扑学中很多问题尚未解决，也就谈不上网络在非常情况下(如遭攻击发生故障)损失最小的优化结构，不同于生物有免疫能力和自我恢复能力，无生命的信息系统全靠事先将各种意外情况充分估计，设定状态以应对特殊情况。种种信息系统中，包含了很多人类尚不完全认识的规律。外加事先不可能充分估计情况和设定应对状态，这就是发生各种信息安全问题的一种根源。

3.3.4　社会中多种矛盾反映至信息系统产生安全问题

人类进化形成过程持续了数百万年，而有历史记载的只有五千余年，虽然近一百多年尤其是近半个世纪科技迅速发展推动了社会发展(尤其物质文明方面)。但就人类社会总体情况而言存在不少问题，距离较理想状态差距仍很大。如欠发达国家中很多人处在饥饿状态，很多儿童营养不良，更谈不上享有良好教育；一些发达国家依仗自己经济、科技优势，在国际交往中处于不平等优势地位；超级大国总在千方百计实施霸权主义，把自己的意识形态强加于别人，实质上是力图控制、驾驭别国，甚至不顾其他人的生存发展权。这种国家间、社会中不合理的客观存在，扭曲正常人性，激起各种反抗，包括信息对抗，而“反抗”中也有过激伤及无辜的情况，信息安全对抗问题严重者构成犯罪。人们知道社会犯罪是一种社会现象，社会中总有少数犯罪分子要伺机犯罪以达到其个人不法目的。当信息科技广泛嵌入社会服务社会里，其反面效应体现在高科技信息犯罪具有的隐蔽性、快捷高效性等，吸引犯罪分子利用信息对抗手段进行犯罪，呈增加趋势，犯罪原因有多种，其中有部分原因“社会”应承担道义上的责任(甚至诱因责任)，如一些青少年成长处于种种逆境，社会关心帮助不够多，养成孤僻或强烈逆反报复心理。有的青少年“平权”思想浓厚，反对知识产权带给个人创造巨大财富(如软件专利等)，对此认为不公平，要讨回公道。有的人对他人拥有大量财富心理失衡，而在信息网络中攻击掠取既方便又隐藏，又可达到心理平衡。有的法盲还错误认为没有实地动手抢劫不算犯罪，也助长种种信息犯罪行为。总之，很多社会原因及犯罪原因在信息科技、信息系统密切融入社会情况下，必然会在信息领域有所反映，形成各种信息安全及信息犯罪问题。

3.3.5　人在工作时各种失误造成的信息安全问题

人虽然是万物之灵，但在高度紧张的长期工作中，会因种种原因不可避免地发生疏漏、错误，其中部分会形成信息安全问题和在对抗环境中造成损失。

3.4 信息安全对抗中对立双方对抗要点

3.4.1 按主要阶段步骤列出的简要过程

单就对抗行动而言，攻击方占主动。因为总是他们主动发起攻击，可在任何时间，对任何信息系统采用各种方法进行攻击，当攻击者仅进行思考如何进行“信息”攻击和破坏，而没有采取攻击行动前很隐蔽也不违法，甚至还受法律保护；也不得随意对其动用法律，这就使得广大信息系统使用者、系统运行者处在被动状态，充其量只能思考如何防范，找自己的弱点和漏洞，有“经验”者总结过去教训，以此防止更大损失发生等。综合实际情况构成双方简要对抗过程，如图 3.1 所示。

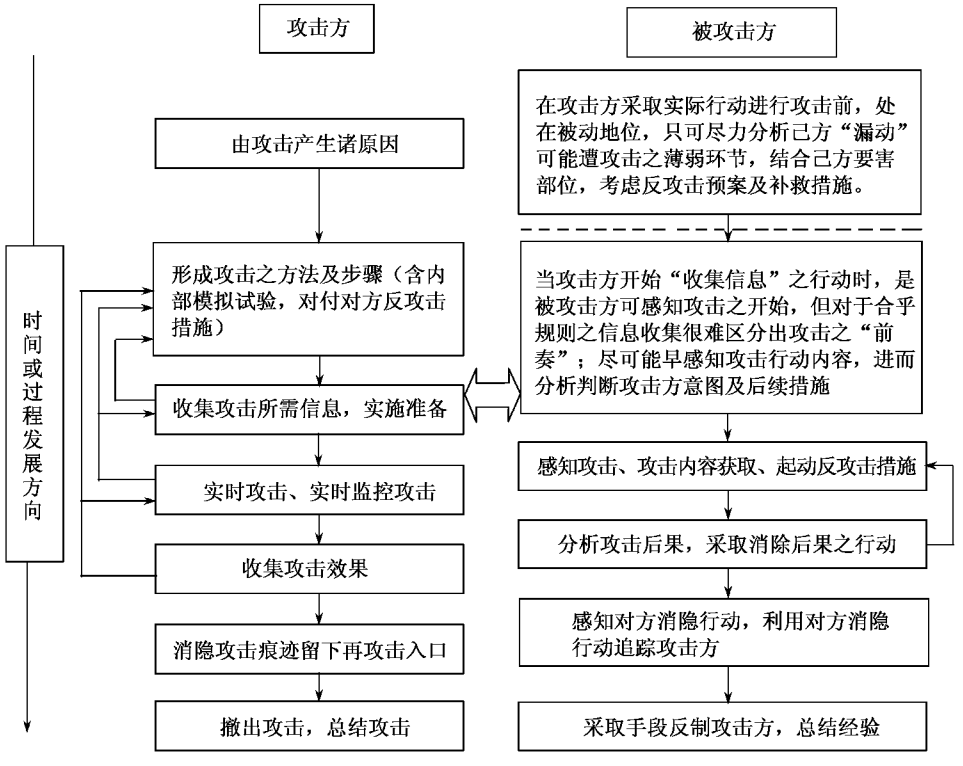


图 3.1 攻击与对抗过程简图

3.4.2　对抗过程要点注释

上小节已列出对抗过程简要步骤及双方行动关键，本小节进一步注释要点，并阐明以下四点：第一，信息攻击和防范是一个激烈复杂的过程。第二，攻击与被攻击对抗序曲为争夺制攻击信息权，即在获得对抗所需信息的斗争中占主动地位，它也是一个激烈复杂的过程融入对抗全过程。第三，攻击方实现攻击目的的主攻击阶段是对立双方斗争主阶段，尖锐复杂的对立斗争情况往往是前一阶段斗争的结束，又是后续斗争的序幕，形成连续—间断—连续的对抗过程。信息安全与对抗领域有其基本规律和方法，将在第四、第五章详细分析基础性原理及对抗的原理性方法，第四，信息安全问题是一个复杂严肃的问题，如不持续重视及动态发展将对国家、社会的发展产生重大影响，故一方面积极研究综合性、系统性防范措施，另一方面应建立促进信息安全科学技术“发展”观点。

一、信息攻击与防范是一个复杂过程

上小节说明在信息对抗过程中，攻击方在总体上处于主动地位，具有时间、方式、地点、环节及对象等方面的主动选择权，而防范方只能限于防范领域，尽可能延伸至预先防范。现实发展情况，是多数信息系统具有一定的信息攻击防范功能，可以说是设防系统。欲达攻击目的必定是个复杂的对抗过程，绝非简单行动。一个复杂过程可分为多个阶段，每个阶段还包括子阶段，子阶段中又具有多个对立步骤（如上节所述）。各步骤阶段也不一定依次进行，往往多次反馈重复，双方采取多种对抗措施，“过程”具有随机性、后效性，绝非简单的马尔可夫随机过程所能描述。这种复杂的后效（随机）过程，数学上尚缺乏有效定量系统性分析、综合方法，一般只能定性或部分近似定量分析。信息安全与对抗的发展呼唤科学的支持（尤其是复杂性科学、系统科学、数学、物理等前沿性和基础性科学的支持），科学基础性支持以及信息安全与对抗领域的科技发展及体系建设归根结底落在人才发展上。

二、信息对抗过程的序曲是双方以“对抗信息”为核心的对抗

根据“信息”定义，在信息安全与对抗领域双方对抗斗争的机理，我们提出“对抗信息”这样一个新概念用于研究对抗问题，并在第四章提出相关原理及解释，本小节结合攻击与对抗过程图简要说明。

对抗信息是指信息安全与对抗领域，人们实现“对抗目的”所采取对抗行动时必定相应伴随产生相应“信息”，我们称这种“信息”为对抗信息。根据“信息”定义，将对抗行动看做一种具体“运动”，它自然会产生“信息”。它是“对抗行动”所产生的“信息”，有“对抗”性质，故称“对抗信息”。“对抗信息”对于对抗双方都非常重要，双方展开了一系列持续的“对抗”，这些内容将在第四章第五节详细论述，在本小节只提出一个值得进一步注意的问题，即信息系统运行时，

有众多“信息”在运行流通(信息系统特征以“信息”为运行媒介)。如何判断“对抗信息”?这个问题的答案是依照系统运行的“道”来判断,只有违反运行的“道”的对抗信息才有可能被感知。这里引出“反其道”的重要概念,说明围绕对抗信息斗争的复杂性。不违反“道”的“对抗信息”,即使存在也难于被感知,这样又增加了一个“共道”(遵守规则机理)和“逆道”(违反规则机理)的因素,“共道”、“逆道”机理伴随“在共道基础反其道而行之相反相成”的原理而形成,它是另一条重要核心原理,在以后章节将详细结合“对抗信息”及有关原理讨论“信息安全与对抗”领域的规律,争取斗争的主动态势,在此只是“序曲”。

三、信息安全对抗过程中围绕实现攻击目的及挫败攻击是对抗主要阶段(成败关键)

在对抗阶段中双方将竭力采取各种方法、手段、措施达到己方目的,第四章、第五章中详细讨论对抗领域基本原理及基本方法,此阶段对抗“过程”概念体现在:一个过程是以多个子过程所构成,一个子过程结束,又是一个子过程的开始。当一个子阶段结束时,攻击方无论“成败”与否,要消除痕迹,脱身避免报复。防范方要弥补损失、追踪攻击源,开始进行报复(在新一轮对抗过程前双方总结分析,为后续新一轮信息安全对抗过程作准备,可认为是新对抗过程的开始。)“信息安全对抗”实际上是一个既连续又间断的持续过程。

在 3.4.1 小节所列框图 3.1 主要以“事件”为主线所构成,现再构成一个包括对抗双方介入的主要相互对抗的环节框图,以表达人介入的主导作用:对抗中人的“行动”主要依据的规律为“关系映射反演法”,其表示如图 3.2 所示。

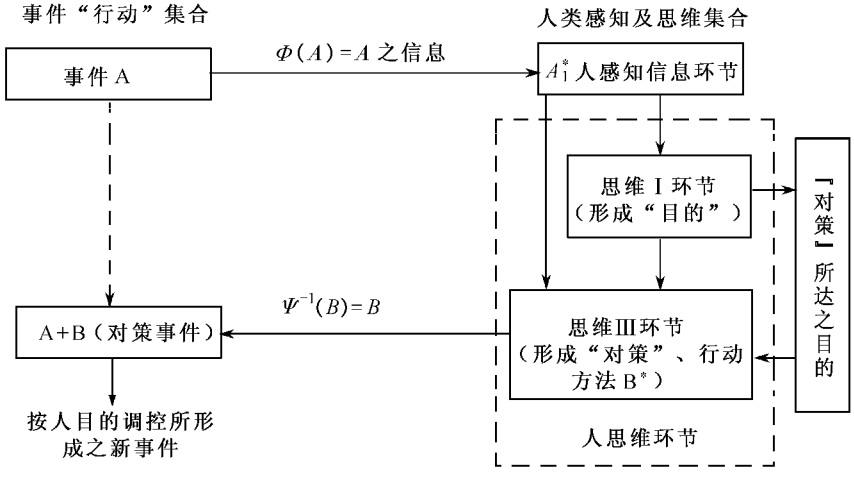


图 3.2 各方形成“对抗”的关系映射反演法示意图

框图表示人达到调控事件 A 的过程,首先事件 A 映射至“人”,“人”感知“信息(A^* 为人所感知的信息)”后经过思维对 A 进行认识,然后思考针对事件 A 的调控形成“对策目的”(欲达

“目的”），再根据事件 A 状态及“对策目的”形成对策行动方法 B，经 $\Psi^{-1}(B)$ 形成实际行动反映射至事件集合以形成新事件（体现调控目的），主要在人思维中形成行动方法（而不在事件集合）故称“关系映射反演法”。

将上述人的感知信息思维对策、形成对策方法诸环节浓缩为“人环节”，形成对抗过程，如图 3.3 所示。

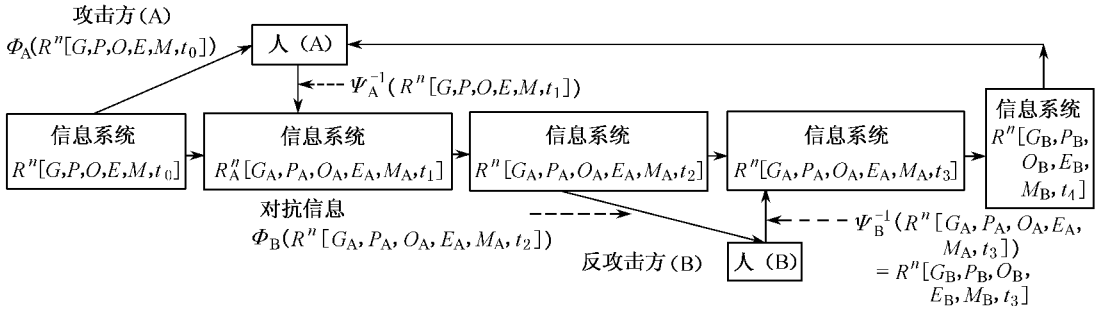


图 3.3　对抗中人介入形式的“人环节”示意图（假定）Ψ_A^{-1} 作用系统产生 $R^n[G_A,P_A,O_A,E_A,M_A,t]$

框图重点表示双方对抗第一回合。信息系统状态用 $R^n[G,P,O,E,M,t]$ 表示；攻击方形成的作用改变了信息系统状态，在 $R^n[G,P,O,E,M,t]$ 中以下标 A 表示，即 $R^n[G_A,P_A,O_A,E_A,M_A,t]$；而反攻击方 B 方的作用在 $R^n[G,P,O,E,M,t]$ 中，以下标 B 表示。发生事件的时间用 t_0,t_1,t_2 等表示。

四、“信息安全对抗”是一个严肃、不容忽视的问题，应积极进行对信息攻击的防范工作，同时应将防范融入发展中，是标本兼治的基本策略

信息科技与形形色色信息系统的嵌入式特性（嵌入社会，嵌入其他系统），起“增强剂”及“催化剂”作用，推动社会发展，这是非常重要的正面作用，但万一发生信息安全问题，则会起很大负面作用，影响社会发展、国家安全、人民正常生活。因此全社会树立信息安全概念，努力防范信息安全问题的发生是最基本观点，应进一步将信息安全问题融入“可持续发展体系（包括科学技术发展体制建设及基础设施、人才培养等）”是更深层次的重要概念。下面将举出一个第二次世界大战实例，以此说明上述观点。

1941 年底，日本联合舰队司令官山本五十六大将策划珍珠港偷袭事件，重创美国太平洋舰队，使美国太平洋舰队损失了几乎全部战舰及大部分陆基空军，造成日海军的相对强大，居于主动地位。美国为了振兴军心及民心并报复日本，杜立德中校组织利用 B－25 中型轰炸机轻载燃油，由航空母舰起飞轰炸东京等日本大城市，造成日本心理上重大恐慌与压力（飞机降落在中国沿海地区）。日方急于扩大其太平洋防御范围，以防美军再次轰炸东京。山本五十六因此制定了“米”字计划，即攻击中途岛美海、空军前沿基地，消除前沿“钉子”，同时可引出美太平洋舰队残部迫使其与日方占绝对优势的联合舰队决战并将其消灭。这是一个“一箭双雕”的凶狠计划，当时实力对比大致如表 3.1 所示。

表 3.1　日美战时实力对比

	日联合舰队	美太平洋舰队
战列舰	17 艘	无
航空母舰	8 艘	3 艘
巡洋舰	33 艘	8 艘
驱逐舰	65 艘	14 艘
潜水艇	21 艘	35 艘
舰载机	700 余架	200 余架，且战斗机性能逊于日本零式战斗机

日方山本五十六大将虽首创海空军为主攻击的海军先进作战模式，而美方太平洋舰队司令官尼米兹上将曾在情报机构工作过，深知“信息”的重要性，信息优势往往可当“雄兵百万”。他责令太平洋舰队情报机构日夜截收日军无线电信号并加以侦破从而获得信息，由侦破信息得知日军将有大规模行动，尼米兹上将估计中途岛为一可能目标，但电讯中采用了对地址幂次加密，即密码再加密，代号为 AF，无法破译。尼米兹便采取攻击试探方法，用美方较低密级的密码发报，故意声称中途岛淡水设备损坏亟待修复，日军截获美方电讯后上报日司令部，电讯中出现 AF 淡水设备损坏亟待修复的内容。美方由此确定日军攻击地点为中途岛，并倾太平洋舰队全部剩余力量，事先有计划、有准备地迎击日本舰队，重创日军，炸沉多艘主力航母及大部分舰载机，使得山本五十六大将首次吃败仗，时间为 1942 年 6 月。美军得胜后在相当长的时间内并未继续利用所破译日军密码扩大战果，以隐藏真实情况，日军也没有认真研究战役前后的一切情况，也没分析出是由于信息泄露造成战败，山本五十六本人丝毫没有“怀疑”信息泄露，1943 年 4 月山本五十六不听部下以信息可能泄露而危险的劝阻执意去前方视察。美方利用破获日军密码得知山本的行动计划，在空中派遣战斗机伏击，当山本座机缓慢降落、护航战斗机返航的时机由高空俯冲，一举击落山本座机，震动全日本。

该事件充分说明了信息安全的重要性，也说明“观念”的重要性，以及信息科技发展的重要性（中途岛战役日军没有雷达，美军却充分利用了作为一种信息系统的雷达为作战服务）。再讨论具体信息安全问题，二战时通信安全是靠利用密码，但当时密码领域的系统理论水平和具体技术水平都与现在不可相比。现在已经掌握密码安全的条件，并有各种类型密码供不同条件选择使用（例如公钥 RSA 码，码长 1 024 位是安全的，如加上一次一密钥用法则是保证安全的，除非利用尚在探讨中的量子态计算模式），而二战时密码系统理论尚不能从总体上分析判断密码的安全性，才发生日军所用密码自己以为安全实际上不安全。二战时用的密码现在已不成为密码。以 20 世纪 80 年代流行的 RSA 码为例，128 位、256 位都不安全，密钥要加长，至少 512 位才安全，现在 512 位也变得不十分可靠，说明“除旧立新”与“发展”是同步提高的，是密码系统进步和发展的主要模式。同样，信息系统发展及信息安全领域的发展也以不断除旧

立新、对立统一的发展作为主要模式。

3.4.3　信息安全对抗问题的系统实质特征

上几小节论述了信息安全对抗过程是复杂对立斗争的动态过程，同时也是发展过程，是嵌入社会共同发展，侧重“过程”概念（过程剖面）对信息安全对抗双方的动态对立斗争进行讨论，本小节将进一步对“问题”总体特征，即系统性特征进行论述。

· 信息系统是信息科技发挥作用不可缺少的平台，它本身就是系统而且可能是很复杂的系统，具有明显的系统特征。信息系统嵌入功能使其嵌入其他系统，作为子系统发挥重要作用，在更大的系统范围内体现系统特性。信息系统“安全问题”，是信息系统生存运行过程中的重要问题的一个，就其总体而言必具有明显的系统运动特征。

· 信息系统在发展过程中量变、质变互相转换交替，在质变阶段，信息及信息系统状态是远离平衡状态、耗散地发展的。无论功能、结构还是约束条件的变化，一般都是非线性的，安全对抗问题所引发的信息系统发展也必随之具有明显的多层次，量变、质变互相转换交替的性质。

· 信息系统自组织特性，会形成多层次宏观“序”，并且与环境共同进化，称为通过“潮落”（对立斗争的起伏）达到新序形成及进化机制的进化，信息系统安全对抗问题的发展明显具有这种特征，并已成为信息系统发展的一个核心“剖面”。

· 信息安全对抗具有明显的系统对抗性质，受系统理论中普遍规律以及“信息安全与对抗的一些专门原理规律（在第四章中介绍）制约，利用这些规律可促进其发展，对一个具体信息安全对抗问题，还离不开一些专门科学技术未能涉及的众多学科（当然还包括其他社会问题等），形成系统科学技术与各专门学科领域共同发展的总体形势（包括了互相促进互相制约），而非互不兼容、互相排斥的发展。

3.4.4　信息安全及信息攻击防范的系统发展概念

本小节在上两小节论述结论基础上讨论“发展”，具体有两个方面。第一方面从宽范围支持信息安全发展角度讨论，第二方面从较专门范围即对信息攻击防范角度进行讨论。

一、由社会进步、科技发展、社会成员素质提高作为基础，促进信息安全的发展

社会是人类社会，是人类众多个体结合形成整体活动的社会，科技发展是指人类掌握客观规律及实践的方法、路径（包括人类社会及人自己发展的客观规律），总之都密切关联到人，要以人为本。信息安全问题的最基础根源是来自人与自然关系、在人类社会中人与人关系、人类所涉及的诸多“关系”与状态中的一种，它在社会中越来越重要，值得被人自己注意，同时促进

社会发展。通过社会进步科技发展，不断有新的信息科技和系统进入社会，服务于人，发挥作用，淘汰陈旧的系统和技术，“附着”在淘汰的系统和技术上的安全对抗问题也随之消亡。社会进步不断产生更合理的社会秩序，人素质的提高会有更多人在更多场合下自觉遵守高尚的道德品行，总体上减少由各种违法、违规所产生的信息安全事件，因此更“大”更广泛的社会发展是信息安全发展的广泛基础。

二、加强中华优秀文化的现代化发展是信息安全发展的基础

中华文化是世界上少数延续数千年的优秀文化之一，是世界文明财富的重要组成，也是中华民族的瑰宝，其底层“核心”是哲学文化具有稳固发展的特性，虽不易感觉到它的存在，但它实际上是中华民族的灵魂，须臾不可离，它在深层次对中华民族的生存发展发挥作用。中国哲学思维特点是：崇尚辩证的对立统一，强调整体，非常注重“综合”，争取和谐存在。中华文化讲究兼容并蓄，这与过分注重分析、分离、对立以致容易发生还原论、绝对化、单极化等思维方式（易造成偏差）截然不同。中华文化的核心理念将在 21 世纪及其后续漫长岁月中将对人类文明（包括科学技术、人的道德品行、社会进步等）发展起到重要促进作用，对扎根在社会、科技、人类道德品行而同步发展的信息安全对抗问题，必然起到基础功能。

三、注意社会发展中某些相关机制的完善，促进信息安全发展的社会基础的改善

关怀青少年成长的社会机制是重要战略机制，要注意对逆境和困境青少年心理健康成长、得到良好教育等方面关心帮助的有力措施，此外对社会弱势、困难群体的帮助支持机制等都是减少社会激烈矛盾，减少“对抗”的基础机制。还有一种顶层机制也很重要，即关注社会自身发展机制的机制，它的重要性体现在，社会自身发展能力的加强是一种强化内因的根本作用，类推至信息安全领域，便是一种使全社会关心信息安全的正面发展机制，这是一种造血型发展机制。

四、不断加强基础科学发展以支持信息发展，并由社会人文意义上加强社会理性化发展，从而促进信息安全发展

自然科学与数学领域的发展是信息科学技术及信息安全发展的基础，这是源自自然科学与数学都是由各自的学科领域研究事物运动规律及其状态的表征，它们的发展都是“信息”及信息安全发展的必要基础，众多学科也都是从“物理”角度发挥基础作用。当信息领域所需“基础”有突破性发展后信息及其安全领域定有长足发展。

社会基础学科的发展，是在“人理”及“事理”基础层次支持信息安全的发展。信息安全问题，尤其是信息攻击与防范领域密切涉及社会与人的各种内在因素，先进社会与更高的人的素质水平，是社会更高理性的基础，必然对应于更良好的社会信息安全状态。而人文科学是以研究人本身的完善为目标的学科，人的完善是通过培养德性达到人的博雅、卓越和完善（如公正、

正义、勇敢、谦虚、团结、为公、自强不息等种种品行）。社会科学是研究人类社会不断科学发展的学科，它包括由人类社会多层次、多剖面的功能、结构及其相结合的运行机制等作为研究内容，分别形成如政治经济学、政治学、社会学、犯罪学、法学等学科。这些学科的研究发展，是建立先进社会机制的理论基础。人类社会是一个极其复杂的巨系统，其持续进化非常需要理论基础的支持和人类长期在不断提高理性的实践活动，“信息安全”作为人类社会发展、应用“信息”的重要条件与“社会”存在着互动，社会发展更先进，必然会有利于“信息”的安全利用。

五、加强教育工作发展，是提高人素质和能力的一项实际行动，进而从“以人为本”的本源上促进信息安全的发展

“教育”的本质目的和作用是人类文明的传承和持续人类的进化发展，这里的教育是指整个教育体系，包括各种“教育”，人的素质和能力的提高，是从“以人为本”概念上促进了信息安全的发展，其道理是容易理解和公认的，在此就不再详细叙述。

以下讨论加强信息安全的直接措施，主要讨论科技领域的重要措施及另辟一节法律领域的主要措施。

六、依靠技术科学构建信息安全领域基础设施

① 加强相关领域应用基础对应的技术科学研究及应用研究是在信息领域及信息安全领域取得“创新”和“可持续发展”的直接动力。其“相关领域”内涵非常广泛，有与“信息”直接相关，如电子学、光电子学、信息论、通信理论、数字技术、计算机科学与技术等。另外还包括物理、化学、数学、生物学等有关领域，它们对进一步技术发展起基础性支持作用，如大型软件可靠性问题的提高，大型网络组成结构耐破坏性的提高，密码安全性的提高都需基础学科深层次的支持。

② 建立和发展信息安全基础设施。信息安全基础设施是一个体系概念，是由各种必需的信息安全基础设施（本身是复杂系统）所组成，它同时处于动态发展、不断变化中，按工作性质可分为信息安全运行基础设施、信息安全科技发展基础设施、法律鉴定认定基础设施等。运行类又可再分为公共密码基础设施（只负责公钥制密码使用管理，保证有序运行），各类认证中心，认证中心的认证机构等。建立各种信息安全基础设施，需要多种学科和人才支持，主要是信息科技以及与信息科技相联系的管理学科和人才。

③ 建立较完整的软硬件兼备的安全产品系列。这项工作是保证信息系统安全的直接物质基础，没有这些基础无法构筑安全信息系统，即丧失了“信息安全”的基础条件。信息安全产品种类很多，如有关的密码产品系列（包括算法）就是一种典型产品，水印产品也是。

④ 建立符合安全标准的信息通用基础产品系列。数字技术的应用大大拓宽信息类产品的普及和迅速发展，形成一个庞大领域。各类应用产品门类极其繁多，可划分层次和不同剖面来研究其发展规律，例如由信息安全剖面而言：有专门信息安全类产品系列，这样并不足以保

证信息安全，尚需支持安全产品的基础通用产品系列。“信息安全”防范攻击是一个系统性问题，必须在多层次、多环节上保证安全，如在应用层利用信息安全产品（如加密密文传递），但若在信息未加密前便已泄露，则应用层安全也无意义。而基础层次的安全，往往与一些通用基础性产品密切有关，如 CPU、操作系统、数据库管理，若有漏洞则很容易发生安全问题。同时还应指出，这些高性能标准的通用基础产品系列的发展，不单与信息安全密切相关，而且还与信息领域全面发展（包括扩大市场竞争能力，国防建设发展等）密切相关，应选择几个重点方向大力促进发展，才能使信息系统与信息安全同步发展。

本小节在前几小节概念的基础上提出一些重点发展工作，使我国信息领域呈系统性的可持续发展特性，还需指出核心部分自主知识产权技术的掌握涉及国家安全、国防建设的前沿核心信息科技的发展能力，这些都是中华民族复兴所必备条件之一。由工作原理到“能力”的实现，中间需经过众多艰苦的工作环节以及众多科技人员及从事相关工作人员长期努力才能达到，其中那些从事基础研究和应用基础研究的人们客观上只能少数人成功获得重大突破，大部分人只会给后继者提供“经验”和“基石”，他们的精神是可贵的，值得发扬。

3.5 法律领域加强信息安全问题的措施

3.5.1 概 述

随着信息科学技术及各类信息系统的发展和普及，各种与信息有关的犯罪也大大增加，利用法律与犯罪作斗争（避免犯罪、维护秩序、惩治犯罪）是历来人类的做法。针对利用信息高科技和信息系统（包括涉及信息安全）这一类新型犯罪，设立相应法律制裁手段自然提到议事日程上来，如何设立法律体系是个复杂问题。法律界仍有争论，世界各国做法也不一致。有效打击信息领域跨国犯罪是重要的法律延伸问题，同时也具有相当大的困难。针对信息领域犯罪法律体系正在完备中，它将是法律体系新的重要分支，并与其他法律领域有很多交联，具有很大的系统复杂性，本节只作简述。

作为法律体系中惩治犯罪的主要法律，“刑法”针对信息领域犯罪行为现有四类立法模式：

第一类是继续沿用现有的刑事法律来惩治信息犯罪，将这种犯罪归类于传统犯罪，只不过认为犯罪者用了新的犯罪工具，形成新的犯罪方式。这种模式无需特别立法，通常以立法形式进一步明确传统法律，不加修改地适用信息领域的犯罪。这种模式能保持法律稳定性，但很难涵盖日新月异的信息犯罪的全部类型，会造成打击犯罪不力，若不断延伸某些法律条文及术语的含义，就有可能与通行国际刑法原则相违背。

第二类是将新的犯罪刑法法律规定在原刑法典的章节中。这可再分为两种情况，即一种是依据信息领域犯罪的种类和性质，将有关法律条文分散规定在刑法各章节；另一种是将所有

新的犯罪类型看做一个整体，集中规定在刑法某一章节，使之形成较为完整的罪名体系（包括修改相应条款和增加新条款），如加拿大 1985 年通过的刑法修正案，日本 1987 年通过的刑法部分法律条文修正案，荷兰 1993 年通过的刑法修正案等。这种做法保证了刑法完整性，但由于信息领域的犯罪是一个新犯罪类型，其犯罪内涵在不断变化中，若频繁修订刑法会使之不稳定，如不修改则可能发生刑法不完全涵盖的问题。

第三类是制定单行单独的法律。如美国除了佛蒙特州外，各州都制定了专门的计算机犯罪法，英国在 1990 年修改将计算机网络犯罪完全视为传统犯罪的模式制定了专门的法律《计算机滥用法》，这种立法形式比较灵活，修改起来比较方便，但应注意保证与刑法及至单行法律之间的相互协调。

第四类是在其他法律、法规中设置有关信息犯罪的条款，也就是“附属刑法”。如法国《信息管理法》规定非法进入或在计算机系统功能中设置障碍，干扰数据完整性与真实性，伪造和不当使用计算机等方面的内容。

上述四种立法形式各有利弊，不适于只采用一种模式，不少国家都采用两种以上的立法模式。

我国刑法针对信息犯罪的处理原则是采用第一类、第二类原则相结合方式。如刑法第二百八十七条规定，利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或其他犯罪的，依照本法有关规定罪名处罚。《全国人大常委会关于维护互联网安全的决定》中第二、三、四条规定犯罪的行为明确指出，犯罪者将按照刑法有关规定追究刑事责任，这些规定体现了上述第一类原则。在我国 1997 年修订的刑法中第二百八十六条、二百八十七条所规定的非法入侵计算机系统罪，破坏计算机系统罪属于第二类立法形式，是通过扩大延伸原法律术语的含义、修改原有法律条文、增设新条款来实现对这类犯罪的惩治。

我国涉及信息安全领域的其他法律、法规，经过持续的法治建设，已初步构成法律体系，并正在执行中。随着信息化带动现代化的进程，信息领域涉及安全问题的法律、法规还将进一步建设完善。

3.5.2　我国涉及信息安全的相关法律法规简介

一、直接相关法律法规

1.《中华人民共和国刑法》（节选）

二百八十五条　违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

二百八十六条　违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰、造成计算机系统不能正常进行工作，后果严重的处五年以下有期徒刑或者拘役；后果特别严重的，

处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的依照相关规定处理。

二百八十七条　利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或其他犯罪的处罚，依照本法有关规定定罪处罚。

2.《全国人大常委会关于维护互联网安全的决定》概述

本《决定》是一个法规，其核心目的是在国家大力倡导和推动下，在互联网日益发挥作用的同时，为了兴利除弊，使互联网得到更好的发展，维护国家安全和社会公共利益，保护个人、法人和其他组织的合法权益，规定对破坏互联网安全运行的各种行为构成犯罪者追究刑事责任；对利用互联网非法运行影响国家安全构成犯罪者追究刑事责任；对破坏社会主义市场经济秩序和社会管理秩序构成犯罪者依刑法追究刑事责任；对侵犯个人、法人和其他组织的人身、财产等合法权利构成犯罪者依刑法追究刑事责任，对上述规定范围以外，利用互联网构成犯罪者也按刑法追究刑事责任。《决定》还规定了利用互联网进行违法活动尚构不成犯罪者按其他法规、行政管理规定等进行相应惩治。《决定》会同刑法及其他法规，构成规范互联网运行发展的法律体系。对互联网运行中规定不得违反事项的违反者将依照刑法追究刑事责任。

· 不得侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统。

· 不得故意制作、传播计算机病毒等破坏性程序，不得攻击计算机系统及通信网络致使计算机系统及通信网络遭受损害。

· 不得违反国家规定，擅自中断计算机网络或者通信服务造成计算机网络或者通信系统不能正常进行工作。

在互联网中规定不得影响国家安全和社会稳定的事项主要有：

· 不得利用互联网造谣、诽谤或者发表、传播其他有害信息，煽动颠覆国家政权，推翻社会主义制度或者煽动分裂国家、破坏国家统一。

· 不得通过互联网窃取、泄露国家秘密、情报或者军事秘密。

· 不得利用互联网煽动民族歧视、破坏民族团结。

· 不得利用互联网组织邪教组织、联络邪教组织成员、破坏国家法律、行政法规。

· 不得利用互联网销售伪劣产品或者对商品、服务作虚假宣传。

· 不得利用互联网损害他人商业信誉和商品声誉。

· 不得利用互联网侵犯他人知识产权。

· 不得利用互联网建立淫秽网站、网页，提供淫秽站点链接服务。

· 不得利用互联网编造并传播影响证券、期货交易或者其他扰乱金融秩序的虚假信息。

· 不得利用联网侮辱他人或者捏造事实诽谤他人。

· 不得利用互联网非法截获、篡改、删除他人电子邮件或者其他数据、资料，侵犯公民通信自由和通信秘密。

· 不得利用互联网进行盗窃、诈骗、敲诈、勒索。

3. 中华人民共和国电信条例(2000年9月国务院公布实施)电信安全章节

本条例主要作用为规范电信市场秩序，保障通信网络安全，促进电信业务和互联网健康有序发展，条例包括总则，电信市场、电信服务、电信建设，电信安全、罚则和附则共七章，第五章为电信安全，摘录如下。

第五十七条　任何组织或者个人不得利用电信网络制作、复制、发布、传播含有下列内容的信息。

（一）反对宪法所确定的基本原则的；

（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

（三）损害国家荣誉和利益的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）破坏国家宗教政策，宣扬邪教和封建迷信的；

（六）散布谣言，扰乱社会秩序，破坏社会稳定的；

（七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

（八）侮辱或者诽谤他人，侵害他人合法权益的；

（九）含有法律、行政法规禁止的其他内容的。

第五十八条　任何组织或者个人不得有下列危害电信网络安全和信息安全的行为。

（一）对电信网络的功能或者存储、处理、传输的数据和应用程序进行删除或者修改；

（二）利用电信网从事窃取或者破坏他人信息、损害他人合法权益的活动；

（三）故意制作、复制、传播计算机病毒或者以其他方式攻击他人电信网络等电信设施；

（四）危害电信网络安全和信息安全的其他行为。

第五十九条　任何组织或者个人不得有下列扰乱电信市场秩序的行为。

（一）采取租用电信国际线路私设转接设备或者其他方法，擅自经营国际或者香港特别行政区、澳门特别行政区和台湾地区电信业务；

（二）盗接他人电信线路，复制他人电信码号，使用明知是盗接、复制的电信设施或者码号；

（三）伪造、变造电话卡及其他各种电信服务有价凭证；

（四）以虚假、盗用的身份证办理入网手续并使用移动电话。

第六十条　电信业务经营者应当按照国家有关电信安全的规定，建立健全内部安全保障制度，实行安全保障责任制。

第六十一条　电信业务经营者在电信网络的设计、建设和运行中，应当做到与国家安全和电信网络安全的需求同步规划，同步建设，同步运行。

第六十二条　在公共信息服务中，电信业务经营者发现电信网络中传输的信息明显属于本条例第五十七条所列内容的，应当立即停止传输，保存有关记录，并向国家有关机关报告。

第六十三条　使用电信网络传输信息的内容及其后果由电信用户负责。

电信用户使用电信网络传输的信息属于国家秘密信息的，必须依照保守国家秘密法的规定采取保密措施。

第六十四条　在发生重大自然灾害等紧急情况下，经国务院批准，国务院信息产业主管部门可以调用各种电信设施，确保重要通信畅通。

第六十五条　在中华人民共和国境内从事国际通信业务，必须通过国务院信息产业主管部门批准设立的国际通信出入口进行。

我国内地与香港特别行政区、澳门特别行政区和台湾地区的间的通信，参照前款规定办理。

第六十六条　电信用户依法使用电信的自由和通信秘密受法律保护。除因国家安全或者追查刑事犯罪的需要，由公安机关、国家安全机关或者人民检察院依照法律规定的程序对电信内容进行检查外，任何组织或者个人不得以任何理由对电信内容进行检查。

电信业务经营者及其工作人员不得擅自向他人提供合法用户使用电信网络所传输信息的内容。

4. 公安部关于对《中华人民共和国计算机信息系统安全保护条例》中涉及的“有害数据”问题批复的摘录

“有害数据”是指计算机信息系统及其存储介质中出现的，以计算机程序、图像、文字、声音等多种形式表示的，含有攻击人民民主专政，社会主义制度，攻击党和国家领导人，破坏民族团结等危害国家安全内容的信息；含有宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪等危害社会治安秩序内容的信息；危害计算机信息系统运行，功能发挥和数据可靠性、完整性、保密性，以及用于违法活动的计算机程序（含计算机病毒）。

二、间接相关法规（含规范信息安全的各种行为）

1.《科学技术保密规定》（代替原《科学技术保密条例》）

本规定共五章三十四条，现将第二章国家科学技术秘密的范围和密级节录如下。

第七条　关系国家的安全利益，一旦泄露会造成下列后果之一的科学技术，应当列入国家科学技术秘密范围。

（一）削弱国家的防御和治安能力；

（二）影响我国技术在国际上的先进程度；

（三）失去我国技术的独有性；

（四）影响技术的国际竞争能力；

（五）损害国家声誉、权益和对外关系。

第八条　国家科学技术秘密的密级。

（一）绝密级

（1）国际领先，并且对国防建设或者经济建设具有特别重大影响的；

（2）能够导致高新技术领域突破的；

（3）能够整体反映国家防御和治安实力的。

（二）机密级

（1）处于国际先进水平，并且具有军事用途或者对经济建设具有特别重大影响的；

（2）能够局部反映国家防御和治安实力的；

（3）我国独有，不受自然条件因素制约，能体现民族特色的精华，并有社会效益或经济效益显著的传统工艺。

（三）秘密级

（1）处于国际先进水平，并且与国外相比在主要技术方面具有优势，并且社会效益或者经济效益较大的；

（2）我国独有，受一定自然条件因素制约，并且社会效益或者经济效益较大的传统工艺。

第九条　有下列情况之一的，不列入国家科学技术秘密范围。

（一）国外已经公开；

（二）在国际上无竞争能力且不涉及国家防御和治安能力；

（三）纯基础理论研究成果；

（四）在国内已经流传或者当地群众基本能够掌握的传统工艺；

（五）主要受当地气候、资源等自然条件因素制约，很难模拟其生产条件的传统工艺。

第十条　属于国家科技秘密和民用科学技术，原则上不定为绝密级，确需定为绝密级的，应当符合本规定第八条关于绝密级的规定，并报国家科委审批。

2.《计算机信息系统国际互联网保密管理规定》(2000 年 1 月国家保密局发布)有关条款

第六条　涉及国家秘密的计算机信息系统不得直接或间接地与国际互联网或其他公共信息网络相联，必须实行物理隔离；

第七条　涉及国家秘密的信息，包括在对外交往与合作中经审查批准与境外特定对象合法交换的国家秘密信息不得在国际互联网计算机信息系统存储、处理、传递。

第八条　上网信息的保密管理坚持“谁上网谁负责”的原则，凡向国际互联网的站点提供和发布信息必须经过保密审查批准。

第九条　凡以提供网上信息服务而采集的信息，除在其他新闻媒体已公开发布外，组织者在上网发布前，应当征得提供信息单位的同意。凡对网上信息进行扩充或更新，应当认真执行信息保密审核制度。

第十条　凡在网上开设电子公告系统、聊天室、网络新闻组的单位和用户应由相应的保密工作机构审批，明确保密要求和责任。任何单位和个人不得在电子公告系统、聊天室、网络新

闻组上发布、谈论和传播国家秘密信息。

第十一条　用户使用电子函件进行网上信息交流，应当遵守国家有关保密规定，不得利用电子函件传递、转发或抄送国家秘密信息。

3.《中华人民共和国保守国家秘密法》

共五章三十五条。第一章总则，第二章国家秘密的范围和密级，第三章保密制度，第四章法律责任，第五章附则。详细内容可查阅专门文件。

4.《计算机软件保护条例》（国务院令 84 号发布）

共五章。第一章总则，第二章计算机软件著作权，第三章计算机软件的登记管理，第四章法律责任，第五章附则。详细内容可查阅专门文件，由章节目录可得到本条例主要内容。

5.《中华人民共和国计算机信息系统安全保护条例》

共五章三十一条。第一章总则，第二章安全保护制度，第三章安全监督，第四章法律责任，第五章附则。主要目的为保护计算机信息系统安全，促进计算机的应用和发展。保护制度中将计算机信息系统的建设和应用纳入遵守法律法规及其他国家规定，如计算机房建设不得危害计算机信息系统安全，各单位应建立健全安全管理制度，报告发生案件，规定了安全监督内容和法律责任等。

6.《计算机信息系统安全专用产品分类原则》

涉及实体安全、运行安全和信息安全三个方面，每个方面再细分若干方面，明确了分类原则，定义了专门术语，并按上述三个方面分别建立了类别体系，是一个基础性法规文件。

7.《计算机病毒防治管理办法》

本办法规定了公安部公共信息网络安全监察部门主管全国的计算机病毒防治管理工作及各级地方公安部门为地方分管部门，规定了个人、单位不得制作计算机病毒，不得有各种传播病毒的行为（包括销售、出租、赠送含病毒媒体，生产制造、销售防治病毒者行为规范，社会各单位个人在防治病毒工作中的行为规范（含报告“疫情”，防治病毒等各种职责）以及罚则。

8.《计算机信息系统安全保护等级划分准则 GB17859—1999》

本准则规定了计算机系统安全保护能力的五个等级。第一级，用户自主保护；第二级，系统审计保护；第三级，安全标记保护；第四级，结构化保护；第五级，访问验证保护（依次为最高级）。定义了专门术语，建立各等级划分准则（各级安全功能内涵），本准则实质上是一个标准。

9.《商用密码管理条例》（商用密码技术属国家秘密）

对不涉及国家秘密内容的信息进行加密保护或安全认证所使用密码技术和密码产品，国家实行自研究、制造、销售、使用、监督管理的专控管理为本条例核心内容。其他法律、法规从略。还将不断有新法律、法规产生以促进信息安全的有序发展。

10.《中华人民共和国电子签名法》

2004 年 8 月 28 日，中华人民共和国第十届全国人民代表大会常务委员会第十一次会议通过了《中华人民共和国电子签名法》。作为我国电子商务领域的第一部法律，《电子签名法》

的出台，第一次从法律上将数字化活动推到了实际操作的阶段，开启了中国电子商务立法的大门，它为解决司法实践中亟待回答的问题，扫清网络交易行为的障碍提供了立法保障，为互联网从单纯的媒体时代过渡到全面应用时代奠定了基础，并将进一步规范网上行为，净化网络环境，消除网络信用危机，保障用户的各项权利，为我国的网络立法与国际立法的接轨起到了示范性作用。该法自 2005 年 4 月 1 日施行。该法共分五章，总则、数据电文、电子签名与认证、法律责任、附则。下面是电子签名法的法律责任（第四章）部分。

第二十七条　电子签名人知悉电子签名制作数据已经失密或者可能已经失密，未及时告知有关各方，并终止使用电子签名制作数据，未向电子认证服务提供者提供真实、完整和准确的信息，或者有其他过错，给电子签名依赖方、电子认证服务提供者造成损失的，承担赔偿责任。

第二十八条　电子签名人或者电子签名依赖方因依据电子认证服务提供者提供的电子签名认证服务从事民事活动遭受损失，电子认证服务提供者不能证明自己无过错的，承担赔偿责任。

第二十九条　未经许可提供电子认证服务的，由国务院信息产业主管部门责令停止违法行为；有违法所得的，没收违法所得，违法所得三十万元以上的，处违法所得一倍以上三倍以下的罚款；没有违法所得或者违法所得不足三十万元的，处十万元以上三十万元以下的罚款。

第三十条　电子认证服务提供者暂停或者终止电子认证服务，未在暂停或者终止服务六十日前向国务院信息产业主管部门报告的，由国务院信息产业主管部门对其直接负责的主管人员处一万元以上五万元以下的罚款。

第三十一条　电子认证服务提供者不遵守认证业务规则、未妥善保存与认证相关的信息，或者有其他违法行为的由国务院信息产业主管部门责令限期改正。逾期未改正的，吊销电子认证许可证书，其直接负责的主管人员和其他直接责任人员十年内不得从事电子认证服务。吊销电子认证许可证书的，应当予以公告并通知工商行政管理部门。

第三十二条　伪造、冒用、盗用他人的电子签名，构成犯罪的，依法追究刑事责任。给他人造成损失的，依法承担民事责任。

第三十三条　依照本法负责电子认证服务业监督管理工作的部门工作人员，不依法履行行政许可、监督管理职责的，依法给予行政处分。构成犯罪的，依法追究刑事责任。

11.《电子认证服务管理办法》

为了规范电子认证服务行为，对电子认证服务提供者实施监督管理，依照《中华人民共和国电子签名法》和其他法律、行政法规的规定，制定了《电子认证服务管理办法》，并于 2005 年 1 月 28 日由中华人民共和国信息产业部第十二次部务会议审议通过，该办法自 2005 年 4 月 1 日起施行。该法共分八章，总则、电子认证服务机构、电子认证服务、电子认证服务的暂停终止、电子签名认证证书、监督管理、罚则、附则。下面是罚责（第七章）部分。

第三十七条　电子认证服务机构向信息产业部隐瞒有关情况、提供虚假材料或者拒绝提供反映其活动的真实材料的，由信息产业部依据职权责令改正，并处警告或者五千元以上一万元以下罚款。

第三十八条　信息产业部和省、自治区、直辖市的信息产业主管部门的工作人员，不依法履行监督管理职责的，由信息产业部或者省、自治区和直辖市的信息产业主管部门依据职权视情节轻重，分别给予警告、记过、记大过、降级、撤职、开除的行政处分。构成犯罪的，依法追究刑事责任。

第三十九条　电子认证服务机构违反本办法第十六条、第二十七条的规定的，由信息产业部依据职权责令限期改正，并处警告或一万元以下的罚款，或者同时处以以上两种处罚。

第四十条　电子认证服务机构违反本办法第三十三条的规定的，由信息产业部依据职权责令限期改正，并处三万元以下罚款。

3.5.3　法律维护信息安全的执法过程要点简述

法律维护信息安全最基本作用是将维护信息安全以“法律”形式进行规范化，并纳入法律体系中作为重要组成部分。在法治社会中，法律是一切活动自由度的最后界限（不得超出），除起规范作用外还起威慑作用，通过法律宣传教育对社会公众起提高自觉的教育作用等。法律最后作用是维护社会秩序、法律权威，对触犯法律者进行惩罚，正因为它是最后一道作用，故一方面应严肃、严格，另一方面应科学严密、公正、公开两个方面相互制约又相辅相成。本书非法律书籍，不宜详述，只就执法过程（着重与信息相关内容）作一简述。

一、法律介入信息安全案件过程简述

如图 3.4 所示为信息安全犯罪的执法过程简图。

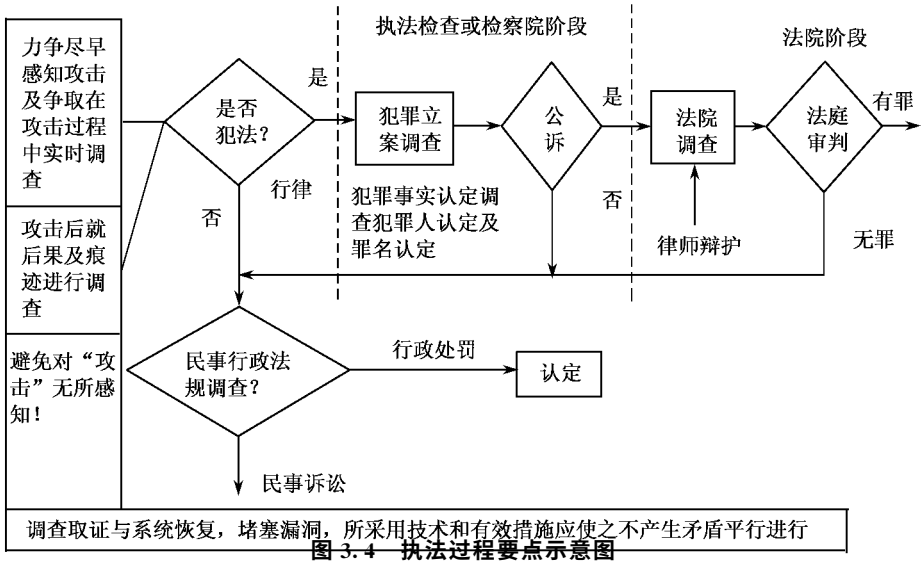


图 3.4　执法过程要点示意图

二、涉及信息安全刑事犯罪罪名

共有四条罪名，由刑法第二百八十五条、二百八十六条、二百八十七条规定，它们是：

- 非法侵入计算机信息系统罪。
- 破坏计算机功能及正常工作罪。
- 破坏计算机程序数据罪。
- 利用计算机进行金融犯罪、窃取国家秘密及其他犯罪。

其中，非法入侵计算机信息系统罪为其他犯罪前奏及必要步骤，在这条罪行中没提及后果，这是值得注意的，造成“入侵”事实即构成犯罪，至于有犯罪行动，但入侵未遂是否构成犯罪？要根据实际情况而定。其他罪名是否成立都与后果挂钩，都可以与“非法入侵罪”共同成立。

入侵计算机信息系统，犯罪人可以物理上并不接触计算机，而以技术手段侵入信息系统。其过程大体与本节开始过程一致，只不过具体情况具体内容有所变化。如操作系统、网络拓扑结构都会有所变化，攻击者在达到入侵计算机信息系统目的采取的手段中（尤其是收集攻击信息阶段），与正常用户正常工作行为一致，很难被察觉，只有反常行为才有可能为被发觉被查找和曝露提供线索。以下用对以 UNIX 为操作系统的入侵为例进行说明。一般情况下分为三步，第一步，攻击者利用 finger 或 send mail 等服务来确定目标系统上某个用户账号，然后使用密码工具获得口令，至此用户已获得 shell 访问权，具有一个普通用户访问权。第二步，进行访问权攻击，进一步获得 root 的权限（利用系统“默认”状态漏洞，利用管理员的漏洞修改系统文件配置、破密码），至此完成了入侵的前期工作。第三步，进入计算机信息系统获取文件，修改文件，最后还可能放置特洛依木马等类似程序，为下次入侵留后门，并尽可能清理系统登记以消除入侵痕迹和罪证。包括清除登记文件可能暴露侵入行为的记录，清除 shell 中使用过命令的记录。入侵者消除入侵痕迹的行为（消除罪证的一）是否得逞与系统管理水平有关，如管理员将登记文件设置成“只能增加内容而不能减少内容”的属性，入侵者就很难将用户 shell 文件曾用命令记录（ban-history 文件）删除或修改日期。另外如 UNIX 主机使用了 syslog 配置作登记备份，也可查到入侵证据！以上说明攻击与防范攻击是一场对立斗争（也有统一处）。

三、计算机信息系统罪证的简要讨论（含其他电子证据）

“罪证”是法律结束案件的重要依据（重物证是我国刑法定案的第一因素）。在计算机信息系统遭受攻击留下的证据，不同于“普通”犯罪罪证，而是有其特殊性。由于计算机作为“工具”，或作为“部件”嵌入其他信息系统，以计算机信息系统罪证为代表，具有普遍性和重要性，所讨论内容也适用于其他电子设备中的电子证据。

1. 数字证据的特点和优点

① 潜在性，需要借助专用设备和科学方法才能显现。

② 易传播性。

③ 脆弱性，易被改变销毁。

④ 时间确定性，易配有对应时间记录。

⑤ 可以被精确复制，可避免对原件的损伤。

⑥ 用适当的软件工具去对比原件，容易鉴别数字证据是否被改变。

⑦ 在一定情况下犯罪嫌疑人完全销毁数字证据有一定困难。

2. 计算机中数据证据

① 用户自建文档（地址簿、日程表、收藏夹、文本、文件、数据库文件）。

② 用户保护文档（压缩文件、改名文件、密码保护文件）。

③ 计算机创建文件（备份文件、日志文件、交换文件）。

④ 计算机系统管理文件，如上小节攻击者力图消除痕迹中所涉及文件。

3. 其他电子证据（模拟形式的证据）

① 自动应答设备记录。

② 数码相机记录。

③ 手持电子设备：个人数字助理。

④ 打印机、复印机、读卡机等的记录。

四、计算机信息系统的罪证提取是广泛、艰巨、细致的技术工作

罪证是犯罪过程状态的记录，也是一种信息。消除证据是一种行动，也包括消除证据信息。绝对隐藏信息是不可能的，但在广泛的信息海洋中提取特殊所需很艰难，是技术性很强的工作，只能因地制宜，针锋相对采取各种方法，这是原则和普遍的方法，下面讨论一些具体取证方法：

1. 收集计算机内所有数据

对运行 Window NT 操作系统的机器，具有限制从硬盘提取数据的权限，故可利用 Linux 命令（绕开 Window NT 操作系统）完全复制硬盘中所有文件。对运行 Unix 操作系统的工作站或服务器，提取证据的步骤是保存内存数据情况下关机，然后再启动机器提取数据。值得注意的是，不同配置的机器会发生从其他磁盘启动计算机。过程复杂，不当操作会损坏内部所需证据，需要精通 Unix 操作系统的科技人员配合。

2. 利用数据恢复提取数字证据（也是消除数据，删除攻击的后果）

数据恢复原理（以 Window 为例）：它采用了 FAT、FAT32 或者 NTFS 三种文件系统，再以 FAT 文件系统为例。数据文件写到磁盘后会在文件分配表上（FAT）和文件目录表上（FDT）记录相应信息，如文件名称、大小、类型、建立时间起始符号，在盘上所占实际扇形区位置。当删除一个文件时，在文件目录表上加上删除标志，但没有新文件写入而全部覆盖情况下，文件还保留着。数据区占据了硬盘的大部分空间，通常所说的格式化程序如 Format 程

序，只是重写了 FAT 表，并没有把 DATA 区的数据全部删除，这是数据很多情况下可恢复的原理。

3. 恢复数据的几个原则方法

① 首先，要保护计算机处在原始状态，对涉案磁盘可“克隆”几个副本，不要对原盘进行恢复操作，以保证数据不被损坏。

② 第二，恢复数据过程中最好外挂一个可引导硬盘，并将其虚拟内存只能放在 C 盘上，以保证不丧失数据。

③ 第三，对内容较明确的数据，若使用常用恢复软件不能有效情况下，可根据文件内容尝试可能获得数据区中未被覆盖的重要数据。

④ 第四，在精通技术的前提下，认真细致，以不放弃任何一点蛛丝马迹的精神努力工作，有时要以“死马当活马医”的原则，做到不丧失任何“可能”。

3.6　本章小结

本章从系统层次论述了信息安全与对抗问题，主要讨论了信息安全与对抗的基本问题和发展问题、产生根源及法律措施，包括：信息安全与对抗问题的基本描述，提出“对抗信息”概念、信息安全、信息系统安全、安全性的四性归纳及攻击与对抗的基本概念；信息安全问题的四种产生根源，矛盾运动发展根源，国家利益斗争根源，科技发展不完备根源，社会矛盾及人的介入根源；信息安全及信息攻击防范的系统发展工作要点，中国涉及信息安全犯罪的法律、法规及执法过程。

习　　题

1. 什么是信息安全问题？什么是信息系统的安全问题？
2. 信息安全问题的四种特性是什么？
3. 信息安全问题产生的根源有哪些？其内涵是什么？
4. 试利用矛盾的运动发展规律观点分析信息安全问题的产生？
5. 论述并举例说明科技发展不完备是信息安全问题产生的一种根源？
6. 论述并举例说明人的介入是信息安全问题产生的一种根源？
7. 论述并举例说明信息系统对抗过程的主要步骤？
8. 信息安全对抗问题的实质是什么？
9. 信息系统攻击与防范系统发展的概念指的是什么？
10. 简述我国涉及信息安全犯罪的主要法律、法规及其内容。

第 4 章　信息安全与对抗基本原理

4.1　引　　言

“信息安全与对抗”是表征在信息领域事物所具有复杂的、对立统一的多层次、多剖面动态演化过程中一个本质特征，它不是孤立、封闭存在的，而是融入人类社会、人类文明发展进化过程中。信息安全与对抗问题的基本原理涉及领域非常广泛，深入研究便涉及“理”体系，各种“道理”具有“开”域的性质，是以真理为中心的无明显边界的问题。依照我国学者所提出的，将“道理”划分为物理、事理、人理、生理四个领域，这种划分是为了便于分类特征研究，不是绝对的。例如，自然哲学也研究物理学中最概括、最基本的理论，又与人理有交叉，因哲学本身就包括人理内容。人们应该有科学的世界观，这就包括了自然哲学。一切真理除了其客观存在以外，还有一项重要属性，即与人结合，被人所理解、掌握才有实际意义（即对人类实际意义）。本章所涉及基本原理，并非哲学理论意义上的“基本”，（该理论意义的“基本”是无尽头的，也无法简单讨论），而只是侧重信息安全与对抗的自然科学领域的基本属性，就应用基础及应用层次中一些基本原理进行讨论。

另一方面，信息安全与对抗问题在实际应用中，是以一些具体领域性问题出现，各领域又可再细化。如通信系统是一个领域，本身再可分为移动通信、卫星通信、电信通信等分领域，计算机网络系统也同样，通信与计算机网络系统现在已交叉。因此，“基本原理”是指非某领域专用，而是各领域共同相关，在此意义上的“基本”意义。

本章基本原理大体上分为两个层次讨论，第一个层次是结合信息及信息安全与对抗领域的特征，应用对立统一规律得出某些基础性原理；第二个层次是在系统层次结合系统结构、功能和动态运行的基本技术原理。具体技术原理和方法的基本应用安排在第五章介绍，还应强调指出：结合信息的特征主要是第二章所叙述基于“宏观物理”的信息特征，尚未包含基于微观量子态基础的信息特征，这种微观状态下“信息”的特征将有变化，安全与对抗问题的特征与基本原理将有所变化，也有待研究。

4.2　信息安全与对抗领域自组织耗散理论基础

本小节主要是延伸自组织耗散理论，构建信息安全与对抗领域基础层次原理的基本思想。

信息科技及系统深深地融入人类社会，形成了与社会共同进化的状态，同时信息安全问题的重要性与迫切性也日益突出，如何看待信息安全问题，如何提高信息安全程度等都是热点问

题，期待研讨与回答。笔者认为，信息安全与对抗问题是信息系统融入社会共同进化事物中矛盾的一部分，具有复杂的系统特征，总体上可以借助开放耗散自组织理论基础，在信息安全对抗领域对应建立分支理论，用以由系统矛盾角度研究信息安全与对抗问题，进而对矛盾进行导引，推动信息科技和信息系统乃至社会发展。

耗散自组织理论可扼要归纳为以下四点结论：

· 开放的耗散结构（非线性、非平衡态、耗散内部不可逆过程产生的熵）必定自组织地形成宏观（系统层次）动态有序（系统层次的运动规律、机制等）。

· 通过“涨落”（矛盾对立斗争造成的状态起伏）开放耗散结构在远离平衡态下达到新的有序，这条结论蕴涵进化概念。

· 大小宇宙共同进化，意指耗散自组织系统融入环境（更“大”的系统）中互相作用共同进化（淘汰不能共同进化者），这样就发展了达尔文的被动选择淘汰理论，也是耗散自组织理论中说明进化过程的重要部分。

· 进化机制不断进化（进化模式也在进化，总的趋势是使世界进化更快）。

以上结论在信息安全对抗领域完全适用，上面已经提到的“信息安全对抗”问题作为一个事物是人类社会进化内容的重要组成部分，它明显地具有系统复杂特征，属于耗散自组织理论适用范围。作为应用研究而言，重要的是结合信息安全对抗领域问题的实际研究，发展信息安全对抗领域的耗散自组织理论分支。也就是在原有基本理论基础上，补充专门内容和原理建立理论分支，进一步促进发展。

笔者认为“具体化”工作中，总体而言应突出“安全对抗”的对立斗争特点（激烈对抗斗争），具体内容（或称补充内容）主要有如下几个方面：

· 特征既然是“斗争”，则进一步自然要向“斗争”围绕“什么”进行，也即斗争围绕什么对象而进行？我们可以说围绕信息系统安全性能而进行，但有着数不清个数、种类的信息系统，有数不清的安全性能，同时只限于安全对抗领域难以联系其他功能。因此，用“安全性能”作为对象仍嫌平淡无特色，应进一步提炼形成更概括、更集中表示对象的概念，笔者认为用“特殊性”较为合适。“信息”核心理念是突出“特殊性”，各种信息系统正常运行可理解为：规则＋信息＋使用目的＝一种特殊性，因此可归纳为“斗争”是围绕“特殊性”展开的，斗争对象是特殊性，也就是保证信息的特殊性。

· “信息”为什么引起“斗争”，引起斗争的基本因素在哪里等等。核心机理是由“信息存在相对性原理”所阐述，即“信息”重要性在于它可表征“运动”（信息表征运动状态，信息集合（群体）可表征运动过程），有“运动”存在必有相应“信息”存在。同时具体的“信息”是可以被“干扰”的（如删节、修改、夺得……）。既体现“存在”又是相对的。由此，存在着的相对性形成了围绕“信息”展开斗争的可能。

· 时间、空间是一切事物存在的基本形式，“信息”作为一个事物，它的时空基本特征是什么？与信息存在相对性如何关联？这是深一层机理问题。“信息”在时间、空间中只占有限尺

度，正是“有限尺度”使得信息存在形式可以被变换，即可形成不同的“特殊性”，这样双方都要利用这基本机理为己方的对抗“服务”。这也体现信息存在相对性的基础。

· 耗散自组织理论中“自组织”功能是一个核心也是基础因素，信息安全对抗的过程特征非常明显，它持续不断又“间断”形成无数个复杂过程，按系统理论推断它必有自组织特征，形成自组织的机理来源于双方为了实现自己目的而采取的各种对抗措施。我们、他们概括为双方围绕保持“特殊性”和破坏“特殊性”的多层次叠套、交织的对抗行为，这也是形成自组织功能的基本机理。

· 信息安全对抗进化机理以及进化机制的进化分析。“通过涨落达到新的有序”（表征着进化）在信息安全对抗领域也有强烈的体现，不断进化的核心机理是对抗双方都必须遵守和竭力运用的“反其道而行之、相反相成”原理（同时也成为核心规律），这条规律导引双方都竭力采用各种相关前沿科学原理、技术方法为己方服务，这是“信息安全对抗”不断进化发展重要动力，也是连接双方形成自组织对抗的机理。

· 将耗散自组织理论用于信息安全对抗领域，除了建立理论框架是重要内容外，研究分析概括类普适性的“切入点”（热点）是另一重要因素。研究认为“热点”就是双方争夺制“对抗信息”权和后续的“抢先”快速反应措施，它是反攻击方重要的斗争切入点，也是双方对抗争夺的焦点。

· 信息安全对抗是信息领域非常重要的问题，但不是全部问题。人类利用信息科技及系统为人类服务，促使社会进化是顶层目的。但信息安全问题作为一个子目标如何融入顶层目标是一个值得注意的问题，“忽视”和过度及不恰当地影响其他功能都不合适，建议在具体场合根据具体条件（功能要求，约束条件）进行系统运筹。对信息安全的正确定位和科学对待是重要的，在以下小节中将依此思考延伸讨论诸“原理”。

以上论述了信息安全与对抗领域自组织耗散理论基础，在此基础上，可以构建信息系统基础层次和系统层次的对抗原理。同时，其原理的引述力图为信息安全对抗领域建立耗散自组织理论分支打基础。

4.3 基础层次对抗原理

本节主要论述构建于信息系统安全与对抗自组织耗散理论基础之上的基础层次对抗原理。

4.3.1 特殊性存在与保持原理

特殊性是与普遍性对立的范畴，两者具有相互依存的统一性，特殊性是事物存在最基本、最概括的本征属性，所有事物的存在都是以各种各样特殊的形式存在，由此将各种各样的存在

形式，如广义空间、时间维中位置、次序、占位大小、持续长短等多维度具体表征，都可概括抽象为一种区分于其他事物的“特殊性”。“特殊性”是一个抽象化的集合名词，具体的特殊性等价于具体事物的存在，特殊性的变化等价于事物的变化，在这个意义上又具有普遍性（每个事物都具有的共同特征）。用到信息领域，仙农教授认为信息量用不确定性的消除来表征，换言之即转化为特殊性的肯定，如将信息理解为运动状态的表征和描述，也是表征和描述各种具体的特殊性。在各种信息系统中，其工作规律、原理可以概括地理解为在普遍性（相对性）基础上对某些“特殊性”的维持和转换，如信息的存储和交换、传递、处理等。“安全”可理解为“特殊性”的有序保持和运行，各种“攻击”可理解为对原有的序和“特殊性”进行有目的的破坏、改变、以至渗入，实现攻击目的的“特殊性”。在抽象概括层次理解信息安全与对抗的斗争是围绕特殊性而展开的，可利用此概念在系统层次考虑系统性方案、主要措施，在技术层次采用具体技术措施以支持合理的系统结构、系统方案，达到科学高效从事信息安全对抗领域的科研和实际工作。

4.3.2　信息存在相对性原理

伴随着运动状态的存在，必定存在相应的“信息”。同时，由于环境的复杂性，具体的“信息”可有多种形式表征运动，且具有相对的真实性。

唯物论者认为客观存在的世界就是运动着的物质，运动是物质存在的特征，列宁的名言是“世界上除了运动着的物质，其他什么也没有”。运动着的物质只有在空间和时间内才能运动（说时间和空间是物质存在的基本形式），再进一步，辩证论认为物质运动的根源在于内部矛盾的对立统一斗争（也就是对立统一的各种矛盾相互作用关系）。运动是按照客观规律进行的，不能随心所欲、违反规律地制造运动。运动与物质存在着等价性，由于物质是不灭的，只有不断地运动、转移，因而运动是不灭的，即运动是名副其实不断地运动（转移）着的（具体体现在一个事物与其他事物间不断变化着的相互关系）。信息是运动状态的表征，它用于表征运动状态，其本身也不断地变化着。信息作为运动状态的表征是客观存在的，在这个最基本概念、哲理意义下，信息不可能被绝对隐藏、仿制和伪造，这是运动的客观存在及运动不灭的本质所形成的，可用一些数学概念简化说明。

设所讨论的处于一定状态的事物集合为 A，其中元素 $a_1,a_2,\cdots,a_i,\cdots,a_j,\cdots,a_n$ 为处于一定状态的各具体事物。事物间发生的某种“关系”，看做集合内元素的运算（实际上它可能非常复杂）用 O 表示。对应 A 集合的信息集合，用 B 表示，其中元素 $b_1,b_2,\cdots,b_i,\cdots,b_j,\cdots,b_n$ 表示具体信息，$\widetilde{O}$ 表示 B 集合中的运算。在理想环境下，人类可借助同构映射概念，得到事物及其关系和对应信息集合及信息间关系，两者是可以等价的。现用数学表达：$a_i \xrightarrow{\Phi} b_i(=\Phi a_i)$，$a_j \xrightarrow{\Phi} b_j(=\Phi a_j)$ 如果 Φ 是一一映射，即是满映射，且是单映射（即 $a_i \neq a_j$，则 $b_i \neq b_j$），加上条件 $\Phi(a_i O a_j)=\Phi a_i \widetilde{O} \Phi a_j = b_i \widetilde{O} b_j$，则称 Φ 为集合 A，B 间对于运算 O 和 $\widetilde{O}$ 的一种同构映射。这样

可将 A 和 B 及 O 和 $\widetilde{O}$ 看做广义上相同(一回事),也就是知道 B 及 $\widetilde{O}$ 等价于知道 A 及 O,即信息集合 B 及其关系 $\widetilde{O}$ 表征了事物集合 A 及其"运动"(关系 O)。也可以由集合 A,O,Φ 以求得 B 和 $\widetilde{O}$,这样便建立了在理想状况下用信息间关系表征运动的基本表达。在实际情况下,干扰因素非常多,往往找不到同构映射 Φ(科学技术发达程度不够或在原理上无法排除各种干扰),相当于无法得到相应准确的信息,或者是 Φ 不是满映射(相当于不真实信息混入),更不是一一映射(不能由信息集合及其运算准确判断 A 内事物个体及其间相互关系 O),在实际情况下,往往争取到了一个同态映射(即 Φ 并不是满映射,更不是一一映射,仅是映射,如 Φ 是满映射则称同态满映射)。在这种情况下,由"信息"不能准确回归所指称对象("信息"的逆像)和表达它们之间的关系,但人们可进一步利用其他方法进一步补充"信息"而达到目的(即以系统性方法补充运作以达到目的)。概括而言,在理想状态下事物运动形成"信息","信息"表征运动状态,两者之间是一种一一映射关系,这是一个基本规律。

以上说明以信息表征事物某个剖面上的运动关系,下面再延伸讨论由剖面"信息"集成,全面表征运动状态(性质)的情况。每种具体"运动"在不同"剖面"有着不同关系,不同"关系"映射形成不同信息(即 b_i,b_j 及 $\widetilde{O}$),"信息"的总体集成表征具体"运动",即物质存在 $\longleftrightarrow$ 运动存在 $\longleftrightarrow \sum_{i=1}^{n} m_i \longleftrightarrow \sum_{i=1}^{n} I_i$,其中 $\longleftrightarrow$ 表示"等价",m_i 表示运动状态,I_i 表示映射形成的信息,$\sum$ 表示总和。我们还应注意到对同一"运动"剖面,由于表征方法不同(即不同种类的 Φ)会造成 B 集合和关系 $\widetilde{O}$ 的不同类型。如在某地区要获得有无飞机飞行的信息,可以用人眼搜索发现,用声波探测,用雷达波,也可借助热辐射探测,不同方法得到的信息种类不同,都可表征有无飞机飞行这一运动状态。

简要总结信息存在相对性原理所含主要内容:

信息是事物运动状态的表征和描述,有"运动"必伴有信息,由此基础概念而言,"信息"必然存在,不能消失。在具体实际情况下,由于复杂环境,"信息"的"存在"呈现相对性。

"信息"有针对运动状态具体剖面的相对性,不同剖面的"信息"一般不同,"信息"有依靠表征方法(即相对映射和运算关系 $\widetilde{O}$)的相对性。

"信息"在形成和应用过程中(如获取、存储、交换、传输、处理等)会有外部"干扰"介入,使得具体"信息"的真实性、保密性、可用性等发生问题而影响使用,因此,信息的"存在"是相对的。

雷达探测飞机形成飞机飞行信息的实例,理想状态为飞机飞行经"同构映射"形成信息,它可在规定的映射条件下表征飞机运动状态。设:

映射关系 Φ 分为两组(皆为一一映射):

$a_i \xrightarrow{\Phi} b_i$,即飞机与回波间的映射。$\Phi(a_i)=b_i$ 意为利用电磁场发射,形成飞机回波。

$a'_i \xrightarrow{\Phi'} b'_i$,即地理坐标与雷达以接收方式进行空间指向测量,所形成雷达坐标点(时空)

间映射。

A 集合	B 集合
飞机子集：$a_1, a_2, \cdots, a_i, \cdots, a_n$（为时间 t 的函数） 空间子集：$a'_1, a'_2, \cdots, a'_i, \cdots, a'_n$（以大地坐标 X, Y, Z, t 所表征空域中的点，$\circ$ 运算为 a_i 与时空子集发生关系形成飞机的时间空间域的位置：$X_{a_i}(t)$，$Y_{a_i}(t), Z_{a_i}(t)$ 运算关系被定义为集合 A, B 各自子集间元素的相互关系	飞机回波子集：$b_1, b_2, \cdots, b_i, \cdots, b_n$（是雷达时间系 T 的函数） 时空子集：无线电定位装置接收定向测量所形成的时空子集（以雷达为原点的雷达坐标），雷达时间系所共同形成的坐标点：$b'_1, b'_2, \cdots, b'_i, \cdots, b'_n$（是 T 与时延 τ_0 的函数） $\tilde{\circ}$ 运算为 b_i 与 b'_i 集发生作用关系形成“回波”在定位时空域中的位置：$\gamma_{b_i}(T), \theta_{b_i}(T), \varepsilon_{b_i}(T)$。其中：$\gamma_{b_i}(T)$为回波相对定位装置的距离（$\gamma_{b_i}(T)=\frac{c}{2}\tau_0$，$\tau_0$ 为回波接收相对发射时刻的时延，c 为光速）； $\theta_{b_i}(T), \varepsilon_{b_i}(T)$为回波相对定位装置的方位角和高低角 T 为无线电定位系统所定的时间系（与 t 之间无需用相对论时间尺度修正）

$X_{a_i}(t), Y_{a_i}(t), Z_{a_i}(t) \rightarrow \gamma_{b_i}(T), \theta_{b_i}(T), \varepsilon_{b_i}(T)$，具体关系为

$$X_{a_i}(t) - X_0 = X_{iR}(T) = X_{iR}(t)$$

$$X_{a_i}(t) - Y_0 = Y_{iR}(T) = Y_{iR}(t)$$

$$X_{a_i}(t) - Z_0 = Z_{iR}(T) = Z_{iR}(t)$$

在对飞机探测中 T 与 t 之间误差可以忽略不计，其中 X_0, Y_0, Z_0 为无线定位系统的坐标（大地坐标系）。

$X_{a_R}(t), Y_{a_R}(t), Z_{a_R}(t)$为 a'_i 相对于定位系统的直角坐标。

$$X_{iR}(t) = \gamma_{b'_i}(t)\cos\varepsilon_{b'_i}(t)\sin\theta_{b'_i}(t)$$

$$Y_{iR}(t) = \gamma_{b'_i}(t)\cos\varepsilon_{b'_i}(t)\cos\theta_{b'_i}(t)$$

$$Z_{iR}(t) = \gamma_{b'_i}(t)\sin\varepsilon_{b'_i}(t)$$

以下验证两集合中运算及映射关系。

A 集合中飞机子集与时空子集经运算后得出飞机飞行在大地坐标系的瞬时位置：$X_{a_i}(t), Y_{a_i}(t), Z_{a_i}(t)$。

$X_{a_i}(t), Y_{a_i}(t), Z_{a_i}(t)$往 B 集合的映射为组合映射，即有飞机与飞机雷达回波的映射，又有大地坐标点与雷达坐标之间映射，用符号 $\Phi\Phi'$ 表示，由物理实现可得出：$\Phi\Phi'(a_i \circ a'_i) = \Phi(a_{it}) \tilde{\circ} \Phi'(a'_{it})$，表明飞机在大地坐标中飞行可同构或同态映射至雷达探测到飞机并确定飞机在雷达坐标系中位置，如 Φ 及 Φ' 为一一映射，则上述情况被认为是同构映射（B 集合“运算”结果在所给定映射含义可完全表征 A 集合中情况）。

在实际复杂环境下，例如低飞时，有地物反射回波施放假回波干扰，破坏了雷达工作所需得到的同构映射，雷达信息就无法确切得知飞机的运动情况，这就演变为“安全与对抗问题”

(即不构成同构映射)。

4.3.3 广义空间维及时间维信息的有限尺度表征原理

各种具体"信息"存在时间与广义空间中,即"信息"以某种形式与时间、广义空间形成某些"关系"来表征"信息"的存在。将"信息"时空关系在时空域构成信息空间,用$[I,R,S,t]$表示,其中I为"信息"(第二章中将信息表示为四元关系组,可进一步概括为信息空间点关系),R为决定"信息"的时空域关系,S为广义空间域,可扩展为包括第二章所述信息存在的直接特征域,T为时间域,对于不同信息有着不同复杂的关系。总可以概括地得出,信息在信息空间只占有限空间,但又不等于零,用数学语言表示,即信息范数$\| I \|$有$0<\| I \|<\infty$,这就是信息有限尺度原理。

上一条原理实际上阐述了信息与运动的紧密相关性,又同时说明具有差别的可能性,在本原理中将进一步细化说明信息存在形式的一些特征,即由表征角度观察各具体表征运动信息的具体形式在广义空间所占大小,以及时间维中所占长度都是有限的。

如有一个永恒的平稳运动,其信息表征是有限的。因为它是平稳的、不变化的,所以表征这个运动信息的有限尺度便够了。

对于一些"运动"其涵盖范围越广,则其内涵(共同的本质属性)就越少,作为其表征"信息",在时空内占位越有限。

对于具体运动过程,其时间、空间范围都是有限度的,作为其表征状态的信息在空间和时间维中只有有限尺度。

信息在时间维及广义空间维的有限尺度原理,在哲学上与具体事物各具特殊性原理相匹配。如果信息在空间维和时间维非有限尺度,占满了广义空间和时间维,信息间互相无法区别,则事物间无法区别,特殊性无法谈起。在信息安全领域的应用现实中,在本原理基础上,可将信息在时间、空间域内进行变换和处理以满足对抗需要。如信息隐藏中常用的低截获概率信号,便是利用信息、信号在广义空间和时间维的小体积难被对方发现截获的原理。

4.3.4 在共道基础上反其道而行之(相反相成)原理

矛盾对立统一律是一切事物运动的基本规律。人们都承认矛盾的对立斗争是促使事物发展的根本因素,承认矛盾对立斗争是第一性的同时,不能忽视与对立同时存在"统一"的重要性。一对矛盾是对立的同时又是统一的,并呈现相反相成性质。如作战双方是极端的"对立",但双方都要争夺战争胜利,都不能让对方获胜,这一点双方是共同的,没有"败"就没有"胜",这是统一的表现。战争双方内因互为对方外因,外因可转为内因,以上所述事实都证明矛盾的"对立"与"统一"相反相成辩证关系。在信息安全对抗领域,"共道"基础上反其道而行之相反

相成原理，是矛盾对立统一律在本领域的一个重要转化和体现（在此只称原理而不称定律是希望进一步验证）。现分几点加以说明：首先说明“共道”与“逆道”间的对立统一，整体而言共道——共其道而行之，逆道——反其道而行之，它们是一对立统一范畴，没有共道就没有逆道，反之也一样，两者对立统一相反相成。“道”在此指原理、方法、规律、规则、机理等（有广泛灵活含义），“共其道”义为承认、遵从某些规则、机理等，在“对抗”场合则是承认、遵守对方的机理、规则。这意味着承认对方存在然后选择利用对方这些机理、规则中的一部分为达到己方目的做准备。不如此就无法与对方接触联系发生关系，也就谈不上通过行动达到自己目的，如通信领域的干扰反干扰，对抗中干扰方需知道对方通信的主要参数、频率调制方式，反干扰方应知道干扰的主要方式等都属于“共其道”的内容，由此可明显看出“共其道”是基础和前提，也是对抗规律的一部分，在信息安全对抗领域以“反其道而行之”为核心的“逆道”阶段是对抗的主要阶段，是用反对对方的“道”（即破坏其“道”从而破坏行动的效果）以达到己方对抗目的的机理、措施、方法的总成。“反其道而行之”有多重含义，可以认为是原理也可以认为是方法、机理等。“反其道而行之”的具体实施方法多种多样要依照具体情况而定，它的实施除了依靠科学规律、技术方法外更重要的是当事人根据实际情况发挥智慧，对科学原理和技术方法进行有效选择。“共其道基础上，反其道而行之相反相成”原理是信息安全对抗双方都要广泛运用的基本原理，以下将着重论述“反其道而行之相反相成”内涵的本源性及规律性，先介绍其时空多层次交织普适特性。

发生的“信息安全对抗”往往是具有尖锐对抗特性的一个复杂事件，是由对抗双方当事人根据双方的具体情况及对抗要达到的目的，经思考后选择了“对抗”所需方法和措施，在行动中互相作用和影响形成对抗过程。将上述斗争过程用一系列相互作用的“关系”来表征，运用“共道基础上反其道而行之”原理研究信息安全对抗问题，可转化为运用此规律研究一组关系集合中复杂的动态关系的相互作用（包括建立新关系），具体的信息安全对抗过程都是在时间和广义空间维中细化展开，运用“共道基础上反其道而行之”原理时应该注意在众多时间片段、子阶段、阶段，空间剖面、子层次中多种动态交织关系中都有所体现，这是在应用“规律”时应该注意到的一个重要问题，只有充分在多阶段、多层次的时空维交织关系中辩证地利用本原理，才能充分发挥它的作用，而不至于引起失误。以下结合应用不同的“对抗”剖面，简要阐述“相反相成”蕴涵的各种内涵。

“相反相成”有多种辩证含义。矛盾对立面相互依存才能使矛盾存在，这与通常所说矛盾统一性有相似之处。深层次多种辩证的相反相成机理表现在对立面互相向对方转换，借对方的力帮助自己进行对抗等，都是事物矛盾时空运动复杂性多层次间“正”“反”并存斗争，在矛盾对立统一律支配下产生的辩证的矛盾斗争运动过程。它在信息安全对抗过程中具有重要意义，如双方对抗中都考虑避免自己的对抗措施反而被对方所利用，以及考虑如何尽力找出对方对抗措施中对己方有利因素加以利用，这样的对抗对方的措施都属于“相反相成”；还有在复杂情况下，相关对立因素的其他剖面呈现重要共同利益，则对立双方可能放弃对抗，追求共同利

益而达到共赢，这是一种广义的“相反相成”。“相反相成”有多种形式，举例说明。

设攻击一方为 A 方，A 方与 B 方“共道”而行是为了自己“逆其道而行之”创立条件，“共其道”是条件，“逆其道”是目的，“条件”与“目的”以相反相成方式互相依存（这是对立方交叉态相反相成）。

当 A 方在获得 B 方机理、规则、管理办法等过程中。碰到困难时（即 B 方对自己的机理采取保密保护措施）就要采取一些强制手段以获得所需的对方之道，这就是 A 方以逆道的方式达到“共其道而行之”，这是“共道”过程中嵌入的“逆道”子过程，是主－子层次中交织的相反相成。同样也会在“逆道”过程中需要嵌入“共道”子过程的情况发生（这是对立方交叉间接层次的动态转换相反相成）。

对双方交互对抗而言，“相反相成”可表征各种对立面之间“关联转换”，试举例说明。

设 A 方为主动攻击方。如双方进行信息安全对抗，其过程总是“共道”—“逆道”—“共道”……在时间、空间中关联转换。A 方由“共道”转成反其道而行之攻击，则 B 方先承认攻击存在（与 A 方共其道），分析清楚后，然后再进行反其道而行之，即采取措施对抗 A 方（反反其道），这时如果 B 方措施奏效，则 A 方应及时分析 B 方的反攻击措施，然后调整自己的攻击方法再次发动攻击，使攻击再次生效。这个过程由多个“转换”所组成，即自己有一方步骤、阶段间相反相成转换，也有双方斗争中交织地“共道”、“逆道”间动态转换，正是这些对立的相反相成构成对抗过程。

在 A 方对 B 方实施攻击时（A 反 B 的道而行），必须有攻击的道，即有具体原理方法，然后才能构成攻击行为，按技术核心措施转移原理（4.4.3 小节），A 方必须具备实施攻击的一些条件如充分条件、必要条件、充要条件，这些条件也是一些“道”构成条件的规律，B 方则可利用这些必定需要的条件，对这些条件进行反其道而行之，即破坏实施攻击的充要条件、必要条件，从而破坏攻击。这是一种深入的借助“攻击”依靠条件实施反攻击的办法，也是一种深层次交叉利用对方动态间接性质的“相反相成”。

还有另外一种深层次相反相成，即利用对方实行攻击中必同时付出的“代价”（包括各种副作用）进行反对方的行动而达到己方的反攻击目的，这也可理解为借对方的“力”进行反对方的一种方法。借对方的“力”的前提是承认对方存在，即“共其道”，这是一种巧妙的“相反相成”，这类相反相成有多种具体的实现形式，现列出一例：如 A 方作战飞机为了干扰对方雷达对自己的探测发现，可在飞机上装有自卫式杂波干扰机，从而起到对抗对方探测发现自己的作用。但副作用是干扰源和飞机同一位置，因此对方火控雷达可不采用反干扰办法，而是采用在角度上跟踪干扰源的办法（干扰越强就越容易进行），这样连续地获得了飞机的方位角、高低角数据，再结合使用控制导弹的三点法制导，便可利用导弹对飞机进行攻击。这个例子实际上是在“共道基础上反其道而行之”原理中，以相反相成核心理念所构成反攻击的有效方法。以上由“相反相成”所形成的对抗过程，以及应用它构成对抗的有效方法，说明了“在共道基础上反其道而行之相反相成”内含的本源规律性故可被称为“原理”。

结合本小节前边讨论，可以进一步指出由于“在共道基础上，反其道而行之相反相成”原理，是根据矛盾对立统一律在信息安全对抗领域推演得出，它具有基础核心作用，可广泛应用，与基础层次对抗原理(4.2 节)及系统层次对抗原理(4.3 节)密切结合发挥作用，如上例也可作为争夺制对抗信息权及快速响应原理(4.3.6 小节)间接对抗原理的应用例子，同时也说明依据相反相成原理可演绎出间接对抗原理。以上不同性质“相反相成”的说明和例子除了表达该原理应用场合外还可作为“举一反三”的应用方法供实际采用。总之，相反于“相互相成”的“相反相成”，也是一种广泛应用辩证思维的方式和方法。中国古代哲人就此早已提出多条哲理，如“祸兮福所倚，福兮祸所伏”，“将欲翕之必固张之，将欲弱之必固强之，将欲废之必固举之，欲将取之必固予之”等，本小节所提出的“原理”，实际上是上述辩证思维方式在信息安全领域的一种应用体现。

在本小节结束之际，本文指出“共道基础上反其道而行之相反相成”原理虽然起核心作用，但不是包办一切的，在具体场合知晓具体的“道”才能“共其道”或“逆其道”，以及进一步做到相反相成。感知对方的“道”有时并不轻而易举，也要付出一定“代价”。下一重要步骤是选择己方针对性的规律方法等。

4.3.5　共其道而行之相成相反原理

中国古代哲人曾多次论及“正”“反”间辩证转化原理，如老子《道德经》曾论曰，祸兮福所倚，福兮祸所伏。说明“正”“反”相互辩证转换哲理，信息安全对抗双方可看做互为“正”“反”，很多哲理的延伸应用可以形成信息安全对抗领域原理。在 4.3.4 小节叙述“以反为主相反相成进行对抗”原理。在本小节中，我们提出了形式上以对方共道顺向为主，实质上达到反向对抗(逆道)效果的原理，称为共其道而行之相成相反原理。共其道而行之达到相反的效果，有多种原因和方法，概括而言是来源哲学规律所规定的一切机理所形成的机能效果都只具有有限性，非绝对的相对性(时空域呈相对性)。外加“信息安全对抗”多是复杂非确定性动态变化事件，更加重了对抗措施机能相对性、有效性的体现。共其道而行之相成相反原理就是在上述规律导引下结合中国哲学智慧(老子所提出)，“将欲翕之必固张之，将欲弱之必固强之，将欲废之必固举之，欲将取之必固予之”，在信息安全对抗领域所提出的一种原理应用，本原理在应用中常具有灵活多种双方“成”与“反”的内涵，并相互结合构成对抗思路与方法，举例说明。

在信息安全对抗中，攻击方经常组织多层次攻击，其中佯攻往往吸引对方的注意力，以掩盖主攻易于成功，而反攻击方识破佯攻计谋时往往也佯攻以吸引对方主攻早日出现，然后痛击之。

对于公开服务的信息系统的攻击，用过量“服务”请求，以使信息系统瘫痪，这是一种常用的依相成相反原理的信息攻击方法。

信息对抗双方往往需要互相收集对方信息，故意放出重要反向假信息配之以假动作，错误

诱导对方是相成相反的方法。

在信息系统中设置假枢纽点吸引对方攻击也是一种相成相反方法。

“在共道基础上,反其道而行之相反相成”规律中“在共道基础”是“反其道而行之”前提条件,也可看做是一种相成相反。

总结 4.3.4 和 4.3.5 所述两条原理,具体应用时有多种组成,可概括其组成框架为:在矛盾对立统一规律作用下某方在某层次某剖面对某事物在某阶段相成;某方在某层次某剖面在某阶段对某事物相反。上述各例都可由具体状态组成具体的“相反相成”或“相成相反”。

4.3.6 争夺制对抗信息权及快速建立系统对策响应原理

本原理在基础性原理系中的作用是,在“共道基础上反其道而行之”相反相成原理的导引下往应用层延伸,从而提出对抗过程中双方斗争夺其焦点的规律,进而构成基础性原理框架。

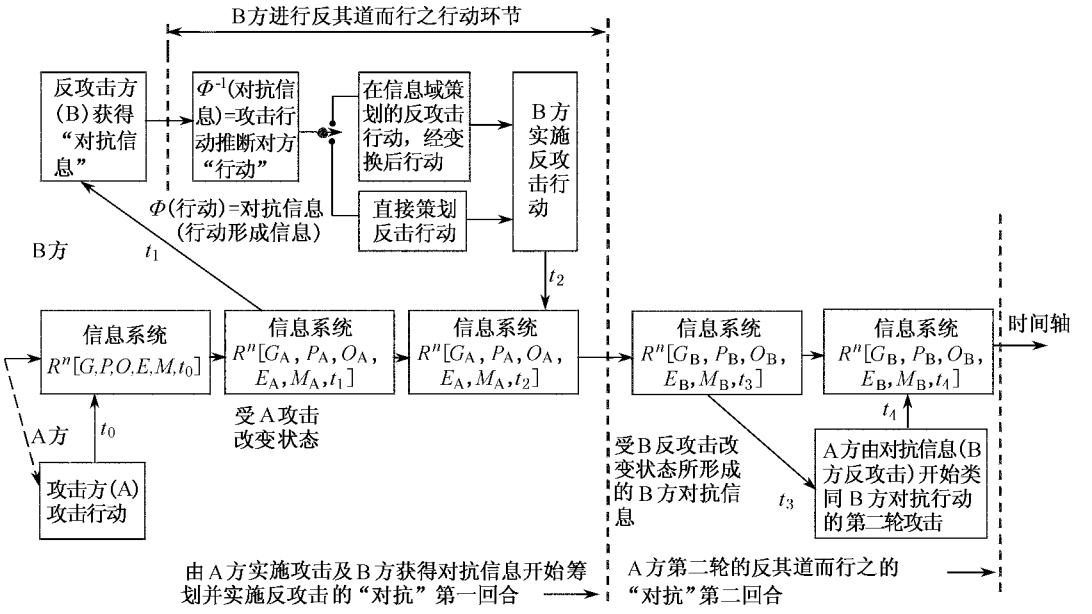
首先定义“对抗信息”。根据信息的定义和信息存在相对性原理,双方在对抗过程所采取的任何行动,必定伴随着产生“信息”,这种“信息”称为“对抗信息”。它对双方都很重要,只有通过它才能判断对方攻击行动的“道”,进而为反应对抗进行反其道而行之提供基础,否则无法反其道而行之更不要说相反相成了,“对抗信息”在时空域中包含对立统一性质,如双方对自己行动所形成的“对抗信息”希望对对方进行隐藏,对方则希望破除“隐藏”而得到它。除了在围绕“对抗信息”隐藏与反隐藏体现在空间的对立斗争外,在时间域中也存在着“抢先”“尽早”意义上的斗争,同样具有重要性。时空交织双方形成了复杂的“对抗信息”斗争,成为信息安全对抗双方斗争过程第一回合的前沿焦点,并对其胜负起重要作用。

在围绕“对抗信息”所展开的双方斗争是复杂的空、时域的斗争,除了举例所说明的最基本双方对抗因素外还有多种时空交织、相交相成的斗争方式,要依据对抗斗争具体情况而定,如佯攻的对抗信息就不应对对方隐藏而恰是相反等。围绕“对抗信息”在对抗过程中影响斗争结果的核心规律是,在“对抗”环境中要取得对抗信息为己方主动利用的优势,以便后续的反其道而行之及“建立系统对策响应”,下面将重点表征围绕“对抗信息”的斗争结合“反其道而行之”原理进行分析,如图 4.1 所示为原理的框架表示。

在框图中,双方获得对抗信息的时间坐标用,t_1,t_3 表示,实施攻击时间用 t_0,t_2,t_4 表示信息系统响应对抗行动用 $R^n[G,P,O,E,M,t]$ 表示,双方都力争在对方实施对抗行动后立刻获得对抗信息,即 t_3 尽量接近 t_0,滞后越少越好,但实际上可能不能直接由对方攻击行动感知对抗信息,而需等待信息系统对攻击行动做出反应,由信息系统的状态改变才得到对抗信息,这就更有一段时间滞后。

Φ(行动)=对抗信息,Φ 为映射符号,也可理解为算子,意为“行动”产生对抗信息。

Φ^{-1}(对抗信息)=攻击行动的企图,表示由对抗判断对方攻击之道,依靠科学技术知识,也依靠局中人的智慧和能力。



4.1　争夺制对抗信息权及快速建立系统对策响应原理框图

以开关形式及两个框图表示两类进行“反其道而行之”的方式，一类是在信息领域即就对抗信息进而产生“反其道而行之”的方法，然后变换至行动域形成实施方法；另外一类是根据对抗信息反演的攻击方法，直接在行动域策划对抗行动，至于采用哪种方式，要根据实际情况而定（属于联想、关系反演等思维方法领域内的各种具体方法）。

框图中只表示两个对抗回合（A 攻击、B 反攻击、A 再次攻击……）实际情况可能是多回合展开。

$R^n[G,P,O,E,M,t]$表示在某信息系统可响应双方对抗行动的动态六元组关系（在第三章中已提到并加以说明过）。在下节中建立“共道—逆道”对抗模型时将再次讨论运用。

在框图获得“对抗信息”过程中蕴涵“反其道而行之相反相成”原理。信息系统以“信息”为运行媒介，系统中充满了“信息”，如何感知“对抗信息”，其根源在于它“与众不同”，即其“逆道”特征的存在。如“对抗信息”的存在和运行不违反“道”（预定的规则机理）是难于感知的。总之，对抗信息的获得与利用蕴涵了激烈对抗与 4.3.4 小节（在共道基础上反其道而行之相反相成原理）与 4.3.5 小节（共其道而行之相成相反原理）紧密结合着。

4.4　系统层次对抗原理

本节结合信息系统结构、功能和动态运行的基本技术原理，给出一些系统层次的对抗原

理，暂时由五条原理组成。需要特别强调的是，在信息安全对抗问题的运行斗争中，基础层次和系统层次原理在应用中，你中有我，我中有你，往往交织相辅相成地起作用，而不是单条孤立地起作用，重要的是利用这些原理观察、分析掌握问题的本征性质，进而解决问题。

4.4.1 攻击方全局占主动地位，被攻击方居被动地位及局部争取主动全局获胜原理

本原理说明，发动攻击方全局占主动地位，理论上它可以在任何时间、以任何攻击方法、对任何信息系统及任何部位进行攻击，攻击准备工作可以隐藏进行。被攻击方在这个意义上处于被动状态，这是不可变更的，被攻击方所能做的是在全局被动下争取局部主动（也包括4.3.6节原理的结合应用）。

争取局部主动主要措施有：① 尽可能隐藏重要信息，例如，在重要时刻对重要信息节点的信息传输与交流进行安全状态控制，使的不泄露。② 事前不断分析己方信息系统在对抗环境下可能遭受攻击的漏洞，事先预定可能遭攻击的系统性补救方案。③ 动态监控系统运行，快速捕捉攻击信息并进行分析，科学决策并快速采取抗攻击有效措施。④ 在采取上述措施同时，应综合运筹，在对抗信息斗争中争取主动权，例如，过早提前采取措施会因此暴露重要对抗信息而打草惊蛇终被蛇咬。⑤ 利用假信息设置陷阱诱使攻击方发动攻击而加以灭杀，也是一种斗争办法，反之这时攻击方可用将计就计的办法进行斗争。总之，斗争方法有多种多样，但每种都不是“绝对”的，要因地制宜正确应用。在反攻击方全局处被动态势下科学地最大程度争取主动。以达到“相反相成”，争取全局获胜。

4.4.2 信息安全问题置于信息系统功能顶层综合运筹原理

信息安全问题虽是个非常重要的问题，应该十分重视。但值得提出注意的是，作为一个信息系统的功能，总体而言是获得信息并利用信息为人服务，安全功能虽然是功能中非常重要的部分，但究竟不是全部功能而是只起保证服务作用。对待安全功能应根据具体情况，科学处理、综合运筹，并置于恰当的“度”范围内，更重要的是，本原理提示人们，将信息安全这一重要问题融入整个系统，利用系统理论及信息安全对抗原理综合运筹，恰当地在系统功能体系中（安全性为其中的一）妥善处理各分项“度”的相互关系，以使信息系统充分发挥功能，同时不发生大的功能失调。如商用公钥制 RSA 1024 位密码是安全的，但因编、解码都是大素数的高阶幂次，运算耗时很多，影响信息传输速度而不能随意采用，一般只用于传递密钥，这就是进行综合不能偏废考虑的明显例子。

4.4.3　技术核心措施转移构成串行链结构，从而形成“脆弱性”原理

每一种安全措施在面对达“目的”实施的技术措施中，即由达目的的直接措施出发逐步落实效果过程中，必然遵照从技术核心环节逐次转移直至普通技术为止这一规律，从而形成串行结构链规律。技术核心逐次转移规律来自于一条普遍原理，即在具体实施过程必由构建充要条件做起。任何技术的实施都是相对有条件的发挥作用，必依赖于其充要条件的建立，而“条件”再作为一个事物又不可缺少地依赖其所需条件的建立（条件的条件），从而形成以条件递推的转移串行链结构（直至不需特别建立条件的普通水平技术为止）。

串行链结构具有脆弱环节主宰全链安全性能以及在同等水平情况下应尽量减少串联环节数的两条原理。例如，某安全措施链由成功概率为 0.3，0.8，0.9，0.9，0.9 五个串行环节组成，则安全措施链的成功概率为 0.174，如最脆弱环节增为 0.5，则全链的概率升为 0.437，可见全局性能由薄弱环节所主宰。

随着社会不断进步，所谓不需要特殊关照的状况也在不断变化，但这条系统性原理却依然适用。只是形成原来需要特别关照的具体条件会有所变化。例如，利用密码进行信息内容隐藏，随着密码发展和不断选用性能优良的密码，在应用中必定要有密钥管理中心，负责密码的方便、可靠、安全运行，密码中心的运行还需要进行管理（因一旦密码中心出问题则后果非常严重），密码中心的成立需要有对密码中心的认证管理工作。再向应用环节延伸，申请环节也是重要的，它又可分解为一系列步骤，直到个人身份有效证件的登记、检验，在身份验证容易伪造情况下对身份证还需要不断改进验证。

4.4.4　变换、对称与不对称性变换应用原理

“关系”是一非常重要的基础概念，因为普遍的事物间相互关联、相互影响从而形成“关系”，“关系”一定意义上表征事物运动，代表事物存在。“变换”可以指相互作用的变换，可以认为是事物属性的“表征”由一种方式向另一种转变，也可认为是关系间的变换，即变换关系。例如，信号的傅里叶变换对是将信号属性在时间及频率域间进行变换，傅里叶变换对本身也有固定明确的关系，在数学上可将变换看做一种映射，在思维方法中将进行变换看做是一种“化归”。“变换”已知有许多种类，并仍在不断研究发现各种新的变换和新“变换”的利用，一些常用的重要变换有：同态、同构变换，对称不对称变换等（同态与同构变换在信息领域的应用在 4.3.2 小节，即“信息存在相对性原理”中已举例说明），本小节着重讨论对称与不对称变换的基本概念与应用原理。

对称的定义为某事物的某性质 A，对某基准 B 进行某种变换 C，如性质 A 经变换后不变化，则称性质 A 在变换 C 下对于基准 B 是对称的，否则称为不对称，并称 C 为关于性质 A 以 B 为基准的对称变换。

例如一个圆形图形对于圆心作各种旋转，图形不变化，则称圆对圆心而言是旋转对称的，椭圆只对轴或短轴作 $180°$翻转是对称的。

对称与不对称是事物运动的一种基本特性，也是作为研究具体事物特殊存在性的重要特征的一，上述参考轴(点)是广义的。例如，设某一时刻为时间维参考点，运动着的系统对时间参考点不对称，它就是进化系统。上述变换可以是一组变换，也可以是一对正反变换。如傅里叶正反变换，信号处理中的扩谱与解扩等都是一对正反变换，对某类特设性质信号实现正反变换形成的对称变换，而对不具有某种特设性质的信号经反变换时则明显衰减，这是利用信号的某种特殊性和对称变换，进行信号的保持而削弱其他信号的常用方法。这种原理也可用于信息安全对抗领域，即利用对称变换保持自己功能，同时利用对方不具备对称变换条件以削弱对方达到对抗制胜目的，现进一步用图 4.2 说明如下。

如 S 为信号，$(S_1T_1)T_2=S_1$ 意味着 T_1T_2 对信号对称，同时 ST_1 使信号频谱扩展(如 T_1 倍)，当干扰信号 I 内不蕴涵 T_1S_1 所具有的性质，经 T_2 变换后信号因 T_1T_2 具备对称性质可实现，输出 $S_0=S_1$，同时可做到干扰输出 $I_0=IT_2$，在 I 为干扰信号进行信息攻击情况下，利用上述对称变换概念可对干扰信号进行削弱。

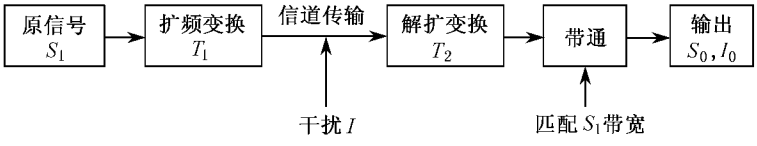


图 4.2　信道传输中利用干扰的不对称变换提高抗干扰效果的示意图(理论上 $S_0=S_1$，$I_0=IT_2$)

在密码应用领域，利用密钥对信息进行加密和解密(密钥可以不只是一个)，是原信息的一种对称变换，而不知密钥则无法完成对称变换，就无法得知原信息，从而保密信息内容。在信息安全对抗领域，还可利用广义对称和不对称变换提高某方面的对抗性能，如选择对象的对抗性能表现在某性能指标 A 上，A 数值高则抗攻击性能强，其他主要功能指标用 S 表示，在两类选择对象 F_1、F_2 中进行选择时，选择原理应是经选择后功能保持但对抗弱者将被淘汰。

即 $S_{F_1}=S_{F_2}$，$A_{F_2}>A_{F_1}$，可看做是一种含广义的对称与不对称变换相结合的选择，目的是有利于抗攻击，对称性体现在不同的措施选择中具有相同无变化的功能指标，不对称性体现在选择抗干扰性能较好者。

4.4.5　对抗过程多层次、多剖面动态组合对抗特性下间接对抗等价原理

设系统构成可划分由层次为 $L_0, L_1, L_2, \cdots, L_n$ 的结构所集成，且 $L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_n$，如在 L_i 层子系统受到信息攻击，采取某措施时可允许在 L_i 层性能有所下降，但支持了在 L_{i+j} 层采取有效措施，使得在高层次的对抗获胜，从而在更大范围获胜。因此，对抗一方绕开某层次的直接对抗而选择更高更核心层进行更有效的间接式对抗称为间接对抗等价原理。

例如，某防空武器系统由火控系统雷达、计算机及火力系统（高射炮防空导弹）所组成。设火控雷达受干扰，正常信息探测受影响（L_2），但可在 L_3 目标截获、跟踪层次（是 L_2 的后续层次）提高性能（如缩短探测－截获过程所需时间，缩短稳定跟踪过渡时间等），使得在全武器系统层次对敌机流的毁伤概率（顶层功能）保持不降低，还可能有所增加。理由如下：干扰强度 $I\propto\frac{1}{R^2}$，回波信号强度 $S\propto\frac{1}{R^4}$，其中 R 为探测距离。$\frac{S}{I}\propto\frac{1}{R^2}$，如 R 降低为原来的 $1/2$，S/I 比原先值提高到 4 倍，原来探测不到的飞机回波信号便可以探测到，这时虽然会因探测距离的降低（相当于敌机在火力圈内逗留时间的降低）而毁伤也将有所降低，但因雷达截获时间变短而形成全武器系统射击反应时间降低，它可更有效提高对敌机的毁伤概率，综合正负效果后对敌机毁伤效率反而有所提高。较详细分析见有关随机服务理论的文献，从本例中可看出多层次相反相成的机理。

雷达被干扰不能在正常距离上探测目标，这是攻击方的成功，压缩探测距离是我方的一种退守，加之以提高快速截获目标的能力，就为全武器系统以更高的毁伤概率，毁伤攻击飞机提供条件，这是在更高层次中的“成”（某层次的退而全局性的进，不同层次中进退并不对称）。

4.5　“共道”—“逆道”对抗机理博弈模型

4.5.1　建模基本概念

建立模型解决问题是人们利用思维能力对欲解决问题进行抽象、概括，然后进行“化归”的一个最常用环节，它同时也可看做一种映射，是人对运动着的事物，通过掌握其信息及本质特征，经浓缩后映射、建立表征事物运动的本质性关系（称之为模型）。

根据事物实际情况，简单事物可对其本质关系直接建立一个模型便够用，复杂事物有着多层次、多剖面的动态关系，需要建立模型集合，由多层次、多剖面的分模型组合而成。很多情况下需要利用模型研究事物动态运动，此时应在模型的结构中融入表征运动特征的动力学组分，同时往往将动态过程划分为子过程、子阶段进行模型分析。对于复杂事物的模型分析，往往是在时间、空间维度上建立子模型并利用这些模型进行事物运动的分项及综合集成研究。利用模型研究事物运动，虽然可简化并集中于重点方面，但建模和利用模型进行综合研究往往仍很复杂和困难，尚无成套系统性通用的有效方法可提供，只能根据具体场合因地制宜构建模型和寻找研究方法，因此带有很强的技巧性。

根据事物运动机理、规律建立的模型，一般称为物理模型（并不仅限于物理学领域）。依照化学、生物学等原理建立的机理规律组合，也广义称物理模型，这里的“物理”是广义，指事物存在运动的“理”。

将待研究问题高度抽象概括构成以数学概念、理论、方法等为基础的一组数学关系（或称

数学结构),称为数学模型。

此外还有以部分实体混合组成模型的半实物模型等,实际常常是以研究问题、解决问题为目的组成模型。例如可先根据机理建立物理模型,其中的一些相互关系是利用数学建立的,分析问题用数学方法等,构成各种混合模型。

由以上的简要讨论可明显看出,对一个问题建立模型决不能要求唯一性,可能存在多种多样的模型。关键在于:① 模型涵盖了要解决问题的本质性关系(如遗漏本质问题则模型就失去意义);② 模型要能起有效解决关键性问题的作用;③ 模型在表征本质前提下力求简单,简单中蕴涵了巧妙,这实际是将问题进行"化归"的一种模式。

对于复杂问题,本质特点是"复杂"。模型虽力求简单以求取得结果,也只能是突出要点前提下的相对性简单,同时存在"简单"是否"恰当"的问题。另外由于大部分场合是通过模型求解未知问题(少部分是归纳和总结问题),对于未知问题而建立模型,模型的正确性在理论上是不可能达到的,模型理性的"正确"与"未知"内含逻辑矛盾,所以模型存在是否正确和恰当问题,要在实践中加以验证及反馈修正以提高其正确性。验证模型可首先由模型的约束条件和前提条件与所研究实际问题的贴合性与真实性入手,如遗漏了重要的前提条件和约束条件则根据模型所得出的结论,将不具有重要意义甚至起误导作用。对一个复杂问题的模型,虽然是经过对问题原型化简浓缩抽象后所得出,但仍会很复杂,体现在多变量的非线性交织、时变特性等,对这类模型的求解,往往需要进一步利用计算机进行数值模拟计算,实际上模拟计算现已成为人类认识实践中的重要组成部分,定会进一步发展和被利用。

4.5.2 "共道"—"逆道"对抗机理博弈模型

信息安全对抗领域包括了无数具体问题,各不同具体问题,有不同矛盾,也就有不同斗争机制,就其共性和基本性而言,建立"共道"—"逆道"对抗机制的博弈模型是一个基本模型,也可以说是一个表述对抗的框架,它要根据实际情况充入具体内容,也可进行剪裁。模型构成的根据是信息安全对抗双方斗争过程,必遵守矛盾的对立统一律,将矛盾对立统一斗争相反相成作用对应到"共道"、"逆道"环节而构建的,模型可以用做过程后的总结分析,也可在对抗前用于运筹决策,制定措施方法。

"道",源出于老子道德经,是其中的核心概念。在此作规律、秩序、机制、原理等理解,"共道"是遵循共同原理机制、秩序、机制、原理之意,"逆道"是相逆对方的道(在 4.3.4(在共道基础上反其道而行之相反相成原理)小节已有说明)。应强调指出在一个信息系统中"道"是一个集合,一般情况下内容很多(即共道集合内元素很多),同样"逆道"集合内元素也很多。在建立模型中的"共道",对攻击方是指欲达到某攻击目的所需要的对方"道"集合中的元素,对其选择作为进行攻击的部分前提条件,它很可能不只是一个元素而是多个元素。"共道"是"道"集合

一个子集，“逆道Ⅰ”是完成攻击破坏对方的“道”的必要条件集合。“逆道Ⅱ”则是在前述必要条件下完成攻击的充分条件集合，对反击方而言，在“共道”环节中应感知对方建立的“共道”集合，而在“逆道Ⅰ”环节中，则是尽快感知对方的“逆道”攻击行动，并快速做出反攻击响应，为反攻击建立“逆道”。以上是分解为单方面动作来解释“共其道”的含义，在实际对抗中双方“共道”“逆道”措施会多层次、多次相互交织使用（如逆道环节中嵌入共道子环节），并常以相反相成方式起作用（在4.3.4小节已有阐述）。总之，“共道”、“逆道”措施是对抗过程中对抗双方皆必具有的共性特征，用此共性特征组成“共道”、“逆道”斗争节点，进而构成2～3级串联模型，可以用其表述对抗过程。

在第三章提出对抗过程表示为$R^{n}[G,P,O,E,M,t]$的六元素关系组合，将融入模型各环节中充实模型的功能，并完善其作用。

一、信息安全对抗双方基于“共道”、“逆道”为核心特征的博弈简要过程图

由攻击方的攻击目的，反攻击方的信息系统安全性能分析及预测为起始步骤，以“共道”、“逆道”为核心环节，双方博弈对抗的过程简示图如图4.3所示。

现将过程的关键点解释如下：

· 双方对抗的启动点来源于攻击方的攻击目的及后续攻击方案、制定攻击主要方法步骤等，信息系统的运行方（反攻击方）对对方攻击行动，开始处于被动局势，所能做的积极措施仅是对信息系统安全弱点的预先分析，对付弱点引发攻击的措施预案等。

· 在对抗过程中双方的对抗行动都必然伴有与之相应的信息，这类特殊信息称为“对抗信息”，它是连接信息安全对抗双方形成对抗过程的基本要素，对双方都很重要，尤其是反攻击方，它在对发动攻击者而言总体上处于被动态势。尽早获得对抗信息是后续过程中争取主动的核心要素，由此引出时间维中双方的争夺：攻击方要争取攻击行动的突然性，以获得更强攻击效果，同样反攻击方快速通过对抗信息正确感知对方攻击，并快速采取有效反击措施以应对攻击，这就是双方都期望获胜而争取时间和采取措施进行斗争。在一个对抗过程中，有多次上述你来我往的斗争回合。（在对抗过程中的框图，我们用响应综合时间来定量表征时间指标）。

· 双方对抗过程是一个又连续又间断的激烈斗争过程，它的生成、持续、阶段性地一定结局，除了受科学规律和原理支配外，博弈双方在复杂多变环境中，发挥智慧科学地运用谋略非常重要，而谋略是高素质人才发挥主观能动性的一种集中表现。

· 双方的对抗遵循本章以前各节所述原理，并运用智慧以图取得己方胜利的过程可概括为图4.3所示。相互关系的三个串联环节，即“共道”环节、“逆道Ⅰ”环节及“逆道Ⅱ”环节，其中“逆道Ⅰ”环节作为“逆道Ⅱ”环节的准备环节，当攻击方由“共道”环节完成了准备工作，并能直接进行攻击（进入“逆道Ⅱ”环节）情况下，也可能省略“逆道Ⅰ”环节。

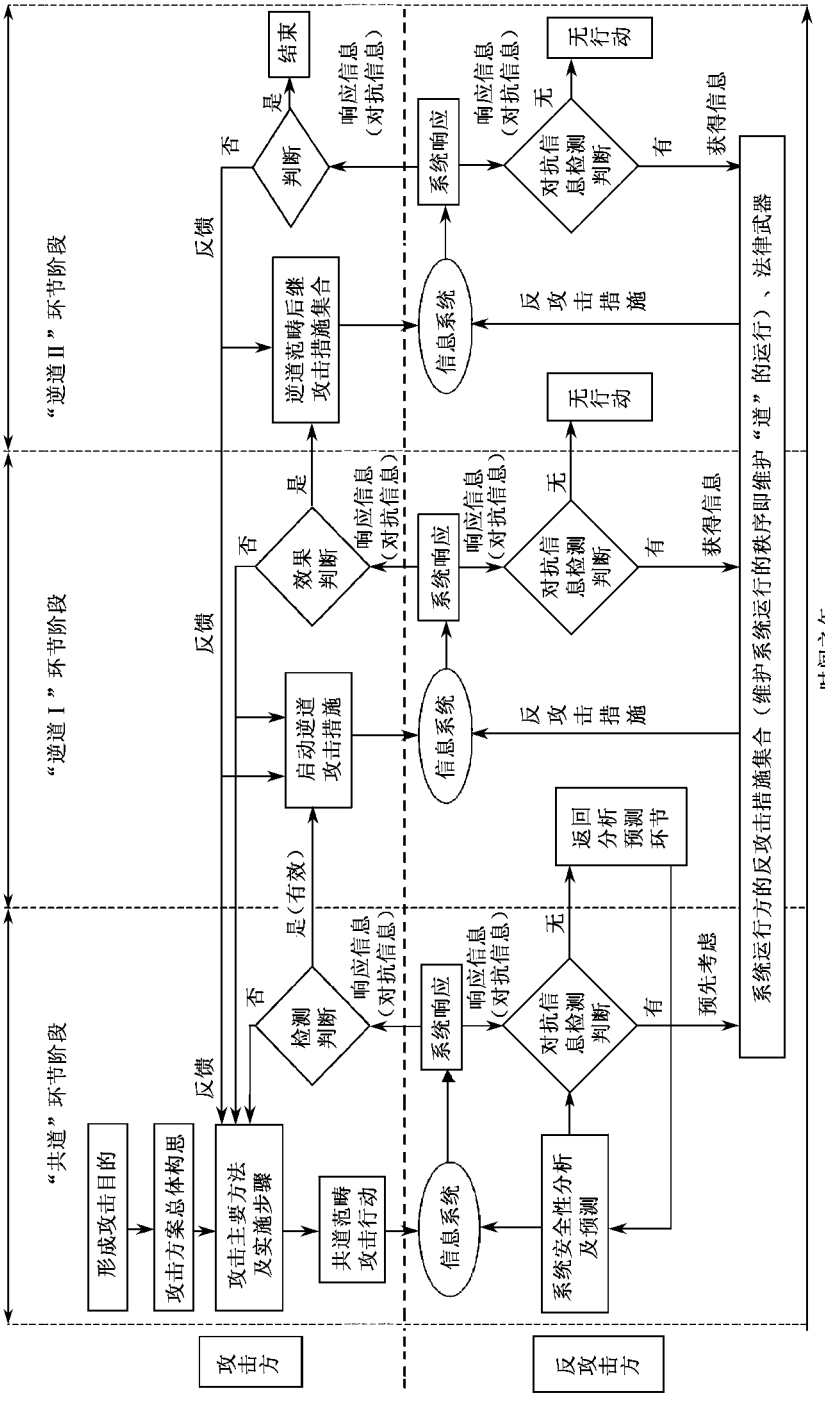


图 4.3　信息对抗过程三环节基本模型

· 在对抗过程中双方都有可能因受挫折回到以前环节，从而重新布置对抗措施，发生这种情况在框图中用反馈线表示。

· 框图起基础表征作用，它可以叠套、多层次使用；可以表示一个对抗过程、子过程也可以用以表征一个斗争环节（如逆道环节）的内部进一步展开（结合例子说明）等。

二、基于关系六元组 $R^n[G,P,O,E,M,t]$ 的“共道”—“逆道”对抗机理博弈模型

在上小节将对抗博弈过程划分为三个基础阶段（“共道”环节阶段、“逆道Ⅰ”环节阶段及“逆道Ⅱ”环节阶段），并进一步将三个阶段展开为三个动态演化对抗关系集合的串联节点（即“共道”、“逆道Ⅰ”、“逆道Ⅱ”对抗关系集合组成的节点），并称为“共道—逆道”对抗机理博弈模型，如图 4.4 所示。

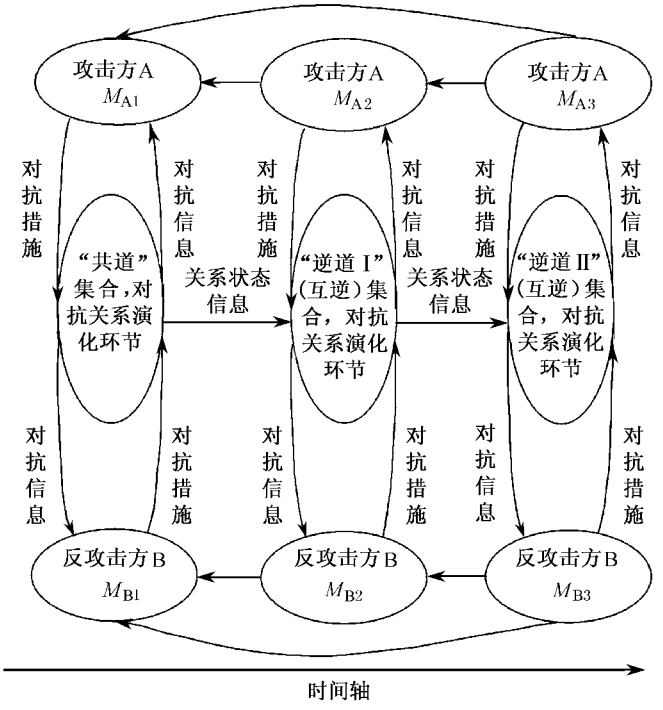


图 4.4　“共道—逆道”对抗过程模型

其中，M_A 代表攻击方法集合，M_{A1}，M_{A2}，M_{A3} 表示在“共道”、“逆道Ⅰ”、“逆道Ⅱ”阶段 M_A 的子集合。M_B 代表反攻击方法集合，M_{B1}，M_{B2}，M_{B3} 表示在“共道”、“逆道Ⅰ”、“逆道Ⅱ”阶段 M_B 的子集合。

整个对抗过程可用多重动态演化的六元关系组表示（$R^n[G,P,O,E,M,t]$），其中，G 代表

目的集合，P 为核心参数集合，它集中表示 E,O,M 的重要状态。E 为环境集合也可理解为双方约束条件，它是在对抗过程中各种复杂原因所形成的复杂约束条件集合。M 为双方对抗所用方法集合，它是双方由各自对抗目的形成的目标并根据约束条件和对方的方法所形成己方针对性的对抗方法。O 是由双方对抗目的所形成的具体行动目标。t 为时间因素，它影响 P、O、E、M、G 等的多种形式。如各因素集合随时间的连续变化可表示为它是时间函数。离散型变化也可用 E 环境因素的约束条件表示，如在某时间间隔中存在，某某与某某间的时间次序关系等，$R^n[G,P,O,E,M,t]$ 的含义除了上述时间因素的嵌入构成函数关系外，各组之间往往还互相嵌入形成复杂相互关系。

下面将解释 $R^n[G,P,O,E,M,t]$ 的构成特征。$R^n[G,P,O,E,M,t]$ 的构成是一件复杂重要的事，通过它表征某具体“对抗”相互斗争的机理、方法、过程和结果，是模型构成的核心，并融入模型各环节中强化并完备模型功能，完成设置“模型”所欲达到的目的。R^n 的构成并不能孤立进行，要紧密结合实际“对抗”环境，综合其中所包含的六个组元情况，有机地进行 R^n 的整体构成，由于双方对抗势不两立，故各组元情况双方都很保密。同时又竭力获取对方信息，因此在利用模型策划实施“对抗”时，只能依靠不完全信息、智慧来设定 R^n，然后预测结果。

综合上述情况，对 R^n 的构成要点可归结如下：R^n 与六元组实际情况密切相关。在复杂情况下，其构成非常复杂且具不确定性，不能完全用定量表达式来表示，必定是定性与定量相结合地表达，除了双方在总体层次建立对抗关系 $R^n[G,P,O,E,M,t]$ 外，也正因上述原因往往还需分段（分环节、分阶段、子阶段、层次、子层次、剖面等）结合实际应用分别建立。R^n 没有固定规范的方法，上两节相关原理的灵活应用是构成 $R^n[G,P,O,E,M,t]$ 及 M 的原则性方法。最后还要指出，$R^n[G,P,O,E,M,t]$ 在应用中是动态演变的（随时间、组元变化而演变），演变的结果即代表“模型”模拟的结果。同时具有不确定性，即对抗结束后 $R^n[G,P,O,E,M,t]$ 的演化过程也往往不能全部明确，即使这样建立和利用模型及 $R^n[G,P,O,E,M,t]$ 仍旧是非常重要的方法。

模型框图中三个核心环节，称为“共道”、“逆道Ⅰ”、“逆道Ⅱ”对抗关系演化环节。它们包含了灵活综合表征对抗的性能。如：可以表示某阶段性对抗，也可表示某一回合对抗，还可综合表示对抗阶段（内含子阶段，如“逆道”中含“共道”等），也可在环节中同时突出某个相反相成核心子环节的作用等，总之“环节”可广泛表征“对抗”并灵活加以应用。在环节内用六元组 $R^n[G,P,O,E,M,t]$ 关系，用于表达节点动态演化，模型整体是三个环节，一般在时间维上形成串联环节，当攻击方首先完成“共道”环节后，转入“逆道Ⅰ”环节，在此节点即很可能发生激烈对抗，当攻击方完成攻击准备后转入最后的“逆道Ⅱ”环节，经激烈对抗谋取完成攻击的目的。当然也存在相反情况，即以攻击方在“逆道Ⅰ”环节和“逆道Ⅱ”环节的失败形成一个回合的攻击失败而告终（环节的 $0\sim1$ 状态表征了某方失败与成功）。很少数情况会发生在共道环节结束对抗，这是因为在共道环节上对抗信息很难完备获取，因而较难形成决定性的对抗结果，注意“对抗信息”对双方都很重要，“共道—逆道”模型应用于信息安全对抗，往往是一个复

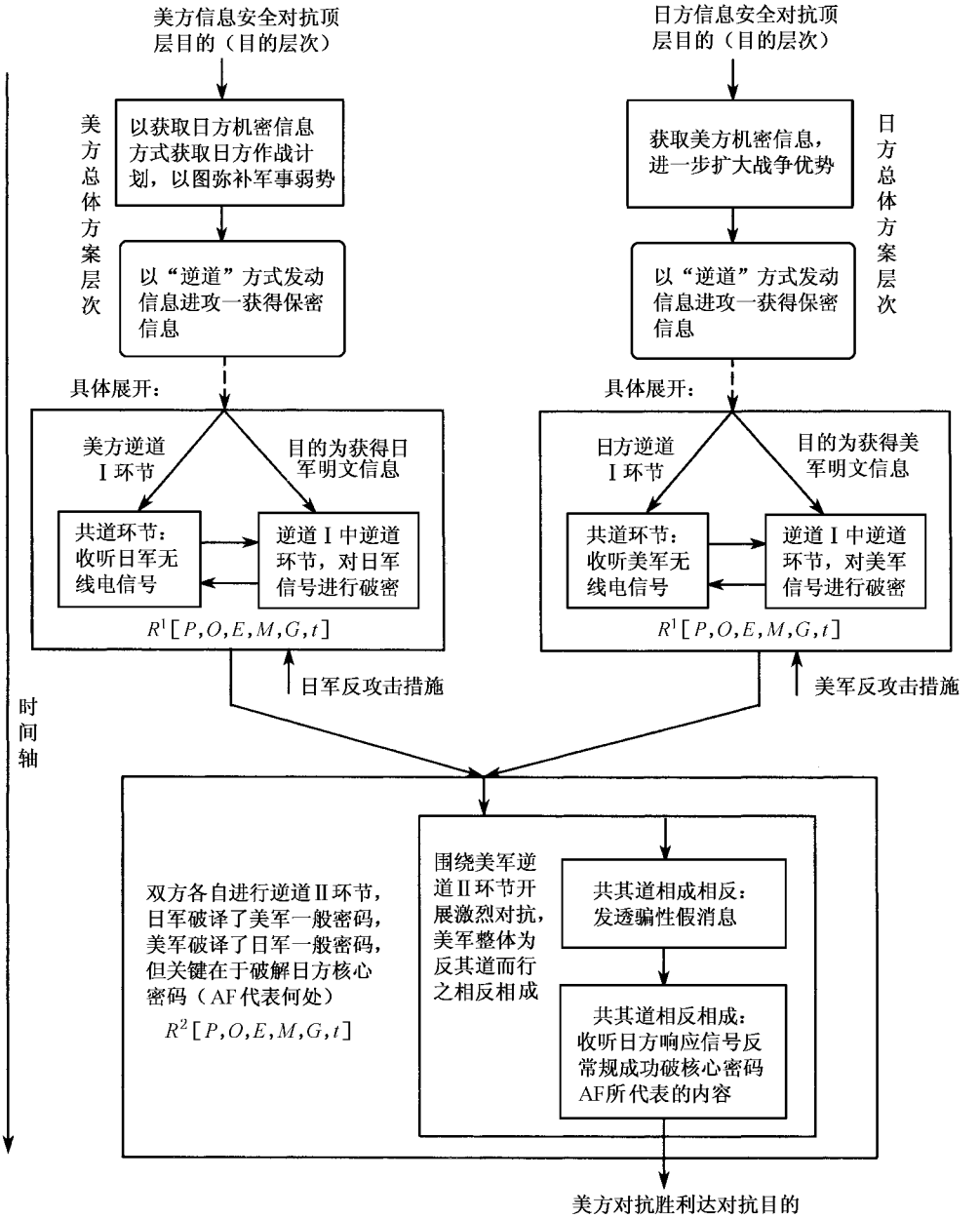
杂系统性过程(因为牵涉到人的介入,故多是开放复杂巨系统)。作为概括普适机理性对抗模型,要能表征对抗过程的重要基本特征,它往往要在多层次、多剖面及多时间片段、阶段、过程的多重交织情况下表征动态过程。因此,需要多次叠套展开建立模型,即往往在建立的每一"共道"或"逆道"环节中再建立下层"共道—逆道"三环节模型,用以表征更具体一层的对抗。每个环节的动态结果也有多种表达,如 $R^n[G,P,O,E,M,t]$ 中某方目的的完全达到另方目的的完全被破坏,则可用 0～1 表示。但实际情况很复杂,往往不能以 0～1 表示,需要建立"评价函数",利用评价函数来决策如何继续对抗。这样往往需要人作最后判断(高层次策者),评价函数的确定一般是很难的事,往往要依靠经验和各种知识。如数学泛函中的距离、内积概念借用以表示现在的结果与理想、预期目的间的差距。为了说明多层次多阶段的"共道—逆道"行为交织,举例如下。

例 1　二战初期美日信息安全对抗实例。

1942 年美国在日本偷袭珍珠港后,太平洋海军力量大受损失,为了抑制日本在太平洋上的强势进攻,特别注意收集日军各种信息,尤其是无线电信息,并大力研究、破译日方密码。由总体层次分析,美方进行的是信息安全攻击,以获取日方机密信息,是一种"逆道"行为。但前提条件是不破坏日方正常通信的"共道"行为,当收到日军频繁通信的无线电信号时,美方判断日军将有大规模军事行动,否则不会这样频繁通信,更加强了对日无线电信息破译工作。不久后破译出日方无线电信号,说明日本联合舰队将向代号为 AF 的地点进攻,但 AF 是何处不得而知,时间非常紧迫,不能再花费更多的时间去破译、探知 AF 为何处,猜测可能是中途岛或另一处。美方想出一个"欲擒故纵"、"相反相成",在"逆道"环节中嵌套"共道"环节的计策,即用低级密码(日方很可能破译)声称"中途岛淡水设备损坏,亟待抢修"的假情报,过了几天破译的日本电报中出现了"AF 谈水设备损坏亟待抢修"的信息,美军便判断了 AF 为中途岛,此后预有准备地进行了中途岛战役,日联合舰队第一次吃了惨重败仗(几艘主力航空母舰沉没),这是一个很典型的"共道—逆道"诸环节多层次交织融合进行信息安全对抗的实例,现用"共道—逆道"模型加以揭示美方信息安全对抗顶层目的(目的层次)所形成对抗过程。如图 4.5。

对 $R^1(P,O,E,M,G,t)$ 进行分析。其中,P 为双方力图破译对方密码,双方又力图保护自己密码不被破译;O 为双方密码;E 是在对方更换密码前破译及在对方重大军事行动前获得信息(约束条件集合);M 为各种破译密码手段及各种生成密码方法;G 代表这一阶段结果,为:日方破译了美方一般常用密码,美方基本破译日方密码,已知日军将有重大进攻战役(攻占 AF 为核心),但密码中重要内容的再加密部分(即 AF 代码)并未破译,此发现对美军非常重要,引起美方全力以赴确定 AF 代码代表何地。由上述实情对逆道Ⅰ环节双方都各自完成了准备工作,双方共赢达到局部目的。

对 $R^2(P,O,E,M,G,t)$ 分析。其中,P 为美方力图获得日方进攻地点信息;O 浓缩为得知 AF 代码内容;E 在此环节,时间约束是第一约束,第二约束是破解密码且不能让日方察觉;M 为方法的分析综合:AF 的产生是日方对某地 R 作某种运算(实际为加密过程)而得到的结



注： 美方技术措施层次及双方对抗过程的动态展开中，“共道”环节没有值得重点研究的措施，故只对逆道环节展开讨论

图 4.5 美日双方对抗过程

果，即 $\Phi R=\mathrm{AF}$，Φ 是 $R\longrightarrow\mathrm{AF}$ 的映射，攻击方破译 AF，实际是对 AF 作逆运算从而得到 R，是解逆逆向问题，这一般是非常困难的，甚至是不可能的，因而应从顶层思路上想办法，一种思路是改变求逆问题为正向验证问题。

在美方预先设立之 $X_1,X_2,\cdots,X_R$ 中挑选一个最可能者设法使日方自己作映射，找出 $\Phi X_R=\mathrm{AF}$ 者，则可知 $X_R=R$。因此，破译 AF 问题转移至如诱使日方对美方设定的 X_R 作 ΦX_R 的运算，为了诱使日方按美方设定之 X_R 作运算，利用了日方也正在不断截获美方无线电信号的日方对抗行为（日方逆道Ⅰ中内容信息的双刃剑效应系统理论中有得必有付出代价原理），诱使日方上当，总体上是以“相反相成”原理使美方获胜，破译了 AF 密码得知了真实地点，以下是核心环节对抗分析。

日方为了进攻准备，非常注意收听美方军事通信无线电信号，这样也就可能收到美方制造假信息并受其影响（日方风险和代价），美方就利用这种特性转化日方的反向工作为己所用；试探地用低级密码发出了“中途岛淡水设备损坏亟待修复”的假信息进行诱骗。结果是日方受骗，联合舰队向下属通报美方假信息并在其被美方截获的后续电报中出现了“AF 淡水设备损坏亟待修复”，这样美方便确定了“AF 即中途岛”，即日军这场战役目的地为中途岛，从而大大有利战役的准备工作，取得了战役胜利。

由以上对实例的分析，可明确认识到在这场斗争过程中，美方的关键逆道环节，包括了几个子环节。其中，发假消息诱骗日方从而验证 AF 是一种相反相成，利用日方逆道（共其逆道行为）的巧妙对抗，由此看到，发挥人的智慧，运用科学技术在信息安全对抗领域争取主动是极端重要的，而斗智是无“终极”的。从理论上说日方也可将上述一切的一切都作为预设陷阱和假动作，即 AF 中途岛都是放出的烟雾诱引美方注意，而实攻目标却不是中途岛……当然历史事实上日本选择攻击目标为中途岛是有战略顶层的需要。而美国猜日本两个可能的攻击目标之一为中途岛也是有根据的，这些说明信息领域中的斗争具有重要意义，但它仍需服务于战争全局的需要。此例子在此用做分析总结，所分析的美方思路和行动措施是用做谋划“对抗”取胜目的的。

现进一步讨论所建立“共道—逆道”对抗博弈模型与前面基础层次对抗原理（4.3 节）和系统层次对抗原理（4.4 节）所叙述诸原理之间的主要关系，分为三个层次讨论。

第一层次为涉及奠基模型核心理念所应用的诸原理。

“共道”—“逆道”对抗机理博弈模型（以下简称模型）的本征属性是以相对普遍的结构形式形成具有普遍应用的可能性，而在具体应用场合下是通过填充一些实际内容后，从而解决具体对抗问题（得出具有特殊性的答案），在这个意义上“特殊性存在与保持原理（4.3.1 节）起着理论上的奠基作用，4.2 节将建模基础理论与耗散自组织理论相关联。

在“模型”中表征双方形成“对抗”的基础是信息存在相对性原理（4.3.2 小节）、广义空间维及时间维信息的有限尺度表征原理（4.3.3 小节）、4.3.4 小节（在共道基础上反其道而行之相反相成）原理及 4.3.5 小节（共其道而行之相成相反）是双方进行对抗的最基本思维方法以

及形成对抗措施的基本原则，是“模型”各环节形成对抗内容的基础，争夺制对抗信息权及快速建立系统对策响应原理(4.3.6 小节)概括出双方对抗开始争夺的焦点和各斗争环节持续延伸的切入点和重要因素。以上是理念上应用诸原理进行模型奠基性建构。对应用层次而言，上面的思考是隐蔽的，表面上看无关紧要，但由全局角度讨论，以上工作具有基础重要性。

第二层次是讨论支持模型结构组成及形成核心功能的诸原理。

模型由共道、逆道Ⅰ、逆道Ⅱ三个环节所组成，这是根据对实际对抗过程概括提炼同时根据 4.3.4 和 4.3.5 小节；在共道基础上反其道而行之相反组成及共其道而行之相成相反，两条原理在理论上的支持所完成的。

由于 4.3 节 4.4 节所述原理是普适性的，即对抗双方都应争取利用上述原理以使己方取得好的对抗效果，由此这些原理由基本可能性角度支持了模型，适用双方构成博弈对抗过程，此外 4.3.4 和 4.3.5 小节除了对对抗双方的普适性以外还具有时空范畴的普适性，即对对抗过程不同层次不同剖面，不同过程，不同阶段共道逆道措施的普适性，因此由这些定理支持构成的三环节共道—逆道模型可适用对抗过程任何层次、剖面和阶段。

对抗实际过程开始于对抗信息的形成与掌握，即争夺制对抗信息权，正是 4.3.6 小节原理对对抗过程开始(包括了过程和回合)的聚变点给予理论上的揭示和支持。

第三层次讨论对抗双方在对抗过程中利用模型结合 $R^n(P,O,E,M,G,t)$ 填充具体内容，争取得到对己方有利的对抗效果，与 4.3.4 和 4.3.5 小节各原理相结合的关系。

首先在模型各环节中利用 $R^n[G,P,O,E,M,t]$ 填充各项内容时，无论直接对准运行信息或针对信息系统运行正常的“序”，双方构成对抗思维方法方面最核心内容是灵活地应用 4.3.4 和 4.3.5 小节反其道而行之相反相成及共其道而行之相成相反这两条原理，而系统的“序”就可认为是一种“特殊性”的保持。对于“信息”的存在除了对应“特殊性”存在外，还体现“映射”的正确存在。假信息对应以“假”，代替正确的同构或同态映射。双方对抗中，在 $R^n[G,P,O,E,M,t]$ 中，动态地选择一系列的 M，从争夺制对抗信息权开始，展开对抗斗争方法。方法 M 的具体选择中，4.3.4 和 4.3.5 小节叙述的各原理绝大多数都要被多次灵活地应用。例如，4.4.3 小节原理指导双方寻找对方脆弱性和自我防止脆弱。4.4.4 小节原理是指导产生更具体的方法 M 时会起的作用，4.4.5 小节原理的灵活应用，成功体现了系统性全局运筹取胜往往是更全面更高层次的胜利，具有更多的智慧性。

诸定理与模型应用间相互关系体现在 $R^n[G,P,O,E,M,t]$ 具体关系的形成上，具体内容可参考所举实例来体会，这些实例包括了已经举例者和以后章节中的举例者。

上小节结合模型对中途岛战役，美日双方进行信息对抗事例进行了概要分析，本小节将利用 $R^n[G,P,O,E,M,t]$ 关系举例，进行系统层次信息安全对抗定量分析。

例 2 对抗双方基于科学技术形成对抗能力的博弈分析。设有两类信息科技：一类为应用基础类型，另一类为应用类型，各用 $N_1(t)$ 和 $N_2(t)$ 表示，对抗双方 A，B 的对抗能力以 $n_A(t)$，$n_B(t)$ 表示，双方围绕吸取科技知识 N_1，N_2 化作自己的能力而斗争，一方科技能力为零

则被判断为失败并假设每种科技知识只能为某一方所用(这里简单化假设),对抗斗争过程用以下微分方程组表示。设:

$$\frac{\mathrm{d}n_{\mathrm{A}}}{\mathrm{d}t}=[\alpha_{11}N_1(t)+\alpha_{12}N_2(t)]n_{\mathrm{A}}(t)-\delta_{\mathrm{A}}n_{\mathrm{A}}(t)$$

$$\frac{\mathrm{d}n_{\mathrm{B}}}{\mathrm{d}t}=[\alpha_{21}N_1(t)+\alpha_{22}N_2(t)]n_{\mathrm{B}}(t)-\delta_{\mathrm{B}}n_{\mathrm{B}}(t)$$

$$\frac{\mathrm{d}N_1(t)}{\mathrm{d}t}=r_1[(N_1^0-N_1(t)]-M_{11}n_{\mathrm{A}}(t)-M_{12}n_{\mathrm{B}}(t)$$

$$\frac{\mathrm{d}N_2(t)}{\mathrm{d}t}=r_2[(N_2^0-N_2(t)]-M_{21}n_{\mathrm{A}}(t)-M_{22}n_{\mathrm{B}}(t)$$

以上四个联立非线性微分方程组是一类 $R^n[G,P,O,E,M,t]$ 对抗关系的表示,其中 α 为从二类科技知识转为 A,B 方对抗能力的系数;δ 为能力中落伍淘汰系数。其中 N_1^0,N_2^0 为基础科学所支持技术科学(信息领域)的初始值,实际上是缓变增长,现相比缓慢可看做常数;r_1,r_2 为 $N_1(t),N_2(t)$ 的增长力转换系数,M 为科技与能力间转换因素。

利用表示对抗过程的 $n_{\mathrm{A}}(t),n_{\mathrm{B}}(t)$ 解析式,"模型"化归如下形式,见图 4.6。

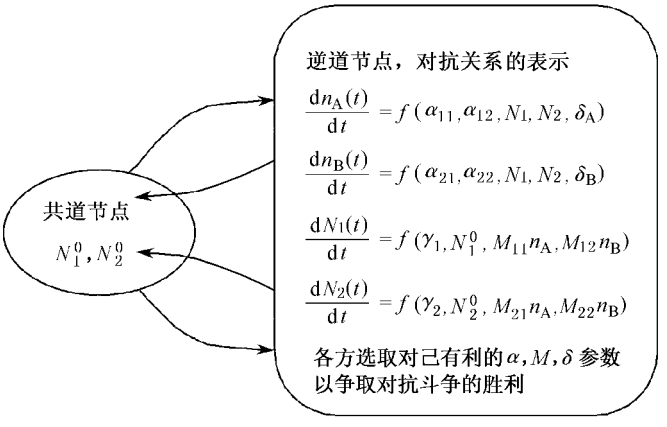


图 4.6　"对抗"化归模型

定量分析及近似结果:上述非线性常微分方程求解析解非常困难复杂,求出的解析形式又往往很难直接得出物理概念。为了绕开数学难题和提高分析实效,常取近似方法分析。假设 $N_1(t)$ 和 $N_2(t)$ 的变化比一场对抗斗争中各因素变化慢。

则可设 $\frac{\mathrm{d}N_1(t)}{\mathrm{d}t},\frac{\mathrm{d}N_2(t)}{\mathrm{d}t}=0$,有如下式

$$N_1(t)=N_1^0-\frac{1}{r_1}[M_{11}n_{\mathrm{A}}(t)+M_{12}n_{\mathrm{B}}(t)]$$

$$N_2(t) = N_2^0 - \frac{1}{r_2}[M_{21}n_A(t) + M_{22}n_B(t)]$$

将其作为约束条件代入$\frac{dn_A(t)}{dt}$及$\frac{dn_B(t)}{dt}$的微分方程可得

$$\left.\begin{aligned}\frac{dn_A}{dt} &= \alpha_1 n_A(t) - \beta_{11}n_A^2(t) - \beta_{12}n_A(t)n_B(t) = f_1[n_A(t), n_B(t)]\\ \frac{dn_B}{dt} &= \alpha_2 n_B(t) - \beta_{21}n_A(t)n_B(t) - \beta_{22}n_B^2(t) = f_2[n_A(t), n_B(t)]\end{aligned}\right\} \quad (1)$$

$$\beta_{11} = \frac{\alpha_{11}}{r_1}M_{11} + \frac{\alpha_{12}}{r_2}M_{21} \quad \beta_{12} = \frac{\alpha_{11}}{r_1}M_{12} + \frac{\alpha_{12}}{r_2}M_{22}$$

$$\beta_{21} = \frac{\alpha_{21}}{r_1}M_{11} + \frac{\alpha_{22}}{r_2}M_{21}, \quad \beta_{22} = \frac{\alpha_{11}}{r_1}M_{12} + \frac{\alpha_{22}}{r_2}M_{22}$$

式中，$\alpha_1 = \alpha_{11}N_1^0 + \alpha_{12}N_2^0 - \delta_A$；$\alpha_2 = \alpha_{21}N_1^0 + \alpha_{22}N_2^0 - \delta_B$

分析对抗结局，应对式(1)求解，由于非线性性质研究稳态解具有终极意义也较方便，下面将在不同平衡点分别进行研究，平衡点共有三组。即

$$n_A = 0,\ n_B = 0$$

$$n_A = 0,\ n_B = \frac{\alpha_2}{\beta_{22}}$$

$$n_A = \frac{\alpha_1}{\beta_{11}},\ n_B = 0$$

现分别加以讨论，为了讨论需要利用式(1)雅可比矩阵，将其中各元素求得如下

$$\frac{\partial f_2}{\partial n_A} = -\beta_{21}n_B$$

$$\frac{\partial f_1}{\partial n_A} = \alpha_1 - 2\beta_{11}n_A - \beta_{12}n_B$$

$$\frac{\partial f_1}{\partial n_B} = -\beta_{12}n_A$$

$$\frac{\partial f_2}{\partial n_B} = \alpha_2 - \beta_{21}n_A - 2\beta_{22}n_B$$

在 $n_A=0$，$n_B=0$ 时，

$$\left.\frac{\partial f_1}{\partial n_A}\right|_{0,0} = \alpha_1,\ \left.\frac{\partial f_1}{\partial n_B}\right|_{0,0} = 0,\ \left.\frac{\partial f_2}{\partial n_A}\right|_{0,0} = 0,\ \left.\frac{\partial f_2}{\partial n_B}\right|_{0,0} = \alpha_2$$

平衡点$\begin{bmatrix}n_A\\ n_B\end{bmatrix}=\begin{bmatrix}0\\ 0\end{bmatrix}$处雅可比矩阵为 $\boldsymbol{J}=\begin{bmatrix}\alpha_1 & 0\\ 0 & \alpha_2\end{bmatrix}$

由 $\det(\boldsymbol{J}-\lambda\boldsymbol{E})=0=(\alpha_1-\lambda)(\alpha_2-\lambda)=0$ 得出特征值：$\lambda_1=\alpha_1$，$\lambda_2=\alpha_2$

如 $n_A=0$，$n_B=0$ 的平衡点为稳定平衡点，则 α_1，α_2 必小于 0，即

$$a_{11}N_1^0 + a_{12}N_2^0 < \delta_A, \quad a_{21}N_1^0 + a_{22}N_2^0 < \delta_B$$

这表明 A，B 双方吸收新科学技术化为能力，小于因过时而淘汰的能力，是内因的“自取灭亡”，而不是因“对抗”造成的被毁灭。

再分析攻击方失败，反攻击方生存（微分方程稳态解 $n_{\mathrm{A}}(t)=0, n_{\mathrm{B}}(t)=\dfrac{\alpha_2}{\beta_{22}}$ 情况）。此时雅可比矩阵为

$$\boldsymbol{J}=\left|\frac{\partial f}{\partial \tilde{n}}\right|_{0,\frac{\alpha_2}{\beta_{22}}}=\begin{bmatrix}\alpha_1-\dfrac{\beta_{11}\alpha_2}{\beta_{22}} & 0\\ -\dfrac{\beta_{12}\alpha_2}{\beta_{22}} & -\alpha_2\end{bmatrix}$$

由行列式 $\det(\boldsymbol{J}-\lambda\boldsymbol{E})=0$，其中 $\boldsymbol{E}$ 为单位矩阵，得

$$\left[\left(\alpha_1-\frac{\beta_{11}\alpha_2}{\beta_{22}}\right)-\lambda\right](\alpha_2-\lambda)=0,\ \lambda_1=-\alpha_2,\ \lambda_2=\alpha_1-\alpha_2\frac{\beta_{12}}{\beta_{22}}$$

若 $n_{\mathrm{A}}(t)=0,\ n_{\mathrm{B}}(t)=\dfrac{\alpha_2}{\beta_{22}}$ 为稳定态点，则 $\lambda_1=-\alpha_2$，必有 $\alpha_2>0,\ \alpha_1-\dfrac{\beta_{11}\alpha_2}{\beta_{22}}<0$，导致

$$\frac{\alpha_1}{\beta_{12}}-\frac{\alpha_2}{\beta_{22}}<0,\ \frac{\alpha_1}{\alpha_{12}}<\frac{\alpha_2}{\beta_{22}}$$

由以上不等式进一步展开后得：$\alpha_2=\alpha_{21}N_1^0+d_{22}N_2^0-\delta_{\mathrm{B}}>0$，这个条件的物理意义非常容易理解，即反攻击方必须保持安全科技能力的不断增加，作为信息安全斗争生存的必要条件，否则便成为“自取灭亡”。

A 方能力增加，即

$$\frac{\alpha_1}{\beta_{12}}=\frac{\alpha_{11}N_1^0+\alpha_{12}N_2^0-\delta_{\mathrm{A}}}{\dfrac{\alpha_{11}M_{12}}{\gamma_1}+\dfrac{\alpha_{12}M_{22}}{\gamma_2}}<\frac{\alpha_2}{\beta_{22}}=\frac{\alpha_{21}N_1^0+\alpha_{22}N_2^0-\delta_{\mathrm{B}}}{\dfrac{\alpha_{21}M_{21}}{\gamma_1}+\dfrac{\alpha_{22}M_{22}}{\gamma_2}}$$

由 α_1 的下标 1 表示与 A 方有关的系数，α_2 表示与 B 方有关的系数，而 β_{XX} 的前第 1 下标表示 A、B 对对方影响增长率，第 2 下标表示另外起作用的一方，如 β_{11} 表示 A 方对自身增长率产生影响，外加 A 方的影响（A 起平方作用），β_{12}，β_{22} 系数中包括了 α_{11}，α_{12}，α_{21}，α_{22} 等原来出现在表示增加对抗能力项目中的系数，式(1)中出现在表示减少对抗能力的项是因由 N_1^0，N_2^0 中越多科技项目被双方转化为对抗能力，则剩余科技项目就越少（假设 N_1^0，N_2^0 本身增长很慢），同时也就会起阻碍能力增长的作用，从而这些因素同时在 α_1，α_2 及 β_{12}，β_{22} 等系数中出现，这体现了事物往往同时具有“双刃剑”效应并形成较复杂的非线性作用（普遍哲理），上述不等式表明 B 方对抗能力的增长系数与减少系数之比应比 A 方两系数之比大，则 B 方在对抗中对抗能力增长比 A 方快，从而使 B 方斗争取胜，使 A 方消亡。现 B 方胜 A 方条件中只涉及 β_{11}，β_{22}，没涉及双方交叉作用是稳态解中另一方已灭亡的缘故，条件变化后，可使 A 生存 B 方灭亡，以及 A、B 方共存持续斗争的结果，其中包括有双方交叉影响，在此就不再推演。

例 3　双方直接进行信息安全攻防对抗系统的总体层次定量分析。本例中假设攻击方准备工作进行顺利，反攻击方并没有察觉攻击先兆，因此可省略“共道”环节直接进入“逆道”攻击

阶段，而“逆道”环节的具体模型可应用随机服务理论构建。假设攻击方的各种攻击行为组成攻击流，反攻击方组成服务台表示；并以“服务”成功表示反攻击成功；若攻击方的“攻击流”中“个体”到达后得不到“服务”而离去，则称此“攻击流”的个体“突防”，代表攻击成功，其模型核如图 4.7 所示。

攻击方根据对抗信息采用不同措施组成攻击流，反攻击方采用不同反攻击措施形成了服务台的服务，将双方“逆道”演化环节利用随机服务理论进一步表示如下：设 A 方为攻击方，B 方为反攻击方。见图 4.8。

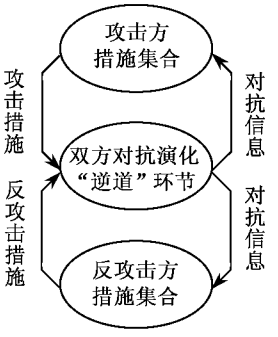


图 4.7　攻击双方“逆道”环节对抗过程演化表示框图

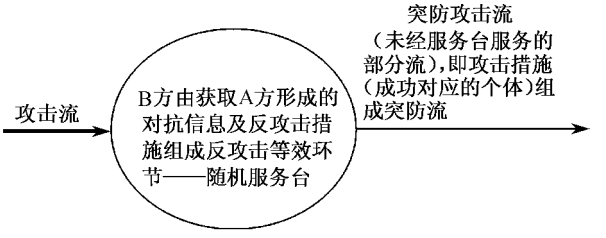


图 4.8　攻击流与服务

现用随机服务理论进行对抗过程的系统进行总体分析（以反攻击方为主进行表征），对 $R^n[G,P,O,E,M,t]$ 中各元素及关系表征为：

攻击方的各种攻击用随机普通流表示（Possion 流），它具有普遍性、平稳性及无后效性三种特性，它使得定量分析较为简单，也是一种实际攻击流的近似表示。但对反攻击方而言，这种近似产生比实际发生非普通流更为严峻的“形势”，普通流在 $0\sim\tau$ 的时间间隔内有 k 个“攻击”到达的概率分布函数 $P_k(\tau)=\frac{(\lambda\tau)^k}{k!}\mathrm{e}^{-\lambda\tau}$ 表示，其中 λ 为普通流唯一参数，称为“流强度”，表示单位时间内到达“攻击”个数的平均值。结合 $P_k(\tau)$ 的表达式说明普通流特性：无后效性，即到达流的概率只与 τ 有关，而与以前分布无关（由概率分布函数表达式中没有以前时间间隔 τ_0，τ_1 等参数介入可明显看出），表达式中没有时间坐标因子 t 的介入，因此分布函数与时间坐标无关而呈平稳性，至于普通性则规定在任何时刻 t 时最多只有一个攻击流到达，以上是攻击方的攻击流 M,P 的描述。

服务台反攻击行为由二级串联组成，第一级为攻击信息（对抗信息）获取部分，第二级为采取反攻击措施部分 ，其性能都用服务时间（获得对抗信息，采取反攻击对抗措施，统称为“服务”）来表示，服务时间具有随机性用随机变量表示（由于复杂性所造成），服务时间 $t_{服务}<t$ 的概率分布，服从负指数性，即用 $F(t_{服务}<t)=1-\mathrm{e}^{-Mt}$ 形式表示，当具有多种获取对抗信息的方

法措施时，则用其各种获取对抗信息时间的加权平均值构成 $1/M_1$，第二级也取各种措施进行反攻击的加权平均时间构成 $1/M_2$。由两个服务台组成一个整体性反攻击动态演化环节。

为了进行较严格情况分析，进一步假设攻击流在服务台逗留时间很短。如到达服务台却得不到服务便要离开而算做突防（攻击成功），因此连同获取服务台反攻击措施构成两级服务台，由第一级攻击流到达后先进行服务，以 $F_1(t_{服务}<t)=1-\mathrm{e}^{-M_1 t}$ 表示服务时间$<t$ 的概率分布函数，相当于提取攻击相关信息（对抗信息）提供第二级服务之用，第二级服务时间（反攻击所需时间），以 $F_2(t_{服务}<t)=1-\mathrm{e}^{-M_2 t}$ 表示概率分布函数，其中 M_1、M_2 为 F_1 和 F_2 的平均服务时间的倒数，在此应指出，假设经过第一级服务台输出的攻击流，本身性质没有受影响而变动，因此到达第二级服务台时仍为泊松普通流，以上是反攻击方 M 及 G 的描述。现在导出反攻击成功概率表达式的微分方程，然后求出稳定解，即表达反攻击成功的概率值。

考虑在 $t+\Delta t$ 后沿时刻各状态解析表达式，同时认为，Δt 间隔很小，可近似看做 $t+\Delta t$ 时刻（因此在其中最多只可能有一个攻击流到达，依据流的普通性而得出的近似认定），状态由到达流被服务和未被服务（突防）两种分状态所组成（没有中间状态）。由 S_{00}，S_{01}，S_{10}，S_{11} 分别代表第一、二级空，第一级空第二级服务，第一级服务第二级空间，和第一、二级都正在服务，组成整个系统的状态组合，在 t 时刻发生各状态的概率用 $P_{00}(t)$，$P_{01}(t)$，$P_{10}(t)$，$P_{11}(t)$ 表示。分析如下：

· 在 $t+\Delta t$ 时刻 S_{00} 状态由以下两种分状态组合形成，各分状态是互不相容的，可用概率相加定理。

分状态 1：系统 t 时刻在 S_{00} 状态，Δt 内无攻击流到达（其概率近似为 $(1-\lambda\Delta t)$），形成在 $t+\Delta t$ 时刻保持状态的概率为 $P_{00}^{(1)}(t+\Delta t)=P_{00}(t)(1-\lambda\Delta t)$。

分状态 2：系统 t 时刻处在 S_{01} 状态，Δt 内火控系统“服务”完毕，也无攻击流到达组成在 $t+\Delta t$ 时刻分状态 2 的概率为 $P_{00}^{(2)}(t+\Delta t)=P_{01}(t)M_2\Delta t(1-\lambda\Delta t)\approx P_{01}(t)M_2\Delta t$。

所以
$$P_{00}(t+\Delta t)=P_{00}^{(1)}(t+\Delta t)+P^2(t+\Delta t)=P_{00}(t)-P_{00}(t)\lambda\Delta t+P_{01}(t)M_2\Delta t$$
$$P_{00}(t+\Delta t)-P_{00}(t)=P_{01}(t)M_2\Delta t-P_{00}(t)\lambda\Delta t$$

当
$$\Delta t\to 0\ \frac{\mathrm{d}P_{00}(t)}{\mathrm{d}t}=M_2P_{01(}t)-\lambda P_{00}(t)$$

· 在 $t+\Delta t$ 时刻系统处于 S_{01} 状态为三个不相容分状态的组合，即

分状态 1：在 t 时刻系统处于 S_{01} 状态，在 Δt 间隔内不变化（无“流”到达，第二级未服务完），故在 $t+\Delta t$ 时刻分状态 1 的概率为

$$P_{01}^{(1)}(t+\Delta t)=P_{01}(1-\lambda\Delta t)(1-M_2\Delta t)\approx P_{01}(t)(1-\lambda\Delta t-M_2\Delta t)$$

分状态 2：在 t 时刻系统处于 S_{10} 状态，在 Δt 间隔内第一级服务完毕进入第二级，无“流”到达：

$$P_{01}^{(2)}(t+\Delta t)=P_{10}(t)(1-\lambda\Delta t)M_1\Delta t\approx P_{10}(t)M_1\Delta t$$

分状态 3：在 t 时刻系统处于 S_{11} 状态，在 Δt 内第一级服务完毕送入第二级服务，此时无

“流”到达：

$$P_{01}^{(3)}(t+\Delta t) = P_{11}(t)M_1\Delta t(1-\lambda\Delta t) \approx P_{11}(t)M_1\Delta t$$

故在 $t+\Delta t$ 时刻，

$$\begin{aligned} P_{01}(t+\Delta t) &= P_{01}^{(1)}(t) + P_{01}^{(2)}(t) + P_{01}^{(3)}(t) \\ &= P_{01}(t) - (\lambda + M_2)P_{01}(t)\Delta t + M_1 P_{10}(t)\Delta t + M_1 P_{11}(t)\Delta t \end{aligned}$$

所以 $\dfrac{\mathrm{d}P_{01}(t)}{\mathrm{d}t} = M_1 P_{10}(t) + M_1 P_{11}(t) - (\lambda + M_2)P_{01}(t)$

· 在 $t+\Delta t$ 时刻系统处于 S_{10} 状态为三个不相容分状态的组合，即

分状态 1：在 t 时刻系统处于 S_{00} 状态，而在 Δt 间隔内有一个流到达，在 $t+\Delta t$ 时刻分状态 1 的概率为

$$P_{10}^{(1)}(t+\Delta t) = P_{00}(t)\lambda\Delta t$$

分状态 2：在 t 时刻系统处于 S_{10} 状态，在 Δt 间隔内第一级未服务完（状态保持与“流”是否到达无关）。

$$P_{10}^{(2)}(t+\Delta t) = P_{10}(t)(1-M_1\Delta t)$$

分状态 3：在 t 时刻系统处于 S_{11} 状态，在 Δt 内第二级服务完毕（状态与有无“流”到达无关）。

$$P_{10}^{(3)}(t+\Delta t) = P_{11}(t)M_2\Delta t \quad \text{所以，} \frac{\mathrm{d}P_{10}(t)}{\mathrm{d}t} = \lambda P_{00}(t) - M_1 P_{10}(t) + M_2 P_{11}(t)$$

· 最后分析在 $t+\Delta t$ 时刻系统处于 S_{11} 状态是三个分状态组合，即

分状态 1：在 t 时刻系统处于 S_{01} 状态，在 Δt 间隔内有一个“流”到达，第二级没服务完，此时分状态 1 在 $t+\Delta t$ 时刻的概率为

$$P_{11}^{(1)}(t+\Delta t) \approx P_{01}(t)\lambda\Delta t(1-M_2\Delta t) \approx P_{01}(t)\lambda\Delta t$$

分状态 2：在 t 时刻系统处于 S_{11} 状态，在 Δt 间隔内第一级、第二级都未完成服务（状态与有无“流”到达无关）。

$$\begin{aligned} P_{11}^{(2)}(t+\Delta t) &= P^{11}(t)(1-M_1\Delta t)(1-M_2\Delta t) \approx P_{11}(t) - M_1(t)\Delta t - M_2 P_{11}(t)\Delta t \\ &= P_{11}(t) - (M_1 + M_2)P_{11}(t)\Delta t \end{aligned}$$

分状态 3：原处在 S_{10} 状态，在 Δt 间隔内第一级服务完，又有“流”到达（二级无限小可忽略）。

$$P_{11}^{(3)} = P_{10}(t)M_1\Delta t \cdot \lambda\Delta t, \quad \text{所以} \quad \frac{\mathrm{d}P_{11}(t)}{\mathrm{d}t} = \lambda P_{01}(t) - (M_1 + M_2)P_{11}(t)$$

由以上分析得到表示系统 S_{00}，S_{01}，S_{10}，S_{11} 状态概率的微分方程组描述为

$$\frac{\mathrm{d}P_{00}(t)}{\mathrm{d}t} = -\lambda P_{00}(t) + M_2 P_{01}(t)$$

$$\frac{\mathrm{d}P_{01}(t)}{\mathrm{d}t} = -(\lambda + M_2)P_{01}(t) + M_2 P_{10}(t) + M_2 P_{11}(t)$$

$$\frac{\mathrm{d}P_{10}(t)}{\mathrm{d}t}=\lambda P_{00}(t)+M_1P_{10}(t)+M_2P_{11}(t)$$

$$\frac{\mathrm{d}P_{11}(t)}{\mathrm{d}t}=\lambda P_{01}(t)-(M_1+M_2)P_{11}(t)$$

我们最关注的是上述微分方程的稳态解(“存在”的实际系统总有稳态解),即 $t\to\infty$ 时,$P_{ij}(t)=$某常数,这时 $\frac{\mathrm{d}P_{ij}}{\mathrm{d}t}=0,(i,j=1,2)$,此时微分方程化为一组齐次代数方程,齐次代数方程若有非零解,则其系数矩阵组成行列式必为零,经验证,其系数行列式为零,用线性代数定理可得出一组稳定解为

$$P_{00}=\frac{M_1M_2}{(M_1+\lambda)(M_2+\lambda)}$$

$$P_{10}=\frac{\lambda M_2(M_1+M_2+\lambda)}{(M_1+M_2)(M_1+\lambda)(M_2+\lambda)}$$

$$P_{01}=\frac{\lambda M_1}{(M_1+\lambda)(M_2+\lambda)}$$

$$P_{11}=\frac{M_1\lambda_2}{(M_1+M_2)(M_1+\lambda)(M_2+\lambda)}$$

结合物理概念来验证由上式求得各种状态的概率:当系统服务很快时(相对流强度),即 $M_1,M_2\gg\lambda$ 时,P_{00} 值应该很大。意即系统很快处理完了,达到的“流”没有滞留,而 P_{10},P_{01},P_{11} 值都很小。

如 $M_1,M_2=100,\ \lambda=1$ 可得

$$P_{00}=\frac{10\ 000}{10\ 201}=0.980\ 3,\ P_{10}=\frac{20\ 100}{20\times10\ 201}=0.098\ 5$$

$$P_{01}=\frac{100}{10\ 201}=0.009\ 803,\ P_{11}=0.000\ 05$$

如 $M_1=100,\ M_2=10,\ \lambda=1$ 可得

$$P_{00}=\frac{1\ 000}{101\times11}=0.90,\qquad P_{10}=\frac{10\times111}{110\times11\times101}=0.009$$

$$P_{01}=\frac{100}{11\times101}=0.09,\qquad P_{11}=\frac{100}{110\times11\times101}=0.000\ 82$$

服务时间短于“流”平均到达的时间间隔,说明 P_{00} 较大,又因第一级处理速度比第二级快得多,第二级平均服务时间已短到“流”到时间间隔的 $\frac{1}{10}$ 倍(第一级为 $\frac{1}{100}$ 倍)。第一级形成“流”滞留的概率很小,第二级相对滞留概率大一些,计算出的概率值证明由物理概念推论的正确性。为了再次验证可设想,M_1,M_2 数值对换,则应 P_{10},P_{01} 数值对换,故计算 $M_1=10,\ M_2=100,\ \lambda=1$ 的概率值

$$P_{00}=\frac{1\ 000}{101\times 11}=0.90(\text{没变}),\quad P_{10}=\frac{100\times 111}{110\times 11\times 101}=0.09$$

$$P_{01}=\frac{10}{11\times 101}=0.009,\quad P_{11}=\frac{100}{110\times 11\times 101}=0.000\ 82(\text{没变})$$

计算结果圆满地验证了物理概念的推理：如入侵流强度(即平均到达间隔)小于二级系统的服务时间，则 P_{00} 应接近于零(服务台都忙于服务，空间概率很小)，而首先接触“流”的第一级服务台更忙于服务，使得 P_{10}，P_{11} 都较大，表示二级服务台都忙于服务。举例如下。

设 $\lambda=100$，$M_1=M_2=1$，计算结果如下

$$P_{00}=\frac{1}{101\times 101}=0.000\ 098,\quad P_{10}=\frac{100\times 102}{2\times 101\times 101}=0.5$$

$$P_{01}=\frac{100}{101\times 101}=0.009\ 8,\quad P_{11}=\frac{10\ 000}{2\times 101\times 101}=0.490$$

很好地验证物理概念的推理结论。

如 λ、M_1、M_2 数值都差不多，则各状态除了第一级服务概率偏大些，各种状态出现概率分散布局情况。设 $\lambda=1$，$M_1=M_2=1$，表示系统服务能力仍较强，故 P_{00} 仍应较大(但不如 $M_1=M_2=100$ 时大)，数值应向 P_{10}，P_{01}，P_{11} 转移，请见下列计算结果的验证

$$P_{00}=\frac{100}{11\times 11}=0.826,\quad P_{10}=\frac{10\times 21}{20\times 11\times 11}=0.087$$

$$P_{01}=\frac{10}{11\times 11}=0.082\ 6,\quad P_{11}=\frac{10}{11\times 11\times 20}=0.004\ 1$$

得出系统各状态存在的概率分布后，重要问题是计算对抗过程的结果，即服务概率(反攻击成功概率)，及突防概率($1-P_{(\text{服务})}$)。突防概率 $P_{(\text{突防})}$ 一定和 λ，M_1，M_2 有关，λ 越强突防可能性越大，M_1、M_2 越大突防可能性越小，在此引用俄文参考书，给出稳态突防概率为 $P_{(\text{突防})}=1-\dfrac{M_1M_2(\lambda+M_1+M_2)}{(\lambda+M_1)(\lambda+M_2)(M_1+M_2)}$。

计算示例如下。

$$\lambda=1,M_1=M_2=100,P_{(\text{突防})}=1-\frac{100^2\times 201}{101^2\times 200}=0.015$$

$$\lambda=1,M_1=M_2=10,P_{(\text{突防})}=1-\frac{100\times 21}{11\times 11\times 20}=0.132$$

$$\lambda=1,M_1=100,M_2=10,P_{(\text{突防})}=1-\frac{1\ 000\times 111}{101\times 11\times 110}=0.091\ 8$$

$$\lambda=1,M_1=10,M_2=100,P_{(\text{突防})}=1-\frac{1\ 000\times 111}{11\times 101\times 110}=0.091\ 8$$

$$\lambda=1,M_1=1,M_2=1,P_{(\text{突防})}=1-\frac{1\times 3}{2\times 2\times 2}=0.625$$

$$\lambda=100,M_1=1,M_2=1,P_{(\text{突防})}=1-\frac{1\times 102}{101\times 101\times 2}=0.995$$

$$\lambda = 100, M_1 = 0.1, M_2 = 100, P_{(\text{突防})} = 1 - \frac{10 \times 200.1}{100.1 \times 200 \times 100.1} = 0.999\ 0$$

$$\lambda = 100, M_1 = 0.01, M_2 = 100, P_{(\text{突防})} = 1 - \frac{200.01}{100.01 \times 100.01 \times 200} = 0.999\ 9$$

$$\lambda = 100, M_1 = 0.01, M_2 = 0.01, P_{(\text{突防})} = 1 - \frac{(0.01)^2 \times 100.02}{100.01 \times 100.01 \times 0.02} = 1 - 10^{-8} = 1$$

由本小节的分析可得出以下简要结论：将对抗过程双方相互反其道而行理念，化归为随机流攻击下随机服务系统表征的相互对抗模型，并将 $R^n[G,P,O,E,M,T]$ 的动态演化具体展开为二级串联服务台对普通流的服务过程。设 λ 表示攻击强度，M_1 表征反攻击方获得对抗信息的能力，M_2 为反攻击能力，都映射到时间维。用反应速度表示能力，对于某种攻击，如无对抗措施，则对应 $M_2=0$，造成对抗失败。同样，如获取不到对方某种攻击信息，则对应 $M_1=0$，突防概率非常接近于 1，这样也使攻击得手，这进一步说明对抗过程中尽快获得对抗信息的重要性。

三、对抗中信息的作用

现举对抗博弈的例子。假设攻击方（B 方）可以从两个方向中选择一个方向作为某种攻击的主攻方向，防守方（A 方）从这两个方向中选择一个方向作为抗击的主要方向，同时部署组织支援，也有一个选择支援方向问题，我们用 A 方对 B 方造成伤害为博弈的支付矩阵。

设 B_1：为攻击方所选择的第一个攻击方向的事件

B_2：为攻击方所选择的第二个攻击方向的事件

A_{11}：为 A 方将防守主力置于第一方向的事件

A_{12}：为 A 方将防守主力置于第二方向的事件

A_{21}：为 A 方将支援置于第一方向的事件

A_{22}：为 A 方将支援置于第二方向的事件

A，B 双方博弈组合共 8 种，如表 4.1 所示。

表 4.1　对抗博弈组合形式

$A_{11}B_1A_{21}$	$A_{11}B_2A_{21}$	$A_{12}B_1A_{21}$	$A_{22}B_2A_{21}$
$A_{11}B_1A_{22}$	$A_{11}B_2A_{22}$	$A_{12}B_1A_{22}$	$A_{22}B_2A_{22}$

考察战斗结果的支付矩阵如下表 4.2 所示，设 A 方对准 B 方攻击方向，对准得益为 3，没对准得益为 1，将支持力量对准攻击方向，则附加得益为 7，没对准得益为 1。

如 A 方无法得到信息，则很难对准，特别是两次都对准是很难的，便不可能获得 $A_{11}B_1A_{21}$ 及 $A_{12}B_2A_{22}$ 得益最高项。

表 4.2　博弈支付矩阵

博弈组合	A_{21}	A_{22}
$A_{11}B_1$	3+7=10	3+1=4
$A_{11}B_2$	1+1=2	1+7=8
$A_{12}B_1$	1+7=8	1+1=2
$A_{12}B_2$	1+3=4	3+7=10

对照上述举例，可以很明显得出结论，获得对己有用的对方信息是很重要的，是一种先决条件。双方都这样做，形成了“对抗信息”的斗争焦点。

4.5.3　关于博弈模型的简要总结

本节建立了基于“共道”—“逆道”的对抗机理博弈模型，模型具有多层次结构特征，总体层次表示模型整体构成，由沿时间维顺序展开的“共道”、“逆道Ⅰ”、“逆道Ⅱ”三个串环节所组成。第二层将“整体构成”动态化，形成以 $R^n[G,P,O,E,M,t]$ 为核心含反馈的多层次交织联系的动态演化环节。第三层以“环节”结合 $R^n[G,P,O,E,M,t]$ 形成可嵌入环节，在使用模型进行对抗运筹时，可根据对抗策划的需要，以“环节”为单元进行功能嵌入，从而完成较科学细致的、多层次交织的对抗策划和仿真研究。第四层进一步对具体某阶段关键措施、方法等，利用 $R^n[G,P,O,E,M,t]$（结合其包含的六个组元）进行定性和定量的分析与综合，以达到尽可能好的模型利用效果。在复杂情况下可用模型结合科学计算进行研究，有广泛应用前景。本节并未涉及具体方法，而原理性的各种方法将在第五章叙述，第五章内容可嵌入本章相关环节，进行更具体的应用。

4.6　本章小结

本章论述了信息安全与对抗的基本原理，包括：信息安全与对抗的基础层次原理；特殊性、相对性在信息安全中的体现，信息广义时空维有限尺度原理，反其道而行之相反相成原理，共其道而行之相成相反原理，快速响应及动态发展原理等；信息安全系统层次原理，主动与被动原理，对称与不对称变换原理，间接对抗原理等；并化了较大篇幅介绍了“共道”—“逆道”模型及模型与诸原理间关系，结合实例说明模型及 $R^n[G,P,O,E,M,t]$ 用在信息安全对抗领域，对对抗矛盾进行分析综合的方法要点。

习　　题

1. 信息安全与对抗问题的基础层次定理有哪些？

2. 试用信息的特殊性原理分析信息安全与对抗问题并举例说明。

3. 试用信息存在的相对性原理分析信息安全与对抗问题并举例说明。

4. 试用广义空间信息的有限尺度原理分析信息安全与对抗问题并举例说明。

5. 试扼要说明在“共道基础反其道而行之相反相成原理”的主要内容及它的核心重要性(举例说明),以及与争夺制对抗信息权及快速建立对策响应原理之间的关系。

6. 试分析信息安全与对抗问题的快速响应原理并举例说明。

7. 信息安全与对抗过程的动态发展原理内容是什么？

8. 信息安全与对抗问题的系统层次原理有哪些？

9. 试分析信息安全对抗过程中攻击方与被攻击方的主动、被动特性。

10. 试用信息安全措施的核心转移原理分析信息安全与对抗问题并举例说明。

11. 试分析信息安全与对抗问题的对称与不对称变换原理并举例说明。

12. 试分析信息安全问题的间接对抗等价原理并举例说明。

13. 为什么需要从信息系统的顶层功能考虑信息安全问题？

14. 简述信息安全对抗过程的“共道”-“逆道”模型的博弈过程,并扼要说明与诸原理的关系。

15. 试说明六元关系组 $R^n[G,P,O,E,M,t]$ 在“共道”-“逆道”博弈模型中各环节中的作用以及对抗双方斗争如何体现在 $R^n[G,P,O,E,M,t]$ 中。

16. 试针对某一信息系统分析其获取对抗信息的重要性和作用。

17. 试针对计算机网络系统分析其对抗过程以及信息安全问题基础层和系统层原理的具体体现。

第5章　信息安全与对抗原理性方法

5.1　引　　言

本章主题是讨论对抗信息攻击，提高信息系统安全的原理性方法，由信息系统的系统层次功能全面考虑问题，安全性能是其中一个重要组成部分，并非全部。建立它们相互间关系的概念是前提，同时也需要有一个参考指标体系及其表征（测度）。按测度我们概略地将信息系统安全问题的考虑分为三类：第一类为信息安全性能放在优先考虑位置，优先采取措施保证系统安全性能满足要求，这是少数情况；第二类即安全性能与其他性能需综合考虑，安全性能重要，但其他性能也不能考虑不够，使其他功能削弱至不能接收的程度，这是一种重要类别，占相当大的比例，也是具有很大难度的问题；第三类是应用环境中其他功能占主要地位，安全功能只是附带考虑。无论是哪一类信息系统，其性能（包括安全性能）都随着社会的发展和科技进步而不断发展。

在实际场合，往往会碰到非常复杂的情况，形成复杂的问题，最复杂的问题是，其复杂矛盾难以确切被界定，难以确切描述，更难以圆满解决，只有酌情近似处理。这种情况属于人类对复杂性的认识和掌握，不在本书讨论范围内。

关于原理性对抗方法，可分为两部分，即系统层次方法及一些按类型划分的技术层次原理性方法（或称技术方案性方法），系统性方法与各类型技术层次方法两者结合、互相支持才能加强实际信息系统的安全能力，系统性方法用于总体思维和构建安全体系，各具体技术层次方法则用于具体实现。本章第四节为系统层次原理性方法，在介绍方法之前，用两节扼要介绍一些重要基本概念，如关系、算法、协议、系统管理运行控制、（管理软件）等为基础，第四、第五、第六节分别介绍各类具体技术方法，它们是信息隐藏方法，对抗信息系统及其服务群体作为整体按“特殊性”加以安全保护的方法，以及信息和其实体的个性保持方法，由于信息系统安全对抗问题具有复杂系统性，为加强有关原理、方法相互关联之理解，专用第一节进行综合举例加以扼要叙述，以加强对问题的理解。本章内容必然涉及信息攻击问题，这是矛盾对立统一的必然，但绝不等于本书提倡信息攻击并对其加以支持。

5.2　信息系统性能指标及安全对抗性能占位分析

信息系统是一大类系统的统称，其内部可再划分为多种类型专门系统，在发展中不断融合产生新功能系统。性能指标不断产生，旧指标随旧系统消亡而消亡，同时，不同类型信息系统有不同具体指标，在本节中只给出为了研讨安全对抗问题的参考框架指标体系。

5.2.1　信息系统性能指标体系之基本观念

信息系统作为为人类服务的一种重要工具，除应考虑基本功能外，在设定指标体系中还应考虑安全因素及使用性能，并应根据实际应用环境加以三因素的系统综合运筹考虑，非此则信息系统很难很好发挥为人类服务的最本质功能。例如不断出现重大安全问题造成重大损失，根本地动摇这种信息系统存在的必要性，使用性能也同样重要，如使用中付出过大的代价会造成“得不偿失”，这种信息系统也难以生存。综上所述，笔者认为，信息系统指标中应就传统常规性能或称理想环境下性能、安全性能、使用性能三因素并列综合运筹，这是构造信息系统指标体系的基本观念。

5.2.2　可裁减增设的指标体系框架

侧重系统性、可持续发展的信息系统性能指标体系框架，其特征具有多层次、动态的系统性质，具有可持续发展的适应性和广泛性构成了多层次开放结构，对各类信息系统根据实况可裁剪应用。

一、常规性能指标维

常规性能指标维（也可称为理想安全环境性能维），按其信息功能划分，如图 5.1～图 5.6 所示。当考虑对抗环境安全因素后，指标名称依然不变，但应体现在结合安全因素后的内容，实质将有较大改变。

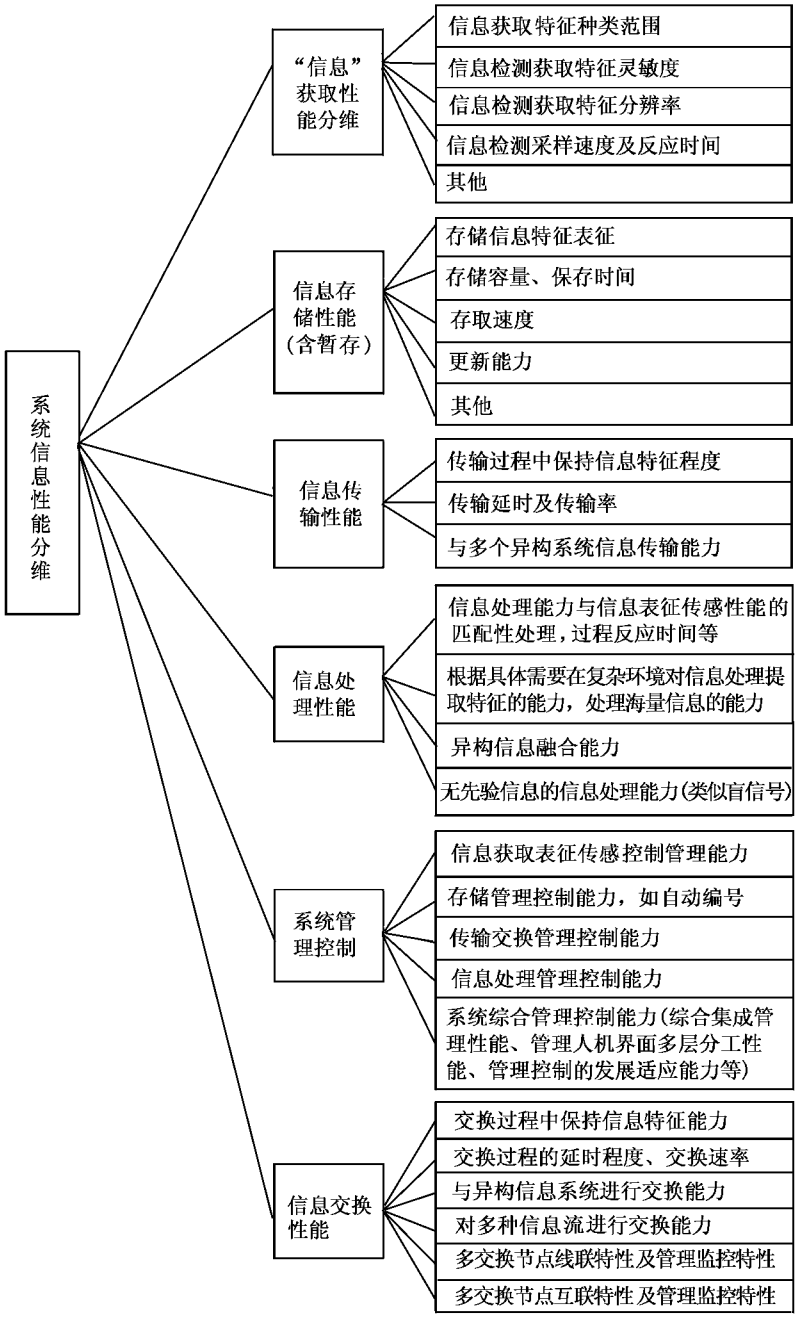


图 5.1　系统理想安全环境下性能分维

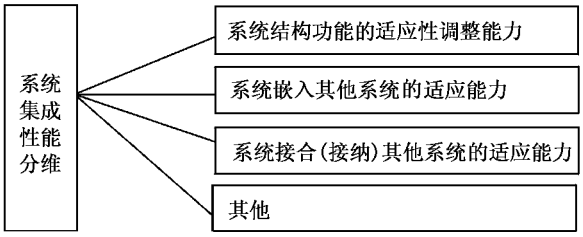


图 5.2　系统集成性能分维

注:本分维主要性能是面对发展而建立的,面对未来总是非常困难的,尽力科学地考虑就会取得一定成效。

二、系统使用性能维

系统使用性能维主要涉及成本,使用方便性及安全性。

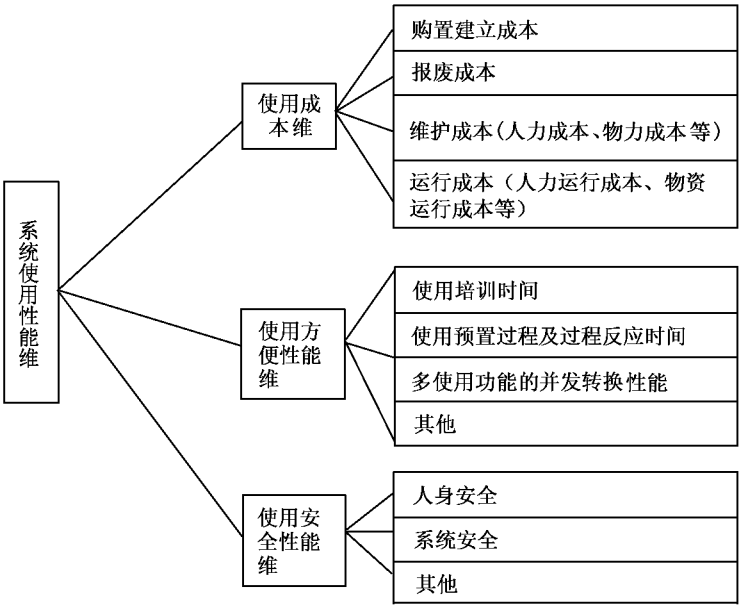


图 5.3　系统使用性能分维

三、系统安全性能维

由现实信息系统的安全性能对应本指标体系而言，大部分系统处在发展阶段，功能不够完备且大部分安全功能属于基本安全性能分维的内容。动态检测快速反应，采取阻断攻击能力尚处在原始起步阶段，是深层次、难度很大的科技问题，有待大力研究。

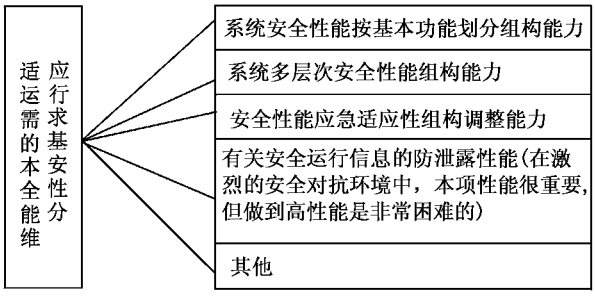


图 5.4　适应运行需求的基本安全性能分维

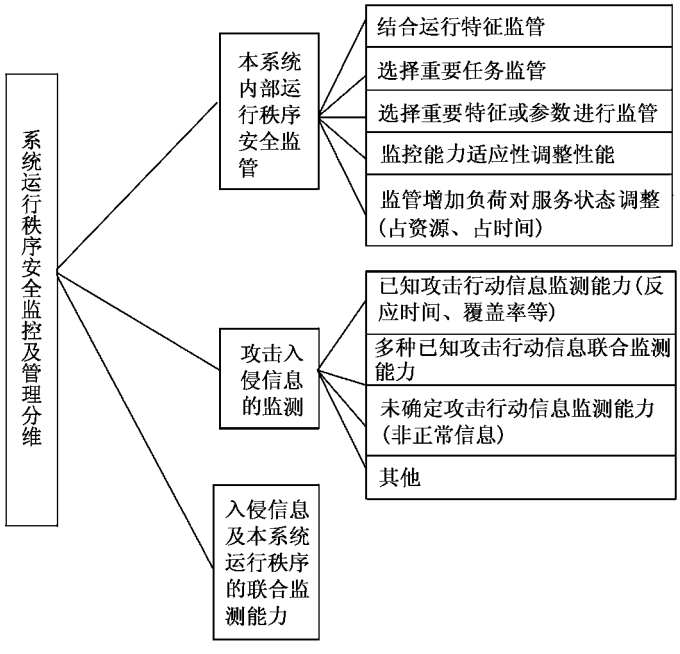


图 5.5　系统运行秩序安全监控及管理分维

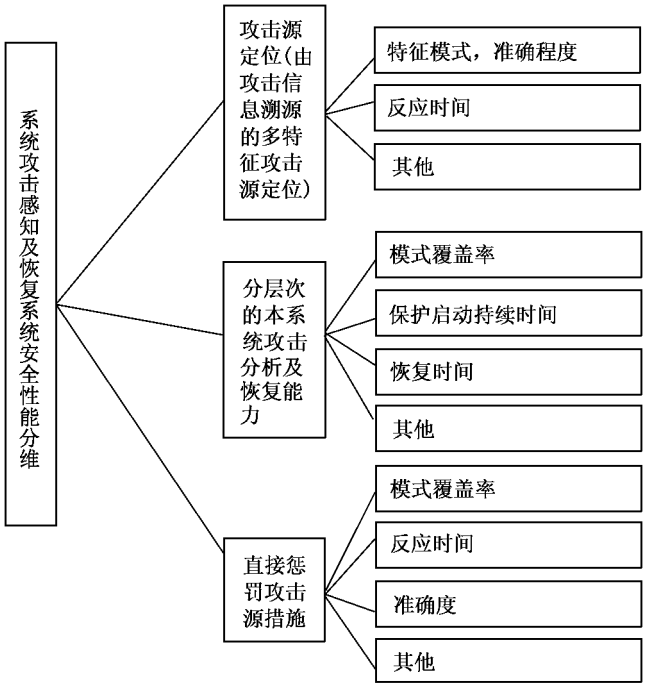


图 5.6　攻击及恢复系统安全性能分维

注：系统性能各维间存在相互制约关系，形成具体性能指标系，是综合协调的结果。

5.2.3　系统指标测度的概念及安全对抗性能占位分析

实际信息系统的设计研制、检测、评估工作中，由于复杂的性能指标体系及各项指标性质不同，缺乏可比性，给原本已非常困难的指标综合运筹增加了更大困难，因此引入测度概念，作为可比性的基础，为指标体系分项间建立可比较的测度奠定基础。

一、测度的概念

测度 P 被定义为环 λ 上集函数的集合，如满足下列条件则称 P 为一测度。

设 $\varnothing$ 为空集，则 $P(\varnothing)=0$；对任意集合 $A\in\lambda$，$0\leqslant P(A)\leqslant+\infty$。

$\{A_n, n>1\}\in\lambda, A_i\cap A_j=\varnothing(i\neq j)$ 且 $\sum_{n=1}^{\infty}A_n\in\lambda$，则

$$P\left(\sum_{n=1}^{\infty}A_n\right)=\sum_{n=1}^{\infty}P(A_n)$$　　（可加性）

测度 P 作为集函数的一种表征，可以有各种具体形式表达事物特征。如体积、面积、长短、质量等，普遍化的数学抽象化的表征；如赋范空间中的范数，可看做事物大小之一种抽象概括化表征，它也是一种测度；如概率是一个随机事件集合中表征可能性的测度。根据实际情况，选择恰当的具体表达，对事特进行衡量和评估是一件重要而艰难的工作，同时不同测度进行比较衡量有一个当量转换问题，一测度群间互相合适的转化更为困难。对于复杂性能的定量分析，利用测度进行定量权衡，仍是一种科学概括方法。除了概率作为测度外，人们常用做某件事所花费时间的长短，试验次数等作为测度。应该指出，在实际工作中所确定测度表征中常蕴涵某些前提“条件”及与另外“测度”相关联，从而形成复合函数式的测度，例如一种密码的安全测度（如多位 RSA 密码）在无合适算法，用穷举搜索法及图灵计算机，在某计算速度条件下破译密码时间（搜索次数×每次计算时间）远大于密码运行时间时是安全的。若条件变化，如破密算法不变，但计算机的计算模型变化后解密时间大大缩短（≒原搜索次数×每次计算时间），变为多次并行计算，引起“测度”内涵发生变化，原安全密码变为“不安全”了。这说明利用“测度”概念评估具体事物时有动态特性。

二、利用“测度”对信息系统安全对抗性能“占位”分析

设构成某信息系统的必要措施数为 n，备选措施集合元素数为 m，设每项措施都具有“双刃剑”效应，完成正向功能的得益为 G_i，同时如使用不当（或发生对抗损失）则损失为 L_i，而发生正面效应的概率为 P_{Bi}，发生负面效应的概率为 $1-P_{Bi}$，设定系统的评价测度 P_{Bi}，n 是 m 中根据指标 C 争取大数值的选项。当由于信息安全因素导致损失 L_i 很大，且 $1-P_B$ 很大时，就意味着有值得注意的安全问题应加以考虑，应采取安全措施使 L_i 及 $(1-P_B)$ 降低或避免采用该第 i 种措施。在信息系统的设计中，如果有由于发生安全问题而导致很大的 L 值则表示有安全问题，必须要考虑。当 $(1-P_{Bi})\cdot L_i$ 具有大数值中的 i 项同时又具有重要的 G_i 值，这种情况意味着信息系统既要求服务功能又要求安全性能。这是一类功能要求很高，约束条件很严，完成设计很难的信息系统，如只有功能要求，而没安全原因可能导致重大损失 L 者，则此类信息系统的设计可较少考虑信息安全措施。还有一类信息系统，设计中信息安全方面失误导致的损失 L 非常大，而系统服务功能的得益却不太高，此时设计时应将主要重点放在信息安全性能方面，据以讨论并突出区分信息系统不同特征，将信息系统概略地分为三类，即：

· 第一类　安全对抗性能是信息系统性能指标体系中极重要组成部分，应优先着重实现相应安全措施，以保证系统总体性能合乎要求。

· 第二类　安全对抗性能重要但并不占“压倒地位”，应就重要性能指标来综合运筹（包括安全对抗性能），使得系统整体性能达到可接受程度（求系统可行解）。

· 第三类　安全对抗性能不占重要部分，不着重考虑其实现措施。附带说明本小节内容是 4.3 节原理（系统层次安全对抗原理）具体应用的延伸，由实际应用情况分析，具有高安全性能要求并将安全对抗措施置于系统组构优先位置的信息系统占少数；较高安全性能要求又需

结合其他功能综合考虑进行组构的系统所占比例越来越大，同时其性能要求也日益提高；较少考虑系统安全或不考虑者所占比例将日益减少。

5.3　信息系统安全对抗问题有关的“关系”表征

5.3.1　基本概念

在第三章中较详细地说明了信息安全与对抗问题的主要内容。第四章中，由“道”出发讨论了信息安全领域两个层次原理及建立“共道”、“逆道”三环节对抗模型，本章将延伸讨论各种对抗方法的实际需要，将以前内容作必要延伸。

第三章所述“信息”及“信息系统”发生安全的内涵以及第四章围绕信息系统“道”的斗争在本章中进一步细化：信息系统的安全对抗问题，可以概括围绕系统运行过程进行斗争，即是通过改变运行秩序而人为改变过程（包括重要状态的改变）和保持原定运行过程间的斗争，由于系统的运动秩序是依靠具体的“道”（规律规则）所建立的，所以由基础角度思考研究信息信息安全问题引出了上边所说的第四章内容。现在往细致示面延伸，根据哲学原理，信息系统作为一个复杂事物，在运动中其内部各部分及内外各部分事物必定处在普遍动态的相互联系、关联、影响中，各种关联联系被称为“关系”，重要的“关系”遵循系统理论耗散自组织原理形成运动的规律和规则，因此对抗双方围绕信息安全进行“道”的斗争，便可转至由“关系”（重要者）入手进行研究，我们将扼要地叙“关系”的表征，信息系统所涉及的几类普遍的重要关系（它们也将涉及信息安全问题），实际上各学科领域都在不断研究各自领域的各专门关系，也正在进行研究学科领域间的交融关系。例如数学研究函数、映射及算子等价同构等关系，物理、化学等都在不断研究各种新的关系，如量子物理就是一种微观物质运动关系，而信息和生物交融研究DNA和生物特性之间关系是重要的交融“关系”。

对关系的研究进而所形成的科学定理就是在一定前提条件下，某特种又普遍存在的“关系”（这就联系到“道”），由此可看出“关系”内容及表达形式的广泛性和重要性。

5.3.2　信息系统状态矢量表示及基于矢量的“关系”表征

一个信息系统的状态可用一多维矢量 $\bar{S}=[S_1,S_2,S_3,\cdots,S_i,\cdots,S_n,t]$，各维可由单位向量 $e_1,e_2,e_3,\cdots,e_n$ 作为基，基间并不一定正交（可能存在相关），可根据需要选择，利用多维向量组可以很好表达系统多层次、多剖面状态。

在某一系统层次、某一剖面的状态，根据有关联的因素可决定向量维数，互相无关联因素用向量的正交分量表示，应注意在本层次、本剖面形不成关联分量，但可能通过“关系”在它剖

面发生重要影响的因素也应通过列入状态组中以备更深入分析之用。实际上一个状态也内含关系，它表示“状态”中各分量间关系，“状态”是系统中关系作用的中间结果，“关系”和“状态”有密不可分的联系。

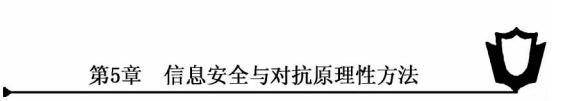
例如，移动通信系统工作过程中建立呼叫关系是缺少不了的，在呼叫关系建立过程中，要用多维向量动态状态来表征过程，其中信源手机号码，信宿机号码是两个重要分量，通过信源手机号与基地台建立连接关系，在寻找信宿机具体过程中很多步骤是利用与电信网（有线）与信宿机方面建立呼叫（除了信宿机在同一小区内），而这段分过程移动基地站也参入其中，有更多层次状态分量介入。由此可看出，一个事物间复杂的相互关联过程要用含时间因素的状态组相互关联而形成。

进一步讨论关系的形成和状态的关系，当某一些“作用”作用于某信息系统上时，系统可用该时系统的状态表示，而“作用”则常可用算子 R 表示，即 $R_1,\cdots,R_i$，而 $R_i\bar{S}$ 表示算子 R_i 作用于状态向量 $\bar{S}$，算子 R_1，R_2 和 R_i 等作用于 $\bar{S}$ 的结果可能是多维向量（包括转化为某分量的正交分量），也可能是标量（一维向量），总之算子可使系统状态起变化。进一步扩充可为系统状态间（也可能是另外系统）的相互作用关系，即 $\bar{S}_i\cdot\bar{S}_j$，其中·表示算子。算子是一个非常广泛、灵活的概念，表示相互间的互相作用，其作用范围是多维的空间、时间联合域。以下结合算子及其他方法讨论信息系统常常涉及算子等表征的几种主要关系。

一、算子等所表征的主要关系

· 直接作用关系：① 正向作用关系，对某事物 A 中某剖面某对象 B 的变化起助长相互作用 C，则称 C 为对事物 A 的 B 剖面的正向关系。例如，利用某相关新工艺可提高某商品质量，则称某新工艺对某产品质量起正向作用。② 反向作用关系：与正向关系作用相反者。③ 正反、向作用关系：在该剖面的某子剖面起正向作用，对另某子剖面起反作用者，很多关系都有此种功能属性，是一种相反相成的体现。④ 条件作用关系：在某条件下起正向作用，在另某条件下起反作用者。如某种细菌感染发病，吃对症药品必须有一定剂量，并持续一定时间，否则病会反复。实际上条件作用关系是约束关系与直接作用关系相结合形成的关系。直接作用关系可用 $R\cdot\bar{S}$ 表示为某种作用算子。

· 约束关系，即指对某指称对象（或某状态）的某种性质（状态）存在时还另外存在某种作为系统运动的限制，这种“限制”对信息系统的运动称为约束关系，约束关系对系统某状态的形成可不起直接作用，只起限制作用。如刑法对社会各种正常活动并不起直接支持作用，它约束、威慑犯罪分子，而对正常活动进行保护（可认为是广泛的间接支持作用）。约束关系多为一组时空关系对系统某“状态”或某对象起约束作用，常在表达关系后加注约束条件，如：$R\cdot S=S_{i+1}$，S 为$(S_1,S_2,\cdots,S_i,\cdots,S_n,t)$，在其后加 $S_{i\min}<S_i<S_{i\max}$，$S_{j\min}<S_j<S_{j\max}$，$t_{i\min}<t<t_{i\max}$ 等。



· 条件关系：即某关系状态存在所需条件，主要分必要条件，充分条件和充要条件。可用以下形式表示：

如在 S_i 为必要条件下，表达形式为

如果 $S_{i条件}=0$（不存在），　则 $S_{j事件}=0$（不成立）

如果 $S_{i条件}=1$，　则 $S_{j事件}=\begin{bmatrix}0\\1\end{bmatrix}$（可成立，也可不成立）

S_i 为充分条件下，表达形式为

如果 $S_{i条件}=0$（不存在），　则 $S_{j事件}=$ 不确定

如果 $S_{i条件}=1$，　则 $S_{j事件}=1$

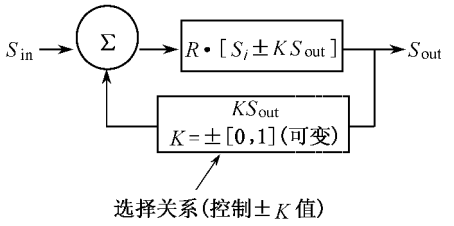
S_i 为充要条件下，表达形式为

如果 $S_{i条件}=0$（不存在），　则 $S_{j事件}=0$

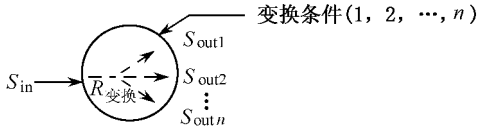
如果 $S_{i条件}=1$，　则 $S_{j事件}=1$

· 联结变换关系（含条件联结变换关系）：即联结变换“关系”组成的关系，它可由关系进行组合构成复杂的关系集合，多数情况下为有条件的联结变换，此时可与上述条件关系联合应用。主要的联结变换关系有：合成关系、分解关系（分岔关系）、变换关系（条件变换关系，包括了“0－1”变换关系）、选择关系（条件关系的一种）、反馈关系（还可再分正反馈与负反馈关系，正反馈关系加一定条件可形成突变关系），由以上讨论可以明显看出利用多个联结转换关系可以组合形成更复杂、更起作用的关系集合来表征信息系统的运动状态，以下举例说明各种关系组合形成更复杂关系。

· 作用关系、条件关系及反馈关系的组成



上图表示，由合成关系、选择关系（控制±K值）、变换关系等组成的闭环及馈关系图。



上图表示，当不同变换条件时 $R_{变换}$ 有不同变换输出 S_{out1}，S_{out2}，…，S_{outn}（也可理解为选择关系与变换关系相结合形成多种变换输出的选择）。

二、“关系”的时间特征

时间空间是物质存在的基本形式，关系中的互相作用作为一种时空运动，它必然与时间有关，上述各种关系与时间的关系结合形成各种各样性质（也称关系的时间特征）大致有下列几种：

· 延时关系，“关系”间的延时状态，$\overline{S}_i(S_1,S_2,\cdots,S_n,t)\cdot R_t=\overline{S}_i(S_1,S_2,\cdots,S_n,t-\tau)$。

· 持续关系，关系的作用持续一段时间（也可很短），$\overline{S}_i(S_1,S_2,\cdots,S_n,t)\cdot R_t=\overline{S}_i(S_1,S_2,\cdots,S_n,t_0<t<t_1)$。

· 时间后效关系，一般情况下某种“关系”的作用会延时产生，然后再随时间增加逐渐减弱，减弱周期有长短区别。因为事物发展的复杂，有时会直接有否定之否定现象，例如，某种药（例如四环素）已经被新的抗生素代替，而被废弃不用，当有一种新病毒在社会（用药环境中）发生，对新药有抗药性，一旦发生这种细菌（病毒）形成流行病，则新抗生素无效而老药很可能有效，现在四环素就发生这种情况。$\overline{S}_i(S_1,S_2,\cdots,S_n,t)\cdot R_t=\bar{s}_i(S_1,S_2,\cdots,S_n,t)\cdot e^{-\pi t}-\bar{s}_i(S_1,S_2,\cdots,S_n,t-T_0)(T_0\gg\tau$，当 $t<T_0\quad\bar{s}_i=0)$。

· 时间反转关系，$\overline{S}_i(S_1,S_2,\cdots,S_n,t)\cdot R_t=\overline{S}_i(S_1,S_2,\cdots,S_n,\tau-t)$。

· 时间压缩及放大关系，$\overline{S}_i(S_1,S_2,\cdots,S_n,t)\cdot R_t=\overline{S}_i(S_1,S_2,\cdots,S_n,t/\tau)$。$\tau>1$ 为压缩，$0<t-1$ 为放大。

· 各种时间关系组合构成复杂时间关系。

· 时间关系的作用可用时间算子来归纳理解。

三、关于 5.3.2 小节内容在应用中的说明

5.3.2 小节较详细地讨论了用以表征信息系统运动存在的几种“关系”的性质和作用，实际上形成了用“关系”代表系统的转化“映射”，有了这个“映射”和转化概念就可将本章后续讨论的系统层次安全对抗方法与技术层次方法，以“关系”为结合点结合起来而不致形成在理论体系上的“空缺”。在实际应用中形成了各种原理方法作用于信息系统的落脚点，为了加深上述概念，在 5.3.3 小节中用实例说明各种“关系”，形成移动通信系统宏观序的机理和形成“序”的简要过程。在 5.3.4 小节延伸讨论了信息系统几类重要的具体关系集合，它们的状态不单影响信息系统服务功能也密切关联着信息系统的安全状态，这也是为研究具体安全技术进行铺垫和奠定基础。

5.3.3 以移动通信近期发展为例说明关系—自组织宏观有序关系的形成

复杂系统宏观层次自组织序的形成体现了耗散自组织理论作用（道），实制上是由系统内外多种关系相互作用所形成，并扼要表征了系统的生存。

正向驱动主要因素：社会发展、经济发展驱动通信系统在任何人、任何地点、任何时间、任何状态进行通信方面前进一步，即人们需要在移动状态进行通信，并构成覆盖广域的通信网络（即移动通信系统）。

约束条件关系：(1) 第一步以语音通信及短信息为主。(2) 需能在广大覆盖地区构成通信网络。(3) 使用方便可靠与普通电话相当。(4) 手机体积、质量（含电池质量），应足够轻小。(5) 耗电及电池工作时间应足够小和足够长。(6) 使用成本低（不同类用户具有不同门限，成本越低用户可能数越多）。技术层次形成多个约束条件集合，如：(1) 多用户面对有限可用信息资源间矛盾的解决，移动用户与联系基地站接力交接、远地漫游问题的解决。采用 TDMA 和 CDMA 优于 FDMA 的分析决策，与电信网络联合工作解决长途远距离漫游。(2) 利用技术发展减轻使用成本约束，（最初为电话通信的几十倍，连续降至十几倍及几倍，个人手机购置费呈十几倍的下降）。利用微电子集成技术形成了成本下降而用户数不断增加、运营获取利润并互动的良性循环。“约束条件”是多层次动态变化，并随社会发展及竞争机制的存在而变化，约束条件的极限不能超越规律形成的自然决定性，如 GSM 的基地站范围内用户数是由体制及所分配资源所决定，不能要求超出极限值的用户数。

多层次关系交织反向作用关系，它同时起排斥和刺激作用，如：(1) 与约束条件最低允许限的超差构成反向扼杀及录求出路正向推动作用关系。(2) 与现有生存相似系统的功能的微小差别主要构成竞争作用关系。(3) 与同类竞争者的微小差距及反差构成反向作用关系，克服各反向作用必促使发展是相反相成规律的体现。

支持关系是相互作用中所形成的一种起支持作用的关系集合，往往具有开放性质，延伸到很多层次直至科学基础。如大规模高频功率集成芯片及嵌入式系统技术，表面安装技术、数字技术及软件协议技术（开放式结构），高级软件技术及网络控制管理软件技术，与电信网络结合漫游寻址技术。以上为技术因素形成直接正向支持关系，支持关系在起支持作用时不可避免产生新约束关系以及潜伏的反向作用。

在移动通信中有众多联结关系，如：用户数 N 的增加（在门限数以下）形成正反馈关系，GSM 与 CDMA（宽带）的特性加以其他因素，构成选择 GSM（TDMA 为主）的体制选择关系。

以上几类关系互相作用，形成了我国移动电话现行主流体制 GSM（CDMA）体制，全国已形成大面积覆盖（包括沿铁路线大部分覆盖）并实现部分国际间移动通信，移动用户数达世界第一位，而且还在不断增加。业务仍以话音为主，加以短信息，形成移动通信系统的存在特征。随着用户进一步增加（特别是较发达地区），将达到基地站内用户数的极限。此时，必将产生具有新“序”的移动通信系统，如第三代移动通信体系或势必出现现行系统的重大改进。

各种关系的作用示意框图如图 5.7 所示。

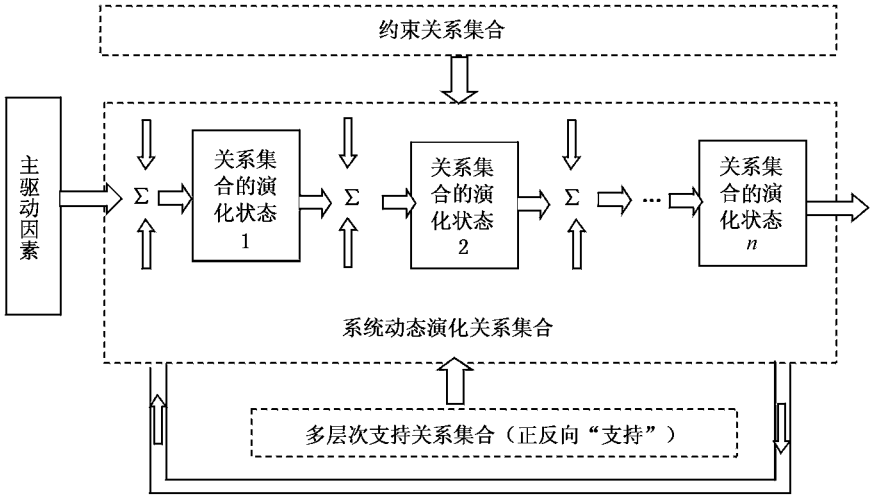


图 5.7　各种关系间的相互作用自组织形成宏观序的过程示意

5.3.4　影响信息系统安全的几种重要关系

在信息系统中，可能影响信息系统正常工作，形成安全漏洞造成损失的关系非常多。如果凡可能影响系统工作秩序，违反运行规律的关系，不论可能造成损失的大小都加以考虑研究，则数量很大难以进行。在此选择主要者加以讨论。

一、算法及算法语言

算法是精确定义的一系列规则，它指明如何从给定的输入信息经过有限步骤产生所需要的输出。算法具有五个特征：① 算法必在有限步骤内结束，称为终止性；② 每一步必有精确定义，而且规定是严格无歧义的；③ 算法在运行前要具备初始信息；④ 算法一般在终止时有确定的结果，输入和输出信息之间有一定的逻辑关系；⑤ 算法的存在，必须同时考虑在一定时间、空间内有可以实现的条件。

算法语言是描述算法，面向解题过程的程序设计语言，算法及算法语言的“算”是广义计算，绝不仅限于算数，或数学“之算”，而是指有规律的计算步骤的集成（符合图灵机模型为基本条件）。算法和算法语言在信息安全与对抗领域中的所以重要，在于攻击方与反攻击方都需要它，攻击方有些攻击的得手是通过破坏算法利用算法中的核心步骤来达到，例如对密码算法而言，掌握新的有效算法就意味着取得在密码领域有较多优势，可以用来攻破密码的保密性。而反攻击方则应掌握算法的核心，尽力避免其为攻击方所利用。

二、系统运行管理软件

一个较复杂的大型信息系统，系统运行管理软件，实质上也是一个复杂的软件系统，它一般由很多子系统整合而成，子系统又可分为子系统，再细化分为软件模块等。算法又往往是构成软件模块的基础，在不同信息系统，各种专门系统运行的管理软件往往有专门的名称。

如计算机领域中的系统软件，其中操作系统、编译系统都是通用计算机系统软件中的子系统。当计算机组成网络后，网络中的运行管理软件系统又常用网络操作系统。又如，电信网络中很著名的 7 号信令系统，实际上是其运行管理软件之一，电信系统开展的各种新业务，其支持核心是各种相应的新运行管理软件，它们建立并融入原系统软件并形成新的全系统运行管理软件系统，其他各类信息系统（特别是大型复杂信息系统）都有各自的运行管理软件系统。它与应用层密切相联，与应用软件相结合，才能形成功能优良、使用方便且安全可靠地发挥应用效能的软件系统，附带指出，很多功能和技术先进且敏感的信息系统（如卫星通信系统）内部核心管理软件列入关键技术中是严格保密而不出售的。

基于信息系统的运行管理软件在信息系统中客观重要性，在安全领域同样具有重要意义。攻击方一旦控制了被攻击方运行管理软件，则很大程度上对系统运行多种攻击的目的都将较容易达到，即使攻击方达不到很大程度上掌握系统运行软件，只要找出其中一些漏洞就可实施相应的攻击；而在信息系统的营运方，使用方（抗攻击方）保持系统运行管理软件正常工作，免遭攻击破坏是件艰难的事。主要原因有：其一，有大型软件的正确性、无错误的验证尚无理论上的方法，有的属于数学上的 NP 难题，因此漏洞不可能完全避免，有漏洞就会引致攻击。其二，由于软件本身的复杂性，要全面分析可被利用或作为攻击之处，即前面所提出“共道—逆道”概念和模型中所有可以反其道而行之处，则更是难上加难。除了复杂性外，攻击方式还有不可知、不确定性因素，追求绝对安全是不可能的，也违反了发展进化不会停顿的基本概念。计算机内病毒主要机理是利用系统运行管理软件的工作机理，夺取其运行控制权，进行病毒繁殖及破坏作用，而企图设计一种能抗各种病毒的操作系统是不可能的。其三，软件系统是开放性的，即要与应用者打交道，而不是孤立封闭状态，攻击者可伪装成应用者与管理运行软件打交道进而伺机攻击破坏。

三、协议

协议的含义是协商议定共同遵守的约束和步骤，用以共同完成某种、某类事物。一个协议完备并起作用，必须具备以下特征：

- 与协议有关的当事人各方，事先必须充分了解协议内容，并知道遵照协议执行的各具体步骤。
- 当事人必须同意严格遵守协议方得入局，并同意接收遵守协议情况的监督。
- 协议内容本身必须是清楚的，有明确定义，不会由于含混而误解协议内容。对完成事

物而言必然是完备的，对完成事物过程中各种具体情况都应涵盖，而有规定具体动作、协议的步骤有固定执行次序，不能跳越执行。每个步骤包括内容为广义的计算（含定理、认证、检测等）及信息传递。

由协议定义可看出，协议涉及的内容非常广泛，在各类信息系统工作时离不开支持其工作运行的各种协议组成的协议子系统，它是信息系统结构中重要软件组成的基础构件之一，也是信息系统运行所不可缺少的。信息系统安全协议是系统协议的重要组成部分，它本身又包含了各种协议。如利用密码保护信息内容不泄露，在系统运行中应首先建立密码运行协议，以保证密码安全有效运行。此外非专门为了保证安全设立的安全协议，往往需考虑安全因素相配合的措施和功能，这是一种系统的客观需要，这就使得信息安全对抗因素的考虑范围扩展到信息系统的协议体系，所以重要的应建立信息安全对抗概念。由于以前安全对抗问题没有现在严重，因此，IPV4 协议没有过多考虑安全问题。

四、个性关系集合

事物个性的关系及个性关系的组合可形成个性关系集合。

个性（即特殊性）是一个相对概念，在一定范围内是特殊性，在另外更具体更小范围内可能就是普遍性。如某些信息系统的协议，在具体关系作用范围形成个性的体现，但对于它的适用领域又呈现共性、普遍性—可普遍适用性。个性（特殊性）与共性还可组合而形成在原共性范围内的特殊性，如信息系统所用某种协议（在其适用范围）呈现共性，一旦加入具体对象（如信息地址、信宿地址）则在原适用范围呈现特殊性。在信息安全领域共性相对而言不如个性对安全性敏感，因此与组合形成个性情况下，组成个性的个性更应注意保持其个性的封闭。个性有多种表现形式，概括说来运动特殊状态的表达即可被认为是特殊性的表现，因此用信息来表达特殊性，特殊性作为一种特殊的运动形式是不能更改的，在实际活动中，特别是在信息系统中往往是利用特殊性的表达形式进行交往，例如个人代号、IP 地址、个人使用口令、个人密码、个人的数字签名等，用这些特殊信息代表具体的个人，进一步而言还有特殊性的个体间进行交往，构成特殊性过程，例如某甲与某乙进行保密通信，签订双方协议，这些过程也可认为是个性关系组合。

5.4 系统层安全对抗方法概论

人们称实现某种目的所遵循的重要路径和各种办法为“方法”，“方法”的产生是按照事物的机理、规律找出具体的一些实现路径和办法，因此对应产生办法的“原理”族（集合）是“方法”的基础，在信息安全与对抗领域上所讲述的原理是本小节所叙述方法的基础，重要的问题是按照实际情况运用诸原理灵活地创造解决问题的各种方法。在本小节中，只能叙述一些指导性方法，或称原理性指导方法。

“方法”按其作用机理也可分为几个层次。

·第一层次即总体层次，全局性方法。该层次方法是针对信息安全对抗领域矛盾演化发展，研究其发展规律、发展方向、发展路径的方法以及结合具体实际研究发展路径、发展进程中掌握控制关键点的方法，这层次的方法实质上是思维方式性方法，是研究具体方法的方法，起着发展战略作用，对认清某领域的发展态势、发展规律和正确决定发展路径起着重要作用。

·第二层次的方法是方案性方法。即针对某些（或某类）信息安全问题结合实际情况研究其内在发展运动机理。挖掘一切可利用因素，形成解决某些信息安全问题的方案性方法。本层次，考虑解决问题的范畴和性质对比第一层次范围要具体深入，属于总体性质即同时具有总体性质又具有具体问题性质，这类方法支持形成正确科学总体方案起重要作用。

· 第三层次是具体技术性方法，这类方法是直接利用各相关技术面对问题进行解决，应用这类方法的要点是选择相关有效“技术”，使实施效果明显，而付出代价较小。

对某种方法而言，其效果性质往往并非绝对局限于某一层次，而有可能兼有几个层次的作用意义。在本小节中，主要讨论前二层次方法，附带第三层次方法。三个层次方法间相互关系有支持也有制约，构成方法整体。

5.4.1　“反其道而行之相反相成”方法（以下简称“方法”）

本“方法”兼有两个层次作用。

首先具有指导思维方式功能，属第一层次方法，具体表现在：① “方法”普遍适用于对抗双方，因为对抗双方都必须应用本“方法”，谁不应用谁必吃亏。然后双方都必须进一步考虑己方与对方同时应用本方法，可能形成复杂交叉对抗环境。② 在对抗展开的时间、空间普遍应用本方法，即在各种类型“对抗空间”各层次、各剖面的“对抗”行动；对抗过程中全时域历程，即过程中各时间阶段、分子段、片段等；对抗过程中时空（广义）域的联合展开中都应有所应用。③ 由于“在共道基础上相反相成”原理是对立统一律在信息安全对抗领域的具体化，“原理”起核心作用，本“方法”是“原理”的应用，起核心作用，“相反相成”体现深层次辩证机理，是一种思维方式也是一种思维方法。

本“方法”在第二层次发挥核心机理作用，对形成方案性方法起重要作用，体现在：① “方法”可以与第 4 章相关原理相结合，根据实际情况挖掘“对抗”内在机理，巧妙地形成各种有效对抗方案性方法（这部分内容，后续进行专门的讨论）。②“方法”中“相反相成”部分往往巧妙地利用各种因素，包括对方“力量”形成有效对抗方法，其基础是 4.3.4 小节原理（“在共道基础上反其道而行之相反相成”）中的“相反相成”部分，该小节中应用举例提前说明了本“方法”与 4.3.4 小节原理相结合所起的作用。

在第二层次本“方法”独自或与其他原理结合，形成信息安全对抗领域的技术方案性方法，现举例说明思路如下：① 对于对方对抗行动的“条件”（充分、必要、充要）实行反其道而行之以破坏

对方的行动。② 对于对方对抗行动的机理直接实行反其道而行之破坏其行动效果。③ 调整己方对抗行动机理使之与对方对抗机理间关系为正交性质，使对方对抗机理对己方机理不发生关系，从而消除对方行动效果，这是在对抗层次的广义“反其道而行之”。④ 利用新量子“信息”具有不同于现“信息”具有的特征，而是具有不可触及性的新特征，即如果外来任何“影响”触及工作机理则它立刻发生变化，变离正常状态以示有外来影响介入了系统而告警。

“方法”的具体应用举例如下：在通信或雷达碰到干扰信号对抗时加大通信功率以压制干扰。在信息系统工作过程利用某种信息媒介受到对抗攻击时，则更换为另一种工作机理不同的信息媒介，以利用与攻击机理无关的机理工作应对攻击，如更换电磁波工作波段便是最普适之例。正在研究的量子通信中量子编码便是以“不可触及”特性，灵敏感知存在攻击以保证正常通信。在下面三小节将就本“方法”与其他重要原理相结合形成一些技术性方案的方法加以举例说明。

5.4.2 “反其道而行之相反相成方法”与“信息存在相对性原理”(4.3.2 小节)、“广义空间维及时间维信息的有限尺度表征原理”(4.3.3 小节)相结合可以形成在信息进行攻击或反攻击的方法

一切对抗的基本机理是反其道而行的，因此在信息对抗领域遵循此机理的反其道而行之方法是基本方法，应用中要结合“信息”的特征是基本前提，因此结合 4.3.2 和 4.3.3 小节原理是重要的。

在应用电磁信号为信息媒介的情况下，进行攻击的有效方法是产生攻击信号、掩盖对方信号使对方难以区别(在时域、空域上)原信号，而反攻击方则在所有信号在时空中只占有限尺度原理基础上，利用己方与攻击信号间的各种存在差异找出信号间的差异，从而区别信号与攻击信号，这是利用 4.3.2(“信息存在相对性原理”)、4.3.3(“广义空间维及时间维信息的有限尺度表征原理”)等小节原理实行互相之间“反其道而行之”。

现代信号处理就是按此原则具体实现(如时空变换、多阶累量分析、现代谱分析等)的一类方法。

5.4.3 “反其道而行之相反相成方法”与“争夺制对抗信息权及快速建立系统对策响应原理”(4.3.6 小节)相结合为对抗双方提供的一类对抗技术方案性方法

争夺率先掌握对抗信息及其内涵是对抗双方都十分在意的事，因为只有在掌握制对抗信息权才能在后续对抗中占主动和获胜。在双方围绕“对抗信息”的斗争中，“反其道而行之相反

相成”是一种重要方法，在多层次场合中起作用，与“双方争夺制信息权及快速反应原理”相结合使运用得体的一方能在相应的对抗中占优势，现简要分析两方法结合形成更有效方法的机理。“对抗信息”之所以重要，其根本原因是对抗信息与对抗行动间的对应关系，即由“信息”推断出行动的机理和意图。对抗双方都竭力获得对方的“对抗信息”以利进行对抗，又防止对方获得己方对抗信息，破坏己方行动。在做法上双方有相同之处，但又各自反对方而行。具体的“反其道而行之”有多种方法：可以隐藏对抗信息的存在，也可藏匿和误导信息内容，还可以在时间维上进行斗争，延误对方知晓的时间，从而达到阻挠对方及时反应及采取对策。结合应用“反其道而行之相反相成”与“争夺制对抗信息权及快速反应”原理形成对抗方案过程中，需要更深层次“原理”结合的考虑。例如某一行动方考虑对抗方案过程中，事前应考虑到对方也会在围绕对抗信息的斗争中，必然要采用多回合的“反其道而行之相反相成”、“共其道而行之相成相反”方法。因此这一方必须有针对性灵活地“运用反其道而行之相反相成”与“共其道而行之相成相反”的组合以对抗对方的组合，形成动态对抗过程，两原理的组合具有多种灵活性。应结合具体情况和技术方法决策性地确定，例如可以“反其道而行之相反相成”方法对抗对方反其道的方法，也可用以对抗对方“共其道而行之相成相反”方法。事实上在复杂的信息安全对抗领域内，“反其道而行之相反相成”及“共其道而行的相成相反”既是规律，又是基本思维方法，还是形成技术性方案的重要方法，其重要性在多处都有所显示，而精彩的发挥应用多成为信息对抗领域的典型范例。

5.4.4　“反其道而行之相反相成方法”与“争夺制对抗信息权及快速建立系统对策响应原理”(4.3.6 小节)、“技术核心措施转移构成串行链结构而形成脆弱性原理”(4.4.3 小节)相结合形成的一类对抗技术方案性方法

“反其道而行之相反相成方法”、“争夺制对抗信息权及快速建立系统对策响应原理”(4.3.6 小节)与“技术核心措施转移构成串行链结构而形成脆弱性原理”相结合，可以形成一类技术方案性方法，使其在对抗过程中起重要作用。例如对抗双方都意识到自己的措施串联链中的薄弱环节最易由对方的反其道而行之而出现问题，应多加防范，这样便形成了通常意义上的“薄弱”环节、“不薄弱”和“薄弱”环节的转移和不固定情况。双方在对抗过程中选择对抗切入点时需根据实际情况所涉及的多种因素，在双方都实施反其道而行之前提下进行斗智的博弈选择。实际情况是对抗双方在反其道而行之核心机理支配下与其他原理相结合构成更复杂、更实际的对抗环境，同时也是发挥人的主观能动性和智慧的场合。

5.4.5 “反其道而行之相反相成方法”及“变换、对称与不对称变换应用原理”(4.4.4 小节)相结合指导形成或直接形成的一类对抗技术方案性方法

“对称变换”与“不对称变换”在直接含义下互为对方的否定,这是两者的对立性,从结合角度上它们是可结合的(对称变换结合不对称变换)、可转换的(有条件的转换),由此呈现统一性。“对立统一”,在辩证意义呈现的“相反相成”特性非常重要,如不对称变换与不对称逆变换构成一个对称变换(压缩变换与解压变换、调制变换与解调变换、加密变换与解密变换等),以上内容可以用于对抗场合。如对抗一方将欲对对方进行隔离的某些事物特性,利用对称和不对称变换及“反其道而行之相反相成”可以实现;利用变换置对方付出代价很大(耗损)的不对称位置,而己方则利用具有的条件,将该事物某性质处于变换对称位置,经变换“性质”不变而不受影响。这种对抗技术方案性方法有多种,如己方利用密码保护通信内容不泄露令对方因不知密钥而需花大量精力、时间破密,从而丧失了获得保密内容的时机,使得使用密码通信方内容保密成功。这时对另一方因条件不同就构不成对称变换而承担不对称变换的损耗,这种损耗值可能很大。

一个较复杂事物常由其多层次、多剖面性质所组成,一个变换(或变换群)某个剖面对变换有对称性质(变换前后该剖面代表的性质不变),另外剖面性质对变换往往就不具对称性质。在对抗场合、这些特点可用于“对抗”,如经变换将对方行动属性置于变换后的谷点,己方某属性保持变换不变性,这样一种“变换”是一种有利己方的对抗行动。利用阵控天线在空间将接收波束零点对准对方干扰方向,峰点匹配己方,便是一种应用(当对抗对方和己方所占空间有区别情况下),这是另一种对抗与不对称变换相结合用于“对抗”中的例子,由以上叙述可看出“反其道而行之相反相成”与对称、不对称变换相结合是一种对抗技术方案方法,可以形成多种具体的对抗方法。

5.4.6 重视对抗复合式攻击方法

复合攻击指攻击方组织多层次、多剖面时间、空间攻击的一种攻击模式,其特点是除在每一层次、剖面的攻击奏效都产生信息系统安全问题外,实施中还体现在对对方所采取对抗措施再形成新的附加攻击,这是一种自动形成连环攻击的严重攻击,因为它使抗攻击方处在左右为难的困难境地,造成不采取反击措施不行,采取措施也不行。

例如攻击火控系统雷达时,采用干扰及反辐射导弹复合攻击模式,干扰雷达的跟踪精度,当雷达增加发射功率以抗干扰时,此时用反辐射导弹攻击雷达就容易瞄准而较易攻击成功。又如对计算机互联网进行复合攻击的一种模式为,先进行某种掩护性攻击(如发送佯攻信息

包)吸引入侵检测系统 IDS 启动监控,如 IDS 大部分能力用于监控佯攻,则主要攻击就较易突破 IDS 监控,如 IDS 不监控佯攻,不采取措施,则佯攻也起攻击效果。

对抗复合攻击的重要原理为:加强对抗信息斗争优势,由对抗信息中尽快正确理解攻击,即掌握攻击目的,攻击机理等攻击要素。采用反其道而行之对抗措施,可利用对方攻击次序差异(时间、空间)各个击破。也可采取这样一种方法,使对抗攻击措施中不提供形成附加攻击的因素。这样使附加攻击无实施条件。如火控雷达利用快速反应性能先发攻击敌方飞机并不增加功率,形不成或减少敌机反辐射导弹快速瞄准火控雷达机会,以减少复合攻击的概率。有效对付复合攻击是件很复杂的事,在不可能避免攻击时,选择损失相对小者。

5.4.7　共其道而行之相成相反方法

在第四章中介绍了“共其道而行之相成相反”原理,根据这一原理,双方也可形成各种对抗性方法,并结合了一些实例,在本节中将就“对抗过程”的展开作进一步说明。

“对抗过程”是由下列多特征因素动态交织组成:对抗双方、对抗特征、对抗展开空间、对抗延续过程展开(时间维)。

“相成相反”展开为:某方在某层次某过程对于某事相成;某方在某层次某过程对于某事相反。前后两个“某方”不一定为同一方。在实际对抗过程中,对抗双方都会应用“共其道而行之相成相反”方法。类同 5.4.3 小节所叙述情况,应灵活针对性地应用本方法(与“反其道而行之相反相成”)组合以对抗对方的“组合”,其中本方法可以对抗对方的“反其道”的方法,也可对抗“共其道”的方法。

例如,A,B 为对抗双方,A 方欲收集 B 方的重要“信息”,则 A 方必须设法进入 B 方信息系统,B 方可以阻挠非法进入自己的信息系统,也可以再备一手,即针对重要信息,反向设置假信息以对抗 A 方。对 A 方而言,第一阶段第一层次的“成”,反而形成效果层次或第二阶段之败(反向结果)是“相成相反”;对 B 方而言,可利用第一阶段第一层次对自己的不利(反),反向取得第二阶段更深层次的获胜,可以认为这是一种“相反相成”。由上述论述可看出,信息安全对抗是复杂的多层次、多剖面,由子片段、子过程、过程组成的,由于双方都竭力隐藏己方意图,希望摸清对方意图,企图制胜,使对结局具有不确定性和意外性。信息对抗结局往往事关重大,信息对抗双方都在不遗余力地研究对抗制胜的规律、办法,从而使问题发展得日益复杂地相互交织斗争,在交织状态中分析“反其道而行之相反相成”与“共其道而行之相成相反”具有相互交织与转变特性。这是在实际应用中很值得注意的特征,由交织转换特征我们容易得出以下认识,共其道而行之相成相反方法在信息安全对抗领域具有思维方法和方案性方法的性质特征,并可与第四章相关原理相结合,扩大发挥作用的范围。

5.5 信息系统安全与对抗技术性方法

5.5.1 信息隐藏(现代密码学)

在信息系统工作过程中将信息进行隐藏是保证系统安全的重要方法的一,隐藏是对不遵守秩序对象非法获得的防御性方法。本节将分析介绍各种原理方法,实际应用中尚需一系列配套关系,如相应协议、算法等。同时通过这些关系根据实况可以采用几种方法配合叠套使用,以获得更理想效果。

一、信息内容的隐藏—密码技术的应用

其基本概念为:通过使用密钥的加密变换,将信息内容变为密文而防止内容泄露。合法用户接受密文后,利用解密密钥将密文经解密恢复明文,其原理过程如图 5.8 所示。

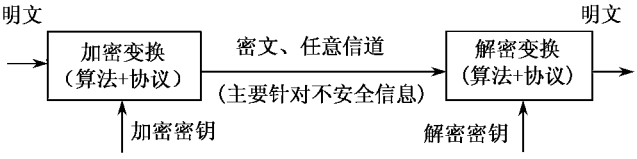


图 5.8 信息加密、解密基本原理

对于合法用户而言,利用对明文的对称变换(加密、解密变换对),使明文无法变化,违规用户因其得不到密钥而无法进行解密变换,得到不明文(处在非对称变换状态)。由此可明显看到,利用密码技术除了密码技术本身的保密性,密钥的合理使用是不可回避的关键,这是第四章所提及问题核心不断转移原理在应用中的体现(将在第六节中通过举例加以系统性叙述)。按密钥类型密码体体系可分为:公开密钥(加密密钥)系和对称密钥系(加解密用同一密钥)密码技术的测度衡量可由两方面内容组成,即安全测度和其他功能及使用性能测度组成。

关于密码体制,可分为序列密码体制和分组加密体制。

分组加密:其加密方式是首先将明文序列以固定长度进行分组,每一组明文用相同的密钥和加密函数进行运算。一般为了减少存储量和提高运算速度,密钥的长度有限,因而加密函数的复杂性成为系统安全的关键。分组密钥常用 Shannon 所提出的迭代密钥体制,即把一个密钥技术强度较弱的函数经过多次迭代后获得强的密钥函数,每次迭代称为一轮,每一轮由上一轮的输出和本轮密钥经过替代盒进行加密。每一轮的子密钥都不同,由主密钥控制下的密钥编排算法而得到。分组密码设计的核心是构造既具有可逆性又有很强的非线性的算法。加密函数重复地使用了代替和置换两种基本的加密变换。即 Shannon 于 1949 年发现隐蔽信息的

两种技术：混乱和扩散。混乱是改变信息块使输出位和输入位无明显统计关系；扩散是将明文位和密钥的效应传播到密文的其他位。另外，在基本加密算法前后，还要进行移位和扩展。单密钥体 DES 密码算法，是一种典型的分组加密体制。

序列加密：另有一种密码体制为对明文每一比特进行密码变换，这种密码体制称为序列密码体制。例如，语音保密通信中就较多采用，其具体实现方法，可用硬件实现定静算法，而临时输入密钥与固定算法相结合实现安全的秘密通信。密钥形成也可有多种方法，通常利用一组较长的随机序列，可用移位寄存器产生，再经各种非线性处理，如删节某些位数、压缩合并等，从而形成一个安全密钥。此密钥为对称的，加密解密共用（必须安全传递），其工作示意如图 5.9 所示。

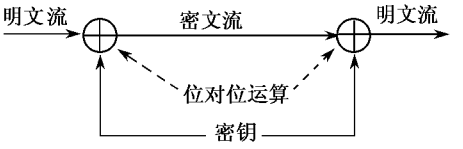


图 5.9　序列加密工作示意图

1. RSA 公开密钥密码

此密码的名称是由三个发明人姓氏第一个字母组合而成，它的安全性是基于数学的大素数分解难题，保证密码安全性。

① 加解密过程分析。设明文数字化表示为 X（可分段为 $x_1, x_2, \cdots, x_m$），选取 n 为某大数，$n=P \cdot Q$，其中 P 和 Q 为两素数。a 和 b 满足：$a \cdot b=1$ 模 $(P-1)(Q-1)$，则 n 和 a 公开，a 为公开密钥（可由密码管理中心管理，或安全途径传至信源方使用）。

加密过程为：X^a 模 $(n)=C$，其中 C 为密文，当 $X>n$ 则分组达到 $x_1, x_2, \cdots, x_m<n$

解密过程为：$(C)^b=X^{ab}=X$

证明恢复明文的解密过程，即证明 $X^{ab}=X$

根据费尔马小定理：若 X, n 互质，则 X^n-X 被 n 整除，即：$X^{n-1}=1$（模 n）

再假设 X 与 P, Q 互质，则按费尔马小定理（注：因有 Fermat's Last Theorem 支持，中文称费尔马大定理）：$X^{P-1}=1$ 模 P，$X^{Q-1}=1$ 模 Q。

现证明 $X^{k(P-1)(Q-1)}=1$ 模 P，证明：$X^{k(P-1)(Q-1)}$（模 P）$=X^{(P-1)} \cdot X^{(P-1)} \cdot \cdots \cdot X^{(P-1)}$ 共 $k(Q-1)$ 个 X^{P-1} 连乘。

按乘法求模数满足交换律，即乘法完成后求模数等于先求模后再作乘法的运算

$$X^{k(P-1)(Q-1)}=[X=X(\text{模 } P)]^{k(Q-1)}$$

按照费尔马小定理，上式$=[(\text{模 } P)]^{k(Q-1)}=1(\text{模 } P)$

同理可得 $X^{k(P-1)(Q-1)}=1$ 模 Q。按照求模数运算概念，可得

$[X^{k(P-1)(Q-1)}-1]$ 被 P 整除，$[X^{k(P-1)(Q-1)}-1]$ 被 Q 整除，则 $[X^{k(P-1)(Q-1)}-1]$ 可被 $P \cdot Q$ 整除，故有：$X^{k(P-1)(Q-1)}=1$ 模 $(P \cdot Q=n)$

再求：$X^{ab}=?$（模 n）　　由于

$$ab=k(P-1)(Q-1)+1$$

$X^{ab}=?$（模 n）等于求 $X=[X^{k(P-1)(Q-1)} \cdot X]$（模 n）

再按照乘法求模等于先求模后作乘法的原理

得求 X^{ab}(模 n)=[$X^{k(P-1)(Q-1)}\cdot X$](模 n)=[$X^{k(P-1)(Q-1)}$](模 n) (X)[X](模)

=1·[X](模)

即解密算法恢复原文 X

② 如 X 与 P 相质,Q 与 X 可分解因子,则 $X^{(P-1)}=1$ 模 P 故

$X^{k(P-1)(Q-1)}=1$ 模 P, X 可被 Q 整除,则 $X^{k(P-1)(Q-1)}$,$X^{(P-1)}$ 也可被 Q 整除。

$X^{k(P-1)(Q-1)+1}=X$ 模 P, $X^{k(P-1)(Q-1)}-X$ 即可被 P 整除

$X^{k(P-1)(Q-1)+1}$ 可被 Q 整除(X 可被 Q 整除),则 $X^{k(P-1)(Q-1)}-X$ 可被 Q 整除

所以,$X^{k(P-1)(Q-1)}-X$ 也能被 $P\cdot Q$ 整除,即:$X^{k(P-1)(Q-1)}-X=0$ 模$(P\cdot Q)$

即:$X^{k(P-1)(Q-1)+1}=X$ 模$(P\cdot Q)$

因为:$a\cdot b=1$ 模$(P-1)(Q-1)$故 $ab=k(P-1)(Q-1)+1$,故 $X^{ab}=X$

③ 如 X 为 P 和 Q 的整倍数时

$X^{K(P-1)(Q-1)+1}=0$ 模 PQ,$X^{K(P-1)(Q-1)+1}-X=0$ 模$(P\cdot Q)$,则

$X^{K(P-1)(Q-1)+1}=X$ 模$(P\cdot Q)$,$X^{ab}=X$ 模$(P\cdot Q)$

2. 应用分析

原理性充要条件的建立,质数的选取以 n 越大越好,才可使因式分解困难,故 P 和 Q 两数需很大才行,但现在没有大质数产生公式,只可根据当数很大时质数间差近似等于 $\log P$,$\log P$ 数字增长比 P 数字增长慢得多,故可依次搜寻直到找到大质数为止。紧接着便是质数如何验证难题,有人会问为什么试除法不行?在绝对意义上讲是可用的,但在现实的时空条件中行不通,例如 $2^{512}+1$ 这样的大数,试除法确定质数,其所需时间大得惊人,利用费尔马小定理即 $X^P=X$ 模P 当 P 是质数时一定满足,P 不是质数只有小概率满足费尔马小定理,当 P 数大时概率更小。

运算方法分析:加密运算先算 X^a 后再求模等同于 X(模 n)·X(模 n)…X(模 n),a 个 X 相乘求模=模的乘积。故可先求模后求方以避免大数运算造成计算机溢出。解密计算[X^a模 n]^b,首先它等同于[X^a]^b 模 n 计算,在计算过程中,也按上述加密过程在 X^a 模 n 基础上作一定方次计算后接着就求模运算,而不必作完 b 次方后再求模,即使这样简化加密解密过程,RSA 码在使用过程中仍嫌太烦琐而不方便,直接对信息使用。

3. 密码应用安全分析

密码安全度的分析有多种测度,对 RSA 算法推荐以下一种安全测度,即在现实科技条件下破密所需时间为安全测度,如所需时间为不可实现的天文数字则称这种密码为绝对安全(如 10 光年以上),若时间远远大于一个密钥运行时间(密钥可以更换),则称密码是安全的。

至于破密码所需时间又取决于有无找到专门的破密算法,由计算数学上分析,如果计算步骤数 S 是确定性的,可由输入量 X 的多项式表达计算,即 $S=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$,则称此计算问题为 P 类问题。P 类问题认为是可以计算的,不能用此类问题构成密码。不确定性多项式即接续计算步骤是不确定的,即 nonidetenministic polynomial,相当于多个甚至无限个 P 问题的组合,称的为 NP 问题。NP 问题中如能找到一条 Hamilton 回路则一定可转化为 P

类问题，但求一个 NP 问题是否有 Hamiltion 回路就需要与输入量成指数级的计算步骤。因此，破解密码算法是一个 NP 问题，这是密码安全的必要条件，如果破密算法步骤与输入量呈指数增长，在输入量很大时计算步骤成天文数字，则该密码体制也可认为是安全的。第二个因素是计算机的计算速度，如计算速度大大提高（如设想的量子计算机能实现则计算模式由现在的图灵机变为全并联式计算），计算时间大大缩短，则一种安全密码会由安全的变为不安全的。因此某一种密码的安全是一个相对概念，利用以上内容具体分析 RSA 密码的安全性。

n，b 是公开的，a ，P，Q 是保密的。

知道 n 求解 P，Q 这是大数分解问题，它是一个 NP 问题。目前已知最好的算法是有人分析得出所需次数为 $e^{\sqrt{\ln n \cdot \ln(\ln n)}}$，当 n 很大时用现代化高速大型计算机，如每秒运行万亿次，$n=10^{200}$（即 200 位十进制数），则需 3.8×10^{3} 年，如改为 1 024 位则无论用何等先进的图灵计算机，其计算时间都是天文数字，计算次数达 2.8×10^{58}，计算时间达 10^{40} 年。

除了 P、Q、a 要保密外，$\Phi(n)=(P-1)(Q-1)$ 也要保密，原因为

$\Phi(n)=PQ-(P+Q)+1=n-(P+Q)+1$，所以 $P+Q=n+1-\Phi(n)$

$(P-Q)^2=P^2-2BP+Q^2=(P+Q)^2-4PQ$，所以

$$P-Q=\sqrt{(P+Q)^2-4n}=\sqrt{(n+1)^2-2\Phi(n)(n+1)+\Phi^2(n)-4n}$$

如 n 公开，$\Phi(n)$ 已知，则由 $P+Q$ 及 $P-Q$ 两式便可解出 P，Q，故 P，Q 与 $\Phi(n)$ 对解密钥 a 是等价的。得到 P，Q 便可由 $(P-1)(Q-1)$ 求出 $\Phi(n)$，再由 $a\cdot b=1$ 模 $\Phi(n)$ 便可解出私钥 a 来，因此 $\Phi(n)=(P-1)(Q-1)$ 也需保密。

4. DES 密码

DES(data encnpytion standard)作为世界范围内的标准已经 20 多年了，尽管它带有过去的时代特征，但它很好地抗住了多年的密码分析，对攻击仍是安全的。它不像 RSA 码算法那样简单，DES 密码算法较为复杂，首先应明确算法应具有的本质属性。

- 算法必须提供较高的安全性；
- 算法必须完全确定且易于理解；
- 算法的安全性必须依赖于密钥，而不依赖于算法；
- 算法必须对所有的用户都有效；
- 算法必须适用于各种应用；
- 算法必须能验证。

DES 是一个分组加密算法，算法对所有的应用是固定的，加密算法步骤固定，解密过程是加密过程的逆过程（分步骤内容不变，但次序相反），DES 是对称密钥码制，即加密解密用同一密码，因此保密通信工作前通信双方必须在安全信道中传输并确定所用密钥，不同于公开密钥制中，解密密钥不需传输，DES 体制中密钥的安全传输是重要问题。

（1）算法描述

DES 对 64 位的明文进行分组操作（每 64 位作一次算法运算），通过一个初始置换将明文分组为左半部和右半部（各 32 位长），然后进行 16 轮相同的运算，其运算用算子 F 代表，在运

算过程中数据与密钥进行异或运算，经过 16 轮运算后，左右两半数据合在一起进行一次初始变换的逆变换，就完成了算法，见图 5.10 和图 5.11 及表 5.1～表 5.2。

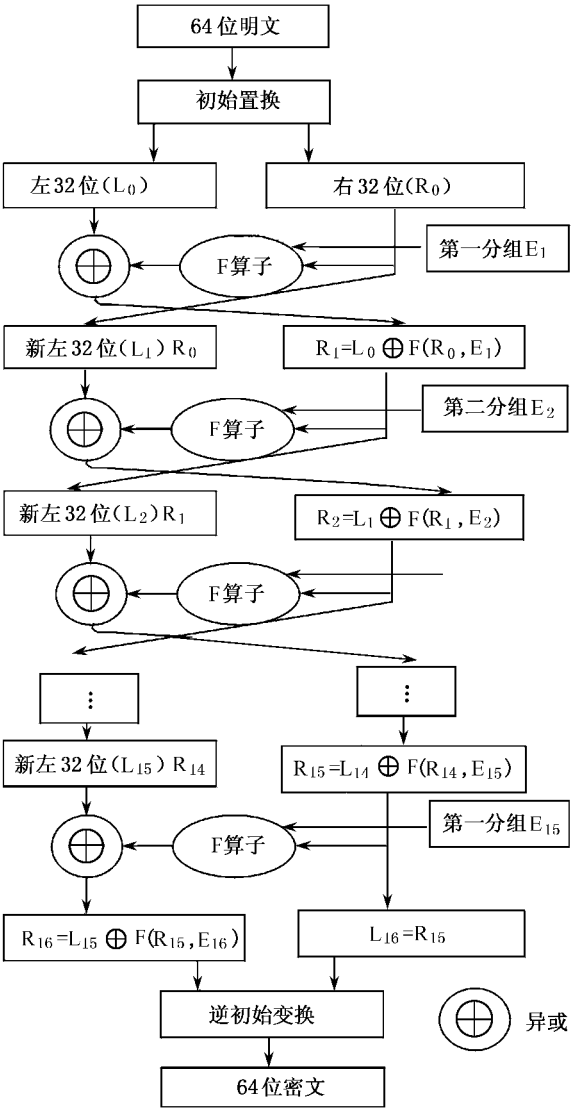


图 5.10　DES 加密过程流程图

（2）DES 解密

在经过所有代换、置换、异或和循环移位后，加密方法有很强的混乱效果，加密和解密算法二者唯一的不同之处是密钥次序相反，加密密钥分别依次为 $E_1, E_2, \cdots, E_8, \cdots, E_{16}$，**解密密钥使用次序正好相反为** $E_{16}, E_{15}, \cdots, E_2, E_1$，**密钥向右移动次序为** 0,1,2,2,2,2,2,2,1,2,2,2,2,2,2,1。

DES **密码的安全分析尚无数学证明，主要靠攻击试验。**

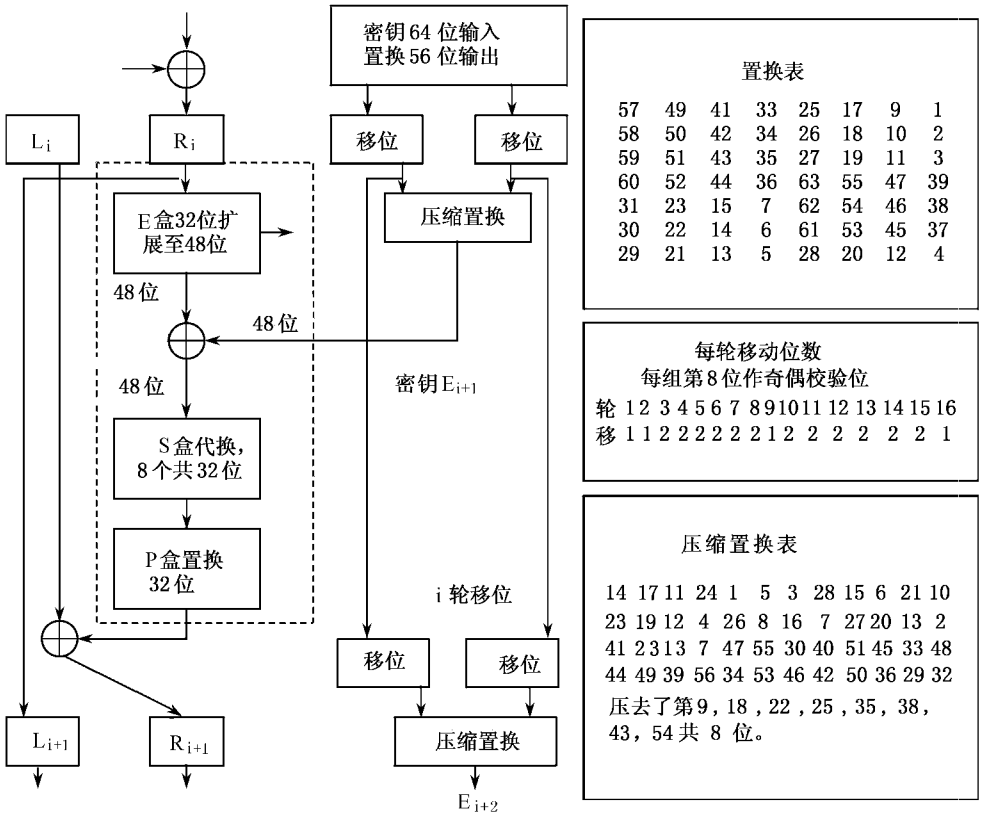


图 5.11　第 i 步加密过程详解

表 5.1　数据的初始置换

后组 \ 位	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
2	62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
3	57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
4	61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

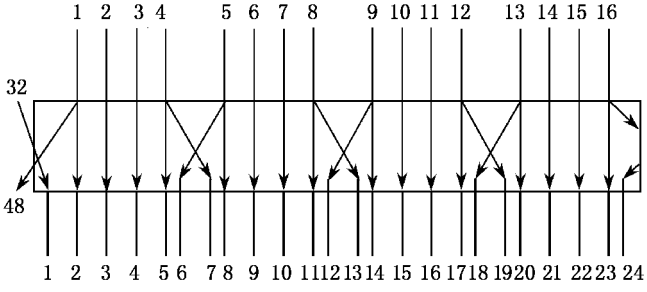
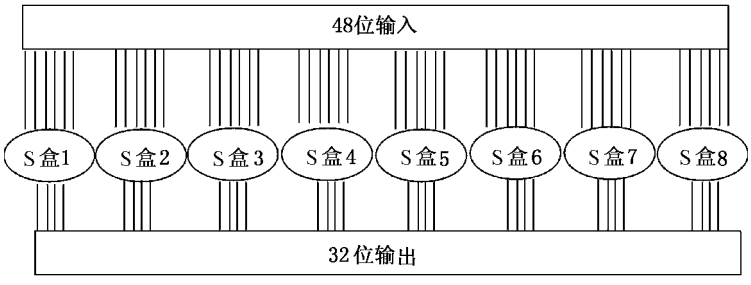


表 5.2　数据的扩展置换(从 32 位扩展至 48 位)

后组 \ 位	1	2	3	4	5	6	7	8	9	10	11	12
1	32	1	2	3	4	5	4	5	6	7	8	9
2	8	9	10	11	12	13	12	13	14	15	16	17
3	16	17	18	19	20	21	20	21	22	23	24	25
4	24	25	26	27	28	29	28	29	30	31	32	1



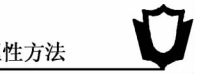


表 5.3　S 盒代换，共 8 个盒（为非线性代换）

后组 \ 位	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
S_1																
1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
2	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
3	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
4	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2																
1	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
2	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
3	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
4	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3																
1	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
2	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
3	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
4	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4																
1	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
2	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
3	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
4	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5																
1	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
2	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
3	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
4	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6																
1	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
2	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
3	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7																
1	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
2	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
3	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
4	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8																
1	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
2	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
3	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
4	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

二、信息附加义的隐藏

信息由于其宿主(运动)众多的关系(即关联特性),必然会有附加义,如语言作品有附加义一样,这也是信息不可绝对隐藏原理的延伸应用。信息附加义有很多正面作用,也有增加信息安全保密隐藏难度的负面效应,举例如下。

茅台酒集团最近开发了茅台啤酒,广告语"啤酒中的茅台",重要意义在后半部。啤酒中的茅台,可理解为众多啤酒的一种为茅台啤酒,附加义为如白酒中的茅台酒。既没有构成侵权(如说明自己胜过谁),又明确表示自己是顶级者。附加义起作用的因素一方面在于事物关联性,另一因素为人所共有的类比、联想思维能力。在形成信息作品时,防止附加义的泄露是一件很困难的事,没有系统性的有效方法,只有针对要隐藏的附加意义信息进行检查,如果发现有联想出附加义的可能,则修改其组成及表达形式,以切断由信息联系附加义的关系。

三、潜信息的信息隐藏

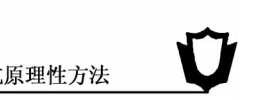
潜信息也称阀下信道,其基本原理是,如存在一种具有特殊性质的密码,即每一种明文可能存在两种密文,这两种密文均可使用同一密钥恢复成同一明文,同时假定这些密文可由发送者和接收者方便地分为两类,即 I 类和 II 类,再利用一种加密法(如 Vernam 加密法)来掩蔽阀下比特,就能建立一个安全地 1bit 阀下信道,在使用该信道前,发送方和接收方须共同确定一组密钥,最好为一次一密。

四、时空维中信息存在形式的隐藏

信息作为运动的一种表征与描述,在时间、空间维的信息特征必定是有限的,如空间、时间维占有位置、持续时间及它们的变化率等,它们的存在相对于时间、空间维全部内容都是一种特殊性。信息的空间、时间特征占位越小,发现这些特征的可能情况越多,在同等约束条件下越难发现,正如在海洋中搜索一条船,船越小越难发现,信息领域也同样。增加发现信息的维数,发现难度成正比例于维度数的方次。在二维角度空间加上时间维搜索某特殊信息的难度是单在时间维搜索难度的立方。为了隐藏信息往往在信息存在形式的表征维度上压缩其所占测度值,如通信中用突发式工作是在时间维上压缩信息存在时间,增加可能地址数,然后再选某特征地址,这是在地址空间增加隐藏性。信息两个维度中有相互倒数关系者,在一维中的测度值少比另一维相应增加,如信号宽度减少一半,则频谱宽度增加一倍,此时采用在某一维上压缩必须估计另一维扩张所带的相对后果。

五、数字水印的信息隐藏

数字水印是信息隐藏的一个重要学科分支,通过加入数字水印,可以有效保护数字信号的版权,进行文件的真伪鉴别以及进行隐含标注等。数字水印的基本原理是将某些标识性数据



(具有个性化,如随机序列、数字标识、文本以及图像等)嵌入到宿主数据中作为水印,使得水印在宿主数据中不可感知和足够安全。数字水印算法包含两个方面:水印嵌入和水印提取或检测。此外从鲁棒性和安全性考虑,对数字水印进行随机化和加密处理。数字水印可以嵌入到图像中,也可嵌入到音频和视频中,下面以图像数字水印为例进行分析。

图 5.12 为图像数字水印嵌入方法原理框图。

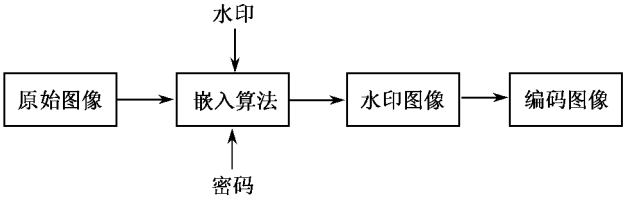


图 5.12　图像数字水印嵌入方法原理框图

设 I 为原始数字图像,W 为水印,K 为密码,那么处理后的水印 $\widetilde{W}$ 由函数 F 定义如下:

$$\widetilde{W} = F(I, W, K)$$

一般函数 F 是非可逆的、单向的、非对称的,为了提高水印的可靠性、安全性,还要对水印图像进行编码,设编码函数 E,原始图像 I 和水印 $\widetilde{W}$,那么嵌入水印后的图像 I_W 可表示如下:

$$I_W = E(I, \widetilde{W})$$

如图 5.13 所示为图像数字水印提取或检测原理框图。图像数字水印提取是数字水印方法中最重要的步骤,将水印提取过程定义为解码 D 过程,则输出的或是一个判定水印是否存在的 0～1 决策,或是包含各种信息的数据流(如文本、图像等),设已知原始图像 I 和有版权疑问的图像 $\hat{I}_W$,则有:

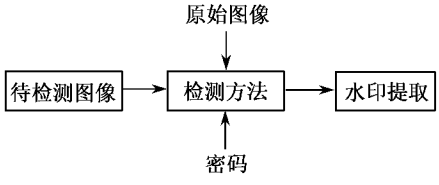


图 5.13　数字水印检测方法原理框图

$$W^* = D(\hat{I}_W, I) \quad \text{或} \quad C(W, W^*, K, \delta) = \begin{cases} 1, & W \text{ 存在} \\ 0, & W \text{ 不存在} \end{cases}$$

其中 W^* 为提取出的水印,K 为密码,函数 C 作相关检测,δ 为决策阈值,这种形式的检测函数是创建有效水印框架的一种最简便方法,如假设检验或水印相似性检验。

方法分析:从技术角度讲,数字水印方法可以通过有效的水印提取或检测达到宿主数据的保护。必须保证水印检测过程和算法的公开性,保证数字水印算法对数据变换(滤波、图像压缩、几何失真等)、攻击(噪声攻击、检测失效攻击、迷惑攻击、删除攻击等)的鲁棒性。从理论上分析,数字水印方法是保证水印的特殊性和个性的信息隐藏的一种方法,且其隐藏是相对的,是一种非对称性变换,其核心技术问题转移至水印的鲁棒性等方面。

5.5.2 个性信息及个性关系的利用与防攻击方法

上节论述信息安全对抗问题，可概括为围绕个性（个性信息）及个性关系的保持利用和破坏间的斗争。要保持和利用个性信息、个性关系，必然要反对和防止破坏，这两者（利用和破坏）是不相容的，应结合在一起对正、反面同时考虑，本节将在原理上讨论一些常用的方法。

一、个性信息的利用与攻击概述

1. 个性信息主要分类

· 主体物理、生理等个性信息变换及表征：主体物理个性是指主体物理特性中具有个性，当其用信息表征（或经变换后表征）同样具有个性（特殊性）时构成了个性信息与主体物理之间一一映射时，个体信息便能完全代表该物理及生理等个性。如利用人的虹膜、指纹、DNA 排列等。

· 在关系相互作用中形成主体个性信息表征：如比较中形成的排序、多因素“与”的结果、置换结果、竞争结果等信息表征。

· 某些运动中个性的信息表征：如个人签名、化名等。

2. 个性信息的防攻击主要类型

· 个性信息的冒名顶替：常发生在个性信息与原关联事物发生分离的前提下。

· 个性信息的非法窃取：常发生于非法窃取者用正常行为得不到的非常重要个性信息场合。

· 个性信息的伪造：为某种目的制造伪个性信息，为后续攻击和破坏奠定基础。

· 个性信息的破坏：破坏原个性信息所起作用。

· 个性信息的抵赖：也可能借存在冒名顶替、伪造的名义进行抵赖。

· 不可鉴定性：是破坏防抵赖、防伪造、保证可利用性造成混乱的重要属性。

3. 个性信息与防破坏的原理性方法

在攻击方常用较强的信号掩盖个性信息的方法进行攻击，这时可以根据掩盖信号与个性信息的特征差别，利用变换突出差别，从掩盖信号中识别出个性信号。攻击方也可以利用直接破坏个性信息的各种办法（反其道而行之），反攻击方则常采用各种反破坏方法（反反其道而行之）。选择变换应注意有效扩大两者的微弱差别。利用数字签名作为个性信息（可用公开密钥加密，用私有密钥解密等）的代表、利用密码将相关主体信息与数字签名紧密结合的防冒充顶替、利用时间标记及密码中心登记认定防止抵赖及不可鉴定性、利用公开密钥制（*RSA* 密码制）的安全性防止伪造或破坏、利用良好性能的算法（高分辨率、低错误率及快速性结合）与基准信息对比鉴定的方法形成物理特征个性信息的认证鉴定，如利用指纹、虹膜信息对伪装鉴定，并严格保护基准信息不被代替或冒充。

二、个性关系的利用与攻击概述

有个性信息嵌入的关系，包括关系集群，称为个性关系。它们在信息系统运行、应用中具有重要意义，因为它是组成信息作品和信息系统运行秩序的重要因素。如下是针对个性关系攻击的反攻击的一些方法。

实际上具体攻击包括个性信息攻击及个性关系攻击，反攻击实际上是将反个性信息攻击及反个性关系攻击整合在一起实施反攻击。本小节侧重反个性关系攻击，各种具体方法也在不断发展变化，在此只讨论几种常用原理性方法（技术方案性方法）。

在时间、空间维中以“反其道而行之”为核心形成一类技术方案性对抗方法。“反其道而行之”包括各种形式的反其道，目的为制服攻击（攻击也是“反其道而行之”），是攻击方与反攻击方互相反其道而行之。反其道而行之脱离不了关系，例如攻击方破坏个性关系的支持关系，反其道而行之可以反破坏支持关系，也可以重建支持关系，在时间上最好应在破坏效果产生前，体现了时间维中的重要性。又如攻击方是攻击运行控制权以实行破坏（如病毒攻击），反攻击方则应反击争夺控制权，这意味着包括了多种具体方法，其核心机理是反其道而行之。

防止攻击连续扩大。这看来似有被动色彩，但实际上是一种相反相成反其道而行之方法，往往很有效。大多数情况下，有的攻击开始效果对全局影响不太大，此时如切断攻击效果扩大，或分离攻击效果是很有意义的。具体可再分为两种，一种为防止攻击效果直接连锁扩大，另一种为防止攻击效果连续扩大对正常关系的影响。例如：计算机网络中某局域网被垃圾邮件包阻断，则首先应从整个网络中剥离该局域网络（包括其入口，然后再解除局域网的阻断），如不采取措施则整个网络的各种功能都可能受影响。

对重要关系（序），检测其重要状态是否存在异常，如异常则修正状态，也可重新设置正确状态。首先这方法难度在于重要的界定，其二，关系往往是多种、多层次交织状态与过程（静态与动态），通过静态状态推测动态性能的完备性是困难的，需要高度技巧。

对重要动态关系（即关系间动态整合和运动）进行隔离状态下的模拟进行检查。若运行有误则立即采取各种措施，如调用迂回路径，备用关系集群，改变算法等措施，其难度在于重要隔离的界定，检查所占资源是否承担得起（含时间资源）等。

在实际运行环境中实行监控，发现状态异常，立即进行溯源并进行病因消除。

实际情况中往往多种方法叠套交融地使用，将在后面的例子中说明。

三、信息作品的利用与攻击概述

信息作品是由多个个性关系、信息和信息媒介合成的整体，它能表征描述事物运动的状态、过程等，当信息作品中某些重要信息消失或重要关系发生一些变化，所描述状态或过程会发生非常重要的变化。例如数字小数点位移，单位变化，关系发生相反性质的变化，又如加减、出入、前进、后退、是、非、合成、分解等。

对信息作品的破坏类型有篡改、盗窃、冒充、重要内容泄漏等，信息运行秩序的破坏种类很多，可以概括为各种重要关系的破坏和其中特殊信息元及个性关系的破坏。

· 利用数字水印对信息作品加以个性保护。

· 利用散列函数对信息作品摘要进行变换“＋”数字签名，再利用密码对两者加密后传输，以检验在传输中对信息作品的篡改，一旦有篡改则信息作品与其摘要会发生差异，差异的产生在于利用散列函数变换的摘要是不可更动的。

· 利用信息隔离技术，保持信息在防泄露区内对外不泄露。防止攻击者在防泄露区中，利用自己的优势获得对方重要信息。按其实施特征隔离封闭技术可分为：(1) 在广义空间封闭区域内切断个性信息的交互关联关系。广义空间包括：三维地理空间、多维物理空间、多维逻辑空间。广义空间内联合采用多种子空间中的隔离措施，如在地理空间和物理空间同时采取隔离措施。(2) 物理隔离是指切断具有物理特征的一些交互关系，如传递电路隔离、电磁场隔离、声场隔离等；逻辑隔离是指切断逻辑关系等。常用信息有防止电磁辐射传输是地理空间与物理隔离同时采用的例子。物理隔离包括利用前沿技术使攻击方不具备攻击条件，是一种广义的物理隔离。(3) 时间隔离：在时间维上切断与信息交互关系称为时间隔离，时间维关系切断的最基本形式是，压缩信息的存在时间(包括快速变化)同时进行空间维的隐藏。信息时间维隔离具有相对性，其概念指对方获得信息的可能性降低，同时还依靠信息所表征运动的存在时间，时间维隔断是一个在不断发展变化的复杂问题。

5.5.3 信息系统及其服务群体作为一个整体按“特殊性”加以安全保护的方法

本节主要讨论信息系统及其服务群体作为一个整体来考虑其安全保护方法。从系统层面上讲，这个整体也具有其本身的特殊性，例如银行信息系统、税务信息系统、客票信息系统等。除有作为服务工具的信息系统外，服务群体也是系统的服务主体，与信息系统是不可分割的一部分，整个信息系统为分布式结构，可以通过专网、公网或其他方法在广阔的区域中分布构成。就服务功能而言离不开个性信息和个性关系、信息作品，也离不开信息系统。如何保护信息系统及其服务群体，要从整体上、系统层面进行综合考虑，全面构建安全保障体系。不仅涉及技术方面，还涉及管理方面，尤其是复杂服务性信息系统往往具有开放特征，更增加了管理保证、安全服务的困难，只有根据不同的重点服务项所可能引发的安全风险威胁程度，结合技术进行动态考虑才可以导引出具体有效方法。

一、信息系统及其服务群体的安全保护需求分析

从整体上讲，信息系统及其服务群体的安全保护，同样要满足其基本安全属性的要求，即保护机密性、保护完整性、保证可用性、保证真实性、实现可控性。

· 保护机密性：是指信息不被非授权解析，信息系统不被非授权使用的特性。这一特性

存在于物理安全、运行安全、数据安全层面上。保证数据即便被捕获也不会被解析，保证信息系统即便能够被访问也不能够越权访问与其身份不相符的信息，反映出信息及信息系统机密性的基本属性。

· 保护完整性：是指信息不被篡改的特性。这一特性存在于数据安全层面上。确保网络中所传播的信息不被篡改或任何被篡改了的信息都可以被发现，反映出信息完整性的基本属性。

· 保证可用性：是指信息与信息系统在任何情况下都能够在满足基本需求的前提下被使用的特性。这一特性存在于物理安全、运行安全层面上。确保基础信息系统的正常运行能力，包括保障信息的正常传递，保证信息系统正常提供服务等，反映出信息系统可用性的基本属性。

· 保证真实性：是指信息系统在交互运行中确保并确认信息的来源以及信息发布者的真实可信及不可否认的特性。这一特性存在于运行安全、数据安全层面上。保证交互双方身份的真实可信以及交互信息及其来源的真实可信，反映出在信息处理交互过程中信息与信息系统真实性的基本属性。

· 实现可控性：是指在信息系统中具备对信息流的监测与控制特性。这一特性存在于运行安全、内容安全层面上。互联网上针对特定信息和信息流的主动监测、过滤、限制、阻断等控制能力，反映出信息及信息系统可控性的基本属性。

二、信息系统及其服务群体作为整体特殊性的保护方法

1. 系统层面分析

如图 5.14 所示为某一信息系统及其服务群体融入更大系统中的体现。最外的圈表示更大的系统，特定信息系统及其服务群体在大系统或更大系统中，是一个具有“特殊性”的系统。

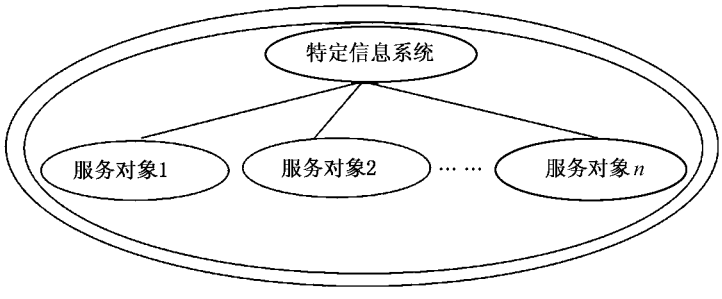


图 5.14　信息系统及其服务群体构成示意图

要保证信息与信息系统基本安全属性的要求，需要使信息系统具有如下基本能力：网络与信息系统对信息安全事件的防御能力、发现能力、应急能力和对抗能力等。防御能力：是指采

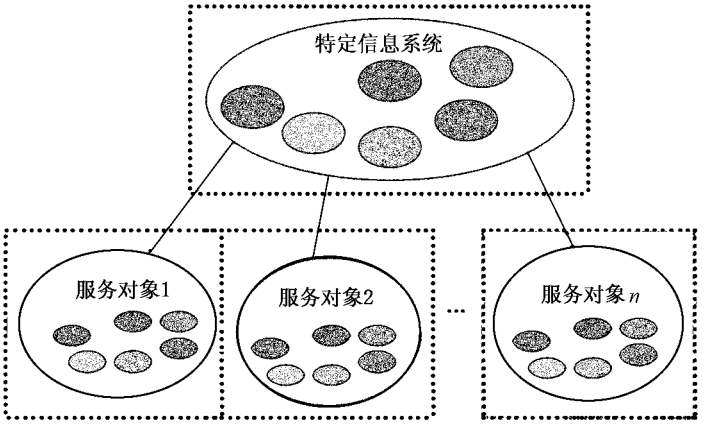
取手段与措施，使得信息系统具备防范、抵御各种先进的针对信息与信息系统攻击的能力。发现能力：是指采取手段与措施，使得信息系统具备检测、发现各种已知或未知的、潜在与事实上的针对信息与信息系统攻击的能力，这与系统制对抗信息权能力密切相关。应急能力：是指采取手段与措施，使得信息系统针对所出现的各种突发事件，具备及时响应、处置信息系统所遭受的攻击，恢复信息系统基本服务的能力。对抗能力：是指采取手段与措施，实施反其道而行之，反反其道而行的能力以对抗攻击信息系统，达到获取信息、控制信息系统、中止信息系统的服务、追踪攻击源头的能力。

系统具有上述基本能力，就要综合运用管理方法、科学技术和信息、有关资源三个基本要素，通过合理配置各项资源，建立管理与技术相互协调的信息安全保障体系。管理方面：实质上安全风险源于不同社会主体所涉及的社会位置和不同的利益属性，需要由不同的法律来规范和调整，也需要由不同的政府职能部门来监督和管理。如何组织实施好上述内容，管理成为解决信息安全问题的基本要素之一。技术方面：各种法律、行政和社会的管理手段在系统中需要由特定的技术措施来支撑，包括各种技术手段、工具及其应用过程。同时，网络与系统的技术环境的有关特性，以及有关技术操作及技术过程所导致的安全问题，需要由相应的技术功能和技术规则来控制，形成了技术是解决信息安全问题的基本要素之一。资源：管理与技术的有效实施，最终都依赖于各种必需的资源，包括人才、资金、基础设施、场所等。人既可以是管理规则的制定者与执行者，也可以是管理规定的遵循者与制约者；资金既是建设管理体系的必要条件，也是建设技术体系的必要条件；基础设施既可以是技术成果的结晶，又可以是服务于管理及技术的资源；那些可以服务于信息安全的成型的、固有的、客观存在的规则、设施、机构，以及人才、资金、教育等，都可以看做是可调配的服务于信息安全保障体系的资源。因而资源也是解决信息安全问题的基本要素之一。

综上，从信息系统及其服务群体整体考虑，其安全保护方法要从管理、技术和资源三个基本要素入手，实现整个系统的防御、发现、应急和对抗能力，从而保证系统正常运行之几个基本安全属性，即保护机密性、保护完整性、保证可用性、保证真实性、实现可控性等。

2. 技术方案

从整体上讲，其安全保护方法要从管理、技术和资源三个方面考虑，这里只讨论技术上的安全保护方法。根据技术上的不同特点，信息系统及其服务群体的安全保护方法可从同不角度加以综合考虑，如可从物理安全、运行安全、数据安全、内容安全四个层面考虑，也可从基础设施、网络边界、计算环境几个方面加以考虑。不同角度的考虑，其侧重点不同，无论从什么角度分析，均要建立一个系统的概念，将系统根据不同的安全需求划分成不同的域和层次，再根据具体的威胁和风险，制定针对性的安全保护措施，如图 5.15 所示。



5.15　信息系统及其服务群体作为一个整体制定的安全技术方案

图 5.15 中的不同颜色的小圈代表系统内不同安全等级要求的域，可根据具体的风险和威胁制定、实施安全方案；图中方型虚框代表主信息系统及其服务群体的外部边界。从图中显然可以得出，安全保护方法不仅涉及系统内部，更要注意外部的边界。如果一个系统与外界是断开的，则无需考虑这一点，随着网络发展，这种情况越来越少。如果将主信息系统与其服务群体作为整体按“特殊性”来考虑，要着重进行边界的保护，保护其内部的“特殊性”以及个性信息、信息关系等。

从技术角度来讲，安全保障体系的建设涉及多项技术，如为了保护计算环境，可采用访问控制、身份认证技术；为了保护边界，可以采用加密解密技术，采用虚拟专用网(VPN)技术；为了防止外部攻击，可以采用防火墙(FW)、入侵检测(IDS)、蜜罐技术等；为了防止病毒可以采用杀毒软件和操作系统加固技术等。此外，还涉及实体安全技术、安全审计、灾难恢复、自动入侵响应技术等。下面简单介绍防火墙、入侵检测和虚拟专用网技术。

防火墙是一种逻辑隔离的方法，通过对到达数据流进行特性和行为的“规则分析”，根据分析结果给出是否允许数据流通过的判断。要注意的是，防火墙的规则是人为设定的，不仅要保证规则配置的合理性，还要进行不断的动态调整和升级。防火墙的体系结构主要包括：包过滤、双宿网关、屏蔽主机、屏蔽子网、合并外部路由器和堡垒主机结构、合并内部路由器和堡垒主机结构、合并外部路由器和内部路由器的结构、两个堡垒主机和两个“非军事区”结构、牺牲主机结构、使用多台外部路由器的结构等。防火墙主要涉及的关键技术包括：包过滤技术、代理技术、电路级网关技术、状态检查技术、地址翻译技术、加密技术、虚拟网技术、安全审计技术、安全内核技术、身份认证技术、负载平衡技术、内容安全技术等。

入侵检测技术是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术，是一种用于检测计算机网络中违反安全策略行为的技术。它通

过对网络中关键结点的信息收集、分析，审计系统中的弱点，统计日常行为中的异常模式，评估系统中的数据、文件的完整性，检测是否有违反安全策略的事件发生或攻击迹象，并通知系统安全管理员。根据入侵检测的时序可分为实时入侵检测和事后入侵检测；根据入侵检测系统所使用的技术的角度可分为基于特征的检测和基于异常的检测；根据入侵检测的范围可分为基于网络的入侵检测系统和基于主机的入侵检测系统。

虚拟专用网(VPN)是通过一个公用网络(通常是互联网)建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。VPN 具有如下功能：加密数据，以保证通过公网传输的信息即使被他人截获也不会泄露；信息认证和身份认证，保证信息的完整性、合法性，并能鉴别用户的身份；提供访问控制，不同的用户有不同的访问权限。根据 VPN 所起的作用，可以将 VPN 分为三类：VPDN，在公司总部和它的分支机构的间建立虚拟专用网，称为“内部网虚拟专用网”；Intranet VPN，在公司总部和远地雇员或旅行之中的雇员之间建立虚拟专用网，称为“远程访问虚拟专用网”；Extranet VPN，在公司与商业伙伴、顾客、供应商、投资者之间建立虚拟专用网，称为“外联网虚拟专用网”。

5.6 信息安全与对抗原理性方法综合利用举例

5.6.1 综合举例一

Bell－Northern 实验室开发的 ISDN 系统实施安全电话。以下将就其安全电话工作原理加以介绍分析。

一、安全通话分析及符号表示

假设 Alice(A)主动呼叫，被叫用户 Bob(B)，Alice 用的电话为 T_A，Bob 用的电话为 T_B，密码管理中心为 K。通话过程可认为事物 A，B，T_A，T_B，K 的间互相联系以及联系的传递最终形成，保密情况下形成 A→T_A→T_B→B 及反向 B→T_B→T_A→A，表示 A，B 经过电话机形成 A，B 间的保密通话，5 个事物间双向联系有 5×5＝25 种单向排列，有 5 种为自己连接自己(自己的规定)，在其余 20 种排列中应选择相关单向联系从而构成安全通话(安全通话采用密码加密方式)即形成：

$$A \rightleftharpoons T_A \rightleftharpoons T_B \rightleftharpoons B$$

A→K(SM)表示 A 主动向 K 联系(SM)事件。

A→B(SM)表示 A 主动向 B 联系(SM)事件。

规定：公开密钥用 E 代表下标为所有者，如 E_A 为 A 的公开密钥；

私钥用 D 代表，下标为所有者，D_A 为 A 的私钥。

事物间用 Diffic Hellman 密钥协议进行联系，以下先介绍该协议及其特征。

双方通话前必须互相验证身份以及授权资格，这些的依据是经认证中心 K 的认证，“验证”要在安全保密的情况下进行，而且总要有一个开始，如何保证安全的“开始”建立以后双方共用密码是非常重要的，这个“开始”可以用 Diffie－Hellman 密钥交换协议完成，按此协议可在不安全信道上相互通信，形成共用密码的密钥，且密钥是基于大素数分解原理形成的故保证是安全的。

Diffie－Hellman 算法：Alice 和 Bob 为当事人，他们协商一个大素数 n 和 g，这两个数可不保密，形成共同密钥过程如下：

① Alice 选取一个大的随机整数 X 并且计算 $X=g^x$，将 X 发送给 Bob。

② Bob 同样选取一个在的随机整数 y 并且计算 $Y=g^y$，将 Y 发送给 Alice。

③ Alice 计算出 $Y^x=k$，即 g^{xy} 作为双方共用密钥。

④ Bob 计算出 $X^y=g^{xy}=k$ 作为双方共用密钥。

共用密钥的最后完成是双方自己计算，不需要传送完成，故可在不安全通道进行建立密钥过程。

利用以上算法，用户可以和密钥管理中心建立密钥用于密码通信，如作为 DES 密码的密钥等。

二、准备工作

通话双方的电话机内共存有以下 4 种公钥、私钥密码对，作为互相识别之用。

① 电话机中嵌入一个自己的密码对，私钥存在电话中不可改变部分，公开密钥则用于对电话的识别。

② 电话中存有电话所有者的密钥对，用公钥来鉴定“所有者”有“所有者”的命令（可以通过所有者签发的指令而改变），使电话所有权可以转移。

③ 电话中存有鉴别来自网络密钥管理设备的指令的密码对，但这密码对可被电话所有者在更变使用网络公司情况下而改变。

④ 短期公钥、私钥对，它包装在一个由网络密钥管理中心签发的证书的中，用做两电话准备通话时验证证书之用，即利用网络的公开密钥来鉴定。

建立个人到个人的保密通信，还需采用另外的措施和步骤；利用称为点火密钥的硬件卡，该卡由所有者将其插入电话中，卡中包括所有者的私人密钥（是用所有者自己才知道的口令加密），以及网络管理中心所签发的证书（其中包括所有者的公钥和某些识别信息如姓名、安全许可、职称、个人爱好（再作一次鉴别之用等）。所有者然后再键入口令密码打开点火卡，打开点火卡后，所有者的私钥暂时留在电话中留做后续通话时解密的用，而公开密钥则将传至对方用作加密的用，其他信息也可为对方鉴别的用，所有这些信息都是暂存的，当所有者拔出点火卡后，所有存入电话的信息将很快自动删除，点火卡还起 A 到电话、B 到电话、电话到电话所有

者互认作用(包括互认所需密码如电话公钥,所有者与电话互认的所有者私钥等)。

三、呼叫过程

① A→T_A(SM),SM 为插入点火卡及键入口令。

② T_A(SM) ⇔ 点火卡(SM),SM 为双方互认及点火卡内容输入电话。

③ T_A→A(SM),SM 为互认,互认无误后,电话送拨号音给 A。

④ A→T_A(SM),SM 为 A 输入欲呼叫电话号码,T_A 呼叫对方电话 T_B。

⑤ T_A(SM) ⇔ T_B(SM),电话间按 Diffic - Hellman 协议建立电话间一次通信密码。

⑥ T_A→T_B(SM),SM 为 T_A 将 A 点火卡内容有关部分内容传送至电话 B。

⑦ T_B 用网络公开密钥验证有关内容。

⑧ T_B→T_A(SM),SM 为 T_B 初始询问文件,要求 T_A 对发出的一切内容发出时间进行回答并进行签名,签名要用 T_A 及 A 的私钥两者同时签名才有效。

⑨ T_A→T_B(SM),T_A 按(8)询问要进行回答,回答无误后接 T_B。

⑩ T_A→T_B(SM),SM 为 T_B 振铃。

⑪ 如果 Bob 接电话则将自己的点火卡插入 T_B,以后将重复(1)～(9)的动作,不过此时过程中所有的 T_A 换成了 T_B,A 换成 B,即 A,T_A 到 B 及 T_B 进行验证。

⑫ 如验证无误,则双方各自利用个人密钥和电话机 T_A、T_B 进行保密通话,通话中一方中断通话,则所建立的一切联系中断并自动删除所有暂存内容,状态自动归零以保安全。

由此例中可见协议算法以及协议中确保 A、B、T_B、T_A 的"个性"无误地传递利用,以及建立"个性"间的个性关系(保密通话),密码的应用是利用 RSA 签名辨认 Diffic - Hellman 形成 DES 密码的密钥并进行交换 DES 密码来加密通话。显然为了通话保密安全,需要付出一定代价(无论广义空间和时间维上都有所体现)。

5.6.2 综合举例二

例如发生在互联网上 A 和 B 双方的一次保密通信过程,图 5.16 所示为保密通信过程示意图。

假设 A 方要将秘密信息发送给 B,且只能由 B 收到;同时 B 方要求验证是否为 A 方发送的数据,如果 B 方收到了由 A 方发送的数据则 B 方发送收到数据的返回信息。具体实现过程描述如下:

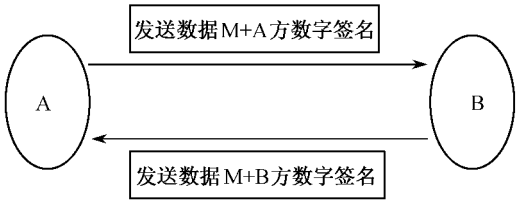


图 5.16 一次保密通信过程示意图

首先 A 方将待发送的秘密数据 M 加上数

字签名 SA 后利用 B 方的公钥加密得到数据 C，而后通过互联网将数据 C 发送给 B，同时将 SA 或 C 留底。B 接到数据 C 后，利用自己的私钥解密，如果得到正确的 M 则说明 SA 为 A 方签名，否则 SA 不是 A 方签名，B 将 SA 或 C 留底，同时将收到数据 M 的信息加上自己的签名发送给 A。A 收到数据后采用同样的方式验证 B 方的数字签名是否正确。

下面对互联网一次保密通信过程分析：

· 通信中为了实现对秘密信息的保护运用了信息内容的隐藏技术，即数据加密、解密技术，其中加密方法可根据不同的测度要求，采用单密钥体制也可用双密钥体制。

· 通信中为了证实数据发送者和接收者的真实性采用了数字签名技术。如果发送的数据需要保护版权，还可以采用数据水印技术，先在数据中加入水印信息，再签名传输。

· 通信中无论是数据加密、数据签名还是数据水印技术，都利用了个 A 方和 B 方所特有信息（特殊性、个性信息），即私有密钥、私有签名和私有版权特征水印标识。如果任何一方或者第三方获得这些信息，都可以对数据、签名或水印实现获得、攻击或破坏。

· 数据的传输还可以采用阀下信道技术，利用潜信息隐藏的方法。

· 通过数字签名、版权水印、加密技术以及其他一些技术，还可以实现发送方和接收方的防否认、防伪造、仿冒充、防篡改和防抵赖等安全问题。

5.6.3　综合举例三

我国《计算机信息系统国际联网保密管理规定》中第六条规定“涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其他公共信息网络相联结，必须实行物理隔离”。对于信息空间链接的直接阻断可以有效地解决信息及信息系统的安全，物理隔离技术是目前一种重要的信息安全与对抗措施（注：目前“物理隔离”的概念还存在一定的分歧，本文暂采用此称谓，目的旨在说明其是一种重要的安全防御方法）。

一般的安全措施（如防火墙、入侵检测、杀毒软件等）都是基于判定逻辑的安全技术，即采用形式化描述方法描述解决安全问题，把是否有安全问题的判定变成一种规则的搜索、匹配和判定过程，不可否认这是描述安全问题的一种有效方法，也是一种比较标准的方法，如：病毒有病毒库描述病毒特征，扫描病毒就是对病毒库的匹配过程；防火墙有过滤规则，阻断非法链接的根据就是看是否违背这个规则；加密技术其实也不例外，加解密过程就是按照一个规则进行变换的过程。显然这些安全措施存在两个问题，一是人们对客观世界进行逻辑描述的不完备性，一是逻辑描述对新问题的滞后性。所谓不完备性就是人们无法证明自己在一个问题上的逻辑模型是否正确，比如：无法证明一个操作系统是不是足够安全，是不是没有漏洞，无法证明一个规则库是不是完全正确，是不是无矛盾等。所谓滞后性就是规则的描述总是针对现有的问题，而新问题总是在不断的出现，比如：层出不穷的各种新型网络攻击，各种新出现的病毒等，规则的修改总是在问题出现以后。正是这种不完备性和滞后性在用户心里隐隐的形成了

一种不安全的感觉。

上述问题的有效解决方法可以采用信息空间的阻断即物理隔离方法。物理隔离就是将待保护的信息系统与其他系统从物理上隔离开来，具体地在信息网络上一是将其物理链接隔离，一是将信息从物理空间上进行隔离。但如果这种隔离是绝对封闭的系统是没有意义的，故这种安全措施既有隔离又有链接。具体体现在计算机网络上一是实现网线的物理隔离，一是实现存储介质上信息的物理隔离。图5.17为物理隔离方法的原理图。

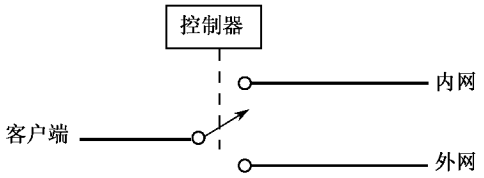


图 5.17　物理隔离基本原理图

如图所示，物理隔离器就是让两个网络物理上互相不连接。既然没有连接，那么各种已有的和可能新出现的网络攻击自然就不存在了。于是有人会有疑问，都不连接了，还能叫网络？如果换个角度说，是在两个网络中各有一台机器互相不连接，各上各的网络，那么就好理解了。隔离技术只是把这种原理实现得更加简单、好用而已。隔离技术彻底避开了采用判定逻辑方法存在的问题，从硬件层面来解决网络的安全问题，因此是解决网络安全问题的全新思路，而且更加简洁，更加安全。

此外物理隔离方法还需要处理内网和外网的信息交流问题，目前一般采用信息交流服务器来解决，图 5.18 为信息交流服务器原理图。A 网和 B 网是通过信息交流系统来传递信息，交流系统与 A 网链接时与 B 网完全断开，交流服务器与 B 网链接时与 A 网完全断开。

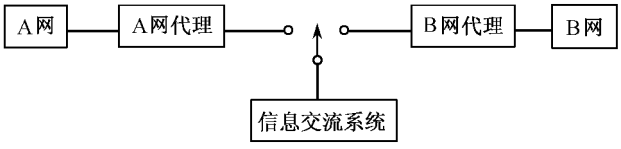


图 5.18　物理隔离信息交流系统原理图

对物理隔离方法的进一步分析：

从技术上讲物理隔离方法解决了信息网络物理层面（通信链路）上和信息层面（信息存储介质）的空间阻断。这种基于物理链路层的通断控制方法，断绝了内网与外网的网络物理直接链接，使得一切攻击行为在物理隔离面前遇到一条鸿沟，无法通过其链接和进入系统，这样的网络安全较之软件方式保证得更安全；较之防范性、检测性的安全策略更可靠，更值得信赖。这样的方式以不变应万变，从物理层空间上把攻击阻挡在外面，具有较高的安全性，较大限度地保证了内部信息网络的安全性。

从理论上讲，物理隔离方法实现了信息空间和时间的阻断，在信息安全与对抗核心链中达到了本身所具有的特殊性（个性），反其道而行之创造了与攻击行为的非对称性（与外网链接中

无法与内网建立信息连接），间接实现了自我信息的隐藏。

5.6.4　综合举例四

例如一个内部重要信息服务系统，可由一台服务器组成，也可由多台组成服务器组。若要求该信息服务系统保存内部的各种重要信息，同时为内部不同人员服务，但对外部不提供任何服务。显然，从重要信息存储、保护的角度来讲，该系统要求具有极高级别的安全性能，要制定如下安全策略，采取综合的、全方位的防护措施。

首先保证系统实体的安全，可采用固定机房，湿度、湿度控制，防雷、防水、防盗等措施。

因对外部不提供服务，该信息服务系统对外部来讲，无论是逻辑上还是物理上应是隔离的，拨号上网时也不能与该信息服务系统发生联系。与外部的完全隔离有效地防止了绝大多数的外部攻击行为（包括对信息和信息系统的攻击）。

因要对内部人员提供不同级别的服务，要求对信息加以访问控制和身份验证，不同级别的人具有不同的访问权限控制。对于身份认证，主要是利用其个性信息或个性关系，可以采用指纹识别、掌纹识别、瞳孔识别、说话人识别、人脸识别等基于生物特征的技术，也可基于密码、身份认证卡等非生物特征技术。

因是重要的信息，即使是在系统内部传输，也要尽可地采用保密通信方式（信息隐藏），如加密或者建立阀下信道，或者建立安全 VPN 通道等。

此外，对各级人员所使用的各种密码要严格管理，并保证其特殊性和个性，不能多人共用一个密码；同时，为了防止信息在传输时的窃听和破坏，除了对信息要进行有效的加密外，重要终端或通信线路要采取屏蔽措施，防止电磁泄露和电磁干扰等措施。

总的，要从技术、组织、管理等多个层次、多个剖面，综合利用多种措施，将信息系统及其服务群体作为一个整体来考虑，综合运筹，才能较为有效地保证重要信息、重要信息系统的安全。

5.7　本章小结

本章主要讨论了信息安全与对抗的原理性方法，主要包括：信息系统性能指标及其占位分析；系统层次的多种对抗原理方法；密码隐藏信息内容、潜信息、信息存在形式、数字水印等方法组成的信息隐藏一类方法；个性信息的关系保持、利用和攻击。最后给出一些原理方法应用的具体实例。本章所叙述内容间有密切关联性，对的应予以理解，在应用中应注意交叉融合、综合利用。

习　题

1. 信息系统的一般性能指标构成要素是什么？

2. 信息安全与对抗性能在信息系统性能指标中的占位如何？

3. 系统层次的信息安全与对抗指导性方法主要有哪些？

4. 信息隐藏的基本原理、特点是什么？

5. 什么是数字水印？其目的和特点是什么？

6. 什么是潜信息隐藏？有什么特点？

7. 试述在信息安全与对抗中如何利用个性信息和个性关系？如何利用个性信息和关系进行攻击？

8. 试举例说明信息安全与对抗过程中个性信息和个性关系保持的重要性。

9. 讨论、分析对信息作品的攻击与防御方法和技术。

10. 讨论、分析“物理隔离技术”的优缺点。

第 6 章　信息安全与对抗应用举例

6.1　引　言

本章主要以典型信息系统为例，说明信息安全与对抗基本定理、方法和技术的应用，典型信息系统如通信信息系统、雷达信息系统和计算机网络信息系统等。

6.2　高安全性能通信系统的安全与对抗问题

在此类系统中将安全性能置于优先考虑地位，采取多种措施，对系统进行多层次、多剖面无漏洞地安全考虑。

6.2.1　安全特点说明

这类安全级别很高的通信系统，在运行使用中不允许发生安全事故，本身也具有这种能力，没有必要在本系统层次设立安全入侵检测，这与高安全性能在逻辑上相悖。更高系统层次特殊的安全评估和安全对抗的研究都是不能间断的，安全对抗的矛盾不会停止。在哪个更高层次以及安全对抗模型、具体技术方向等有关问题上，应根据使用环境的状态及发展动向具体确定。这类高安全要求的信息系统安全问题的科技发展研究，不局限于自然科学与数学领域，还应包括社会、人文科学领域。

6.2.2　抗攻击安全考虑的主要内容

① 通信过程中的信息泄露问题。

② 通信系统正常运行秩序保护的问题，主要有：入网用户身份确认问题，密码管理问题，密码中心管理问题，专用系统管理运行维护等。

③ 通信系统本身层次抗攻击安全问题：特殊安全评估，多层次安全防范工作，防止系统被破坏（硬件破坏、软件破坏）等。尽量达到“绝对安全”，不发生安全事故状态。

6.2.3 对抗攻击安全措施考虑

通信过程防信息泄露的主要措施有：① 采用有线传输方式，防止电磁泄露而造成信息泄露，用高安全性密码体制对信息内容采用密码加以隐藏，并不断更换密钥来保证其安全性。② 形成独立信息系统，其中最严格者采用完全独立隔离结构，即传输媒介、交换机构、用户管理及密码管理中心等核心部分都单独设立，与其他通信系统无交织关系。③ 对进入高安全要求通信系统的用户进行严格认证手续，将用户数目尽量控制在最小可能数字。

安全指标估计：这类通信系统的高安全性要求不允许有任何安全问题发生，其系统安全结构模式采用自主预置型，即以出现安全问题概率非常小（难以估计和统计的小概率事件），构成多重叠套安全措施，使攻击方在一般情况下需要串联突破多个安全攻击才能达到攻击目的。例如，单独地铺设通信线缆，它并不与普通电信线缆置于同一线缆沟中，而是单独埋于地下，可以具有极低地泄露概率。通信中信息用密码隐藏信息内容，密码快速更换最高要求（达到一次一密钥），单独设置隐蔽的自动交换系统并严格地按规范使用，具有完备使用记录。一般情况下安全测度可用发生信息泄露概率$=1-P_0\times P_1\times P_2\times\cdots\times P_n$，其中$P_0,P_1,\cdots,P_n$，表示$n$重安全措施中每种出现安全问题的概率。$n$重措施同时失败发生安全问题的概率会很小，但存在极少的特殊情况，应加以注意，即出现了出乎模型设置的概率分布状态，如密钥管理中心发生问题，失落密钥形成非正常大的失密概率，以及对秘密的埋地通信线缆被对方以特殊技术检测出电磁传输信号（20世纪80年代在柏林的军用有线通信系统被对方在电缆附近设置了高灵敏度信号侦察设备，纪录下军用通信信息，这便是一个攻击信息安全获得成功的例子）。

6.2.4 高安全要求的移动式无缝隙广域通信系统

这类通信系统是一类重要通信系统，其中一些子系统本身就具有复杂结构。例如一个军在野战时的通信系统由成百上千个单元构成，具有层次间及多单元间互相通信的系统结构，同时还应具有高性能的抗攻击安全性及可靠性。军级、师级等野战通信系统是一种重要的复杂通信系统，功能复杂，需要对很多科技问题进行不断研究发展才能动态满足要求，在此仅就其安全对抗性能剖面进行讨论。

一、就野战移动剖面相关问题的讨论

就野战移动特点总体而方言，必定使用无线通信模式。

就电磁频率结合通信、安全等剖面选择考虑，现在有短波、超高频、微波、毫米波可选择，无线光波通信也逐渐进入应用。

短波：借助电离层反射可达远距离通信（但有近距离盲区），信号不能进行高速大容量通

信，且有来自空间辐射及工业的较强干扰。在安全性能而言，天线方向性差，通信速率低，难以利用信息。在时空维中利用很小占位而进行隐藏和隔离，可使用密码。

超短波以上频率：辐射穿透电离层，远距离通信。利用接力方式，可进行大容量高速通信，工业干扰较弱等。在安全性能方面，天线可有方向性，利用压缩技术使信号时空维中有较小占位，从而具有一定时空隔离及隐蔽性能，可与密码技术结合使用。光波在大气层内损耗较大，尤其是恶劣气象条件下更为突出。

综合比较性能后，现在野战通信系统多选择超高频微波、毫米波段作为主要无线通信频率，短波通信只作为辅助手段。

二、远距离无线通信及其安全问题考虑

如果选定 UHF 以上频率进行无线通信，则其远距离无线通信的安全问题分析如下。

① 利用中转接力设备进行通信接力加以远距离通信。接力通信在地面固定通信中可解决远距离问题，但在距离 50 km 处应设置接力点。若中间有山，则接力站地点选择应满足电波传播的通常条件，在移动状态下要在全通信覆盖区设置接力点，商用移动通信系统中称为基站，在野战条件下很难在战区内快速设置多个接力站。实际上移动通信系统如无固定有线电信骨干网支持，就不能完成廉价大容量多用户移动通信业务。

② 利用卫星作通信接力。利用卫星作通信接力具有覆盖区域广，随着卫星技术的发展提高，通信卫星已成为高性能接力设备，可支持多种高性能通信卫星有：(1) 同步轨道卫星，空间位置固定不变，距离达 36 000 km，延时达 ms 量级，时延嫌长，另一方面同步卫星波束对地面的覆盖地域较大，一颗同步卫星便能覆盖我国国土地域。(2) 非同步轨道卫星，其优、缺点与同步卫星的优、缺点正好相对立，如果非同步卫星保证全时域通信则在空间应由多颗卫星组成星座，并事前编制星历供给合法用户使用。利用非同步轨道卫星进行通信，应建立更复杂一些的通信网络管理控制系统。

下面利用低轨道卫星星座组成野战移动通信信息系统的安全对抗要点，分析多维安全措施及简要过程，如表 6.1 所示。

表 6.1　隐藏内容及方式

信息内容隐藏	利用密码进行信息内容隐藏，密钥可控制和变更
信息存在形式（信息媒介特性）随机变动	信号频率随机临时变化，对攻击者是一种隐藏 信号发射时间随机发生 信源信宿地址及标识经加密处理，建立过程保密
信道存在形式	空间安全卫星星历建立经卫星转发通信链路有一定保密性，需要临时建立通信信道，用毕即撤销有一定随机性

其核心是由网管中心所属的密钥管理中心制定的安全工作协议，以及密钥的变更和使用

管理。如图 6.1 所示。

主叫单位应根据安全通信规范和协议工作，经常备管理信道向网络管理中心申请与被叫单位建立互联信道的建立，网管中心审查认定资格后，通知被叫单位并审查被叫单位资格，通知双方有关信道参数、编号、密钥等（也可由双方协商建立密钥如 deffie－hellman算法）。双方互相确认身份后建立通信联系，通信完毕后通知网管中心撤销信道及密钥。

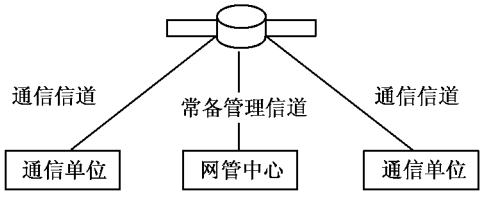


图 6.1　卫星通信及管理部分示意图

6.3　广播电视系统的安全对抗问题

6.3.1　地基广播电视系统

无线广播及电视网是一个重要信息系统，具有多种功能于一体，如传播、弘扬优秀文化、时事宣传、生活娱乐、商务活动的信息交流等，是现代化社会生存发展不可缺少的组成部分，其安全问题自然重要，但发射台功率都比较大。广播频段及超高频段都是组成传播直径几十千米的地区性分布网络，且有法律保护，个人及一般群体都无法严重阻挠无线电广播及电视网的正常工作，在发生战争情况，重要广播电台和电视台往往是敌对方攻击的重要目标之一，中断广播和电视台的战时工作，常起重要的心理攻击作用并造成社会混乱。

有线广播电视网络在城市中所需发射功率远比无线辐射小，网络中可加接力放大器，且不受城市工业电气噪声干扰、大型建筑物对电波传播的遮蔽及多路径效应影响。因此，信号质量可能达到良好水平，此外线缆多隐蔽埋入地下，可调整形成分布式独立子网，战争时有较高生存能力。总体而言，线缆一次性投入成本较大，尚需加入一定运营成本，对分散式独户住宅如果要求宽带接入则成本更高，在集中式多、高层公寓式住宅则成本较低，有线广播电视网络已经是大、中型城市设施之一。

6.3.2　卫星式广播电视系统

利用卫星作为转发器，向广大地区转发广播电视信号，接收后编辑进入本地台网，具有信号质量好且稳定的优点，同时可节省多站传播管理费，是国际文化传播交流及国内交流所不可缺少的信息系统。一般情况下按国际惯例，这些民用为文化交流、社会进步的信息系统是不得侵犯的，但也有罕见的冒天下之大不韪而干扰卫星电视系统的事件，我国鑫诺卫星转播电视节目曾数次被严重干扰而无法正常播出便是一例，说明信息安全对抗攻击措施具有非常重要的

意义，图 6.2 和图 6.3 分析干扰攻击及抗攻击的对抗措施。

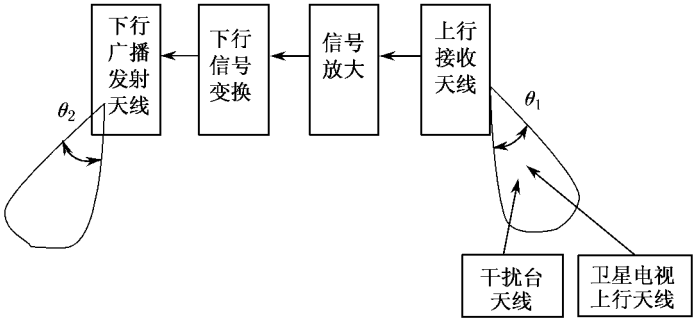


图 6.2　卫星广播系统信号传输示意图

由卫星发射广播天线的波束宽度一般主要决定于覆盖地区所决定，配合以足够的转发功率，使得地面使用不太大的天线便能有良好的清晰度，而卫星天线则受卫星体积重量成本等限制，一般波束宽度在 C 波段波束宽度为 1°～5°，直径为 1～6 m，而在距地面 36 000 km 的同步轨道上，对应地面覆盖直径内达 480 km（如波束宽度为 5°，则达 2 400 km），在覆盖范围内除了接收信号外，也可向卫星发送干扰信号，而鑫诺卫星设计不具备监测分辨干扰信号能力，对干扰信号同样接收放大变频向地面转播形成干扰效果。

在这种情况下，对抗干扰的一种有效方法，是在上行信道中加密码信号，由卫星接收部分进行解密密码识别，如密码结合利用扩谱技术则同时能提高信号干扰的比值利于滤去干扰信号，由于防密码破译，密钥需不时更换，因此，需增加上行密钥控制信道，此信道也应加密，而密钥信息可再加密一次，也可利用密钥代号不暴露具体密钥等，以达更安全状态，其框图如 6.3 所示。

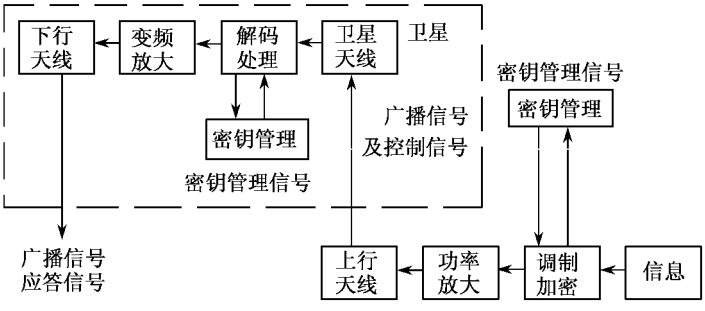


图 6.3　保证安全的卫星通信框架

至于加密方法有多种，上述的对信息加密（可用分组数据加密，也可用序列密码方式加密，

但不应有影响于视觉效果为前提，也可在同步信号中加密，卫星上解密得出同步信号后才进行信号转播），这样便可抑制干扰信号进入卫星接收系统、破坏干扰转播，此外加大地面发射信号功能强度，形成较大信号干扰。功率比也是一种最普通的抗干扰办法，在抗干扰方面还可联合运用加密及加大功能办法，现在利用“共道—逆道”模型扼要分析一下卫星广播电视中攻击和抗攻击情况。

6.3.3 有关鑫诺卫星对抗分析的举例——利用“共道”、“逆道”概念

共道之处：干扰信号利用卫星在接收波束内所有信号能接收而不分辨这一特点，将干扰信息送到卫星转发器上，即利用卫星对接收信号一视同仁加以转发的“共道”规律进行干扰信息的转播干扰。

逆道之处：按法律规定和国际惯例不允许干扰卫星广播，现在地面上对准卫星转发器天线上送干扰信号，经卫星接收及转发在输出端出现干扰信号。这个对抗过程中“对抗信息”兼寓于共道和逆道环节中，在干扰准备阶段都没有获得，直至出现了干扰效果，由干扰效果才获得逆道对抗信息，这当然是处于被动状态，所以对抗的第一阶段攻击方得手。由这个过程看，“共道—逆道”是交织在一起的，上送干扰信号到卫星转发器，在法律层次是逆道行为，在卫星工作技术原理层次是“共道”行为，形成“共道”原理，“逆道”效果，这是一种辩证的“相反相成”现象，这说明现行鑫诺卫星的电视广播系统中本征存有安全漏洞，多次被攻击方利用了。这种漏洞是卫星工作原理上没法鉴别攻击信号所致。干扰正常卫星广播不能允许得逞，在后续对抗行动中反反其道而制胜。进行思路仍是由对抗信息着手，即第一步找出干扰源所在地点，然后由行政、政治、公众舆论等方面进行反击，这是高层次措施，在直接技术层次采用了加大上行信号功率。以压制干扰信号的办法，这种应急对抗方法取得抗干扰攻击的效果，压制了干扰。当然在技术层次的先进方法应在卫星接收端鉴别出干扰信号加以阻断，这就是上行信号加密码（含同步信号）标志上行信号个性，而卫星识别信号排除干扰，即前面图 6.3 所提抗干扰方案。

6.4 雷达系统的安全与对抗问题

6.4.1 雷达对抗基本特点分析

由于雷达功能的重要性和工作的不可缺少性，以及雷达工作原理是利用发射信号对物体反射信号来探测物体的，因此一旦工作对方就必然获得信息，也就是雷达自己的工作方式暴露，给对方提供了基本对抗信息造成雷达工作的安全对抗问题十分严峻，从而使雷达对抗技术措施显得格外重要，需在严格保密下不断动态发展。有的措施一旦应用就会暴露，使用时机是

一个重要问题，对方也往往千方百计获得雷达的对抗技术信息，包括必要时采取佯攻手法在内，诱使雷达露出对抗技术底牌，然后再采取攻击措施，这也是一种围绕对抗信息的斗争方法。表 6.2 简要说明靠目标反射回波工作的雷达机理，容易提供对方进行对抗所需的重要信息。

表 6.2　围绕雷达工作形成的信息斗争

雷 达 方	对 抗 攻 击 方
雷达运用组成网络层次 雷达布置的地理坐标（含高度坐标）、信息，雷达网络组成拓扑结构。包括：雷达类型及系统功能信息等。本类信息往往是由雷达系统的技术层次的各项具体参数综合所形成	雷达基本参数是对方所欲获得的基本信息，往往通过成像侦察接收信号定位等多种手段综合判断确定 利用上述方法和得到的下述信息分析推断雷达网络拓扑结构 攻击方利用侦察截获雷达信息后，形成己方对抗信息如下： · 何种类型雷达：如战略预警、中远程警戒、指挥引导、区域防御火控、点防御火控…… · 雷达工作类应用型：经常值班、预备值班、机动布置
雷达系统技术层次 · 雷达工作频段 · 信号形式及特征：信号调制、信号重复周期、功率电平、天线类型、波束宽度及形状、天线控制方式、雷达抗干扰措施	推测雷达集成的更大规模武器系统的信息。如由区域内雷达可推测出区域防御武器系统的存在；由指挥引导雷达推测空军战斗部队的存在

总体而言，对抗信息的形成是复杂动态变化的，又是相互渗透相反相成的。采用一种对抗措施同时又附带一种对抗信息提供对方进行对抗作用，从而形成了一个双方激烈对抗过程。

6.4.2　雷达安全对抗问题分析举例

由于雷达对抗内容的敏感性，在此只作一般性原理说明。雷达安全对抗可分为三个层次分析，第一层次是围绕“信息－信号”展开的，第二个层次是针对雷达进一步功能展开的对抗斗争，第三层次是围绕雷达生存发展的。每一个层次再可细分若干层次，其对抗内容也不断发展变化。

雷达是通过接收和检测回波信号完成其功能－目标信息的获得，围绕回波信号斗争是一个基本环节，如表 6.3 所示。

表 6.3　围绕信息－信号的斗争说明

雷 达 方	攻 击 方
展宽频带，增加工作频率点，快速变频，增加发射功率及照射功率密度，各种先进的天线波束控制方式	掌握雷达工作频率频段、利用雷达回波强度正比例于 $1/R^4$，干扰强度正比例于 $1/R^2$ 的先天优势，攻击方常用于施放各种频带内，也可快速跟随雷达频率干扰以压制雷达回波，破坏雷达回波检测以破坏获得目标信息
多种方式设计低截获概率信号或隐藏雷达发射信号	加强信号检测分析能力
雷达架高（包括利用空中平台）及提高在地海强回波背景下检测运动目标回波的能力	进入雷达探测区域后低空和超低空飞行，利用地球曲率遮挡及地物回波掩没，避开雷达探测
利用较长波长信号及利用回波谐振现象以对抗隐身目标	对目标进行隐身设计，减小反射回波强度以压缩雷达控测距离
其他包括空间滤波、极化滤波等多维滤波技术滤去干扰，以助回波信号检测	加大干扰功率密度，增强干扰效果

围绕雷达后续作战功能的对抗斗争：雷达后续作战功能对双方更加重要，故对抗是更激烈的斗争，情况更为复杂与多样化，现扼要讨论如表 6.4 和表 6.5 所示。

表 6.4　针对雷达后续功能的对抗斗争

雷 达 方	攻 击 方
敌我目标属性鉴别问题，在技术上快速全面准确鉴别难度很大，只能部分解决，雷达现采用我方目标利用密码应答形成我雷达对目标的专门问询，同时在敌我识别应答系统中不断采取各种先进对抗安全技术以保证正确的询问应答不被对方利用，以便伪装为我机雷达的目标回波成像，可对雷达后续功能的发挥起重要作用（现在正大力研究）	主要攻击询问应答系统，制造假应答或干扰应答产生敌我不分 研究各种破坏雷达回波成像的科技方法
雷达跟踪目标（含多批目标）是完成后续功能的重要特性 雷达利用各种干扰与目标回波特性区别，采用各种反其道而行之方法保持雷达跟踪性能	对抗雷达的目标跟踪功能，制造伪信号引诱雷达错误跟踪，施放干扰（包括铂条干扰丝等）以破坏雷达跟踪
采用复合制导，提高快速反应能力，提高制导信号及通信链传输信号等各种抗干扰能力	破坏雷达制导信号 破坏雷达与指挥系统间的信息链

表 6.5　对雷达站进行毁伤性攻击，以图摧毁雷达

利用可机动雷达快速机动布置，破坏 GPS 预先装的地理坐标	利用巡航导弹及反辐射导弹攻击
利用对攻击雷达目标进行快速认定，采取击毁误导等针锋相对措施	提高攻击导弹低空飞行速度，使对方来不及反应

总之，雷达的攻击对抗是一个复杂动态系统的对抗问题，没有终结答案，所有对抗手段只具有相对有效性，是在矛盾中不断发展的，很多新原理、新技术不断引入，充分体现了对立统一发展规律。

6.5　计算机网络的安全与对抗问题

本节将运用信息安全与对抗的基本原理、基本方法具体讨论计算机信息网络系统的信息安全与对抗问题，主要从以下几个方面来讨论：计算机信息网络的系统组成、不安全因素分析、网络攻击和防御行为分析、网络攻击与对抗过程分析以及目前存在问题分析等。

6.5.1　系统组成

简单地说，计算机网络就是由难以计数的局域网互联而成，局域网络是互联网的基本单位，局域网之间的连接通过传输系统和 TCP/IP 协议链接在一起，从而构成互联网。局域网的基本元素为用户终端、服务器、打印机、扫描仪、交换机、集线器、路由器等硬件部件，以及操作系统、应用软件等软件系统。对于计算机网络的安全性，应从系统角度多个层次来分析，攻击行为最终针对于具体的信息系统或主机，所以计算机网络的安全一般以局域网络和安全作为保护对象（一个部门、一个单位、一个企业等），对于国家基础设施由国家统一考虑。本文的分析主要针对一个局域网络的安全与对抗的综合分析。信息系统一般由物理环境及保障、硬件设施、软件设施和管理者等部分组成。

6.5.2　不安全因素分析

网络系统无论从其信息处理的各个环节，还是信息系统结构上都存在不同程度的漏洞或者本身的脆弱性，这些缺陷导致系统存在不同程度的威胁和攻击。除了由于网络系统本身存在的缺陷构成的威胁和攻击外，还存在其他方面的威胁和攻击，如自然灾害、信息战等。系统、有效地分析系统的不安全因素，评估其产生的风险，就可以依据等级保护的策略，指导系统安全保障体系的建设。

一、面临的威胁

系统面临的威胁和攻击主要来自于自然灾害、人为或偶然事故、计算机犯罪、计算机病毒以及信息战等几个方面。下面简单介绍。

① 自然灾害。自然灾害主要指火灾、水灾、风暴、地震等破坏，以及环境（温度、湿度、振动、冲击、污染）的影响。据有关方面调查，我国不少计算机房没有防震、防火、防水、避雷、防电磁泄露或干扰等措施，接地系统疏于周到考虑，抵御自然灾害和意外事故的能力较差，事故不断，因断电而设备损坏、数据丢失的现象屡见不鲜。

② 人为或偶然事故。常见的事故有：硬、软件的故障引起安全策略失效；工作人员的误操作使系统出错，使信息严重破坏或无意地让别人看到了机密信息；自然灾害的破坏，如洪水、地震、风暴、泥石流，使计算机系统受到严重破坏；环境因素的突然变化，如高温或低温、各种污染破坏了空气洁净度，电源突然掉电或冲击造成系统信息出错、丢失或破坏等。

③ 计算机犯罪。计算机犯罪是利用暴力和非暴力形式，故意泄露或破坏系统中的机密信息，以及危害系统实体和信息安全的不法行为。暴力形式是对计算机设备和设施进行物理破坏，如使用武器摧毁计算机设备，炸毁计算机中心建筑等。非暴力形式是利用计算机技术知识及其他技术进行犯罪活动。1997 年 3 月 14 日我国颁布的《中华人民共和国刑法》对计算机犯罪作了明确的规定，涉计算机犯罪有两类形式，一类是破坏计算机信息系统罪，另一类是入侵计算机信息系统罪（见《刑法》第 285，286，287 条）。

④ 计算机病毒。计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。因为这些程序的很多特征是模仿疾病病毒，所以人们使用“病毒”一词。这些特征包括潜伏与自我复制能力、传播能力，会对系统或网络造成破坏，轻则系统运行效率下降，部分文件丢失，重则造成系统死机，网络瘫痪，正是因为计算机病毒有如此大的危害性，恐怖主义者用计算机病毒制造破坏，一些国家的军事和国家安全部门将计算机病毒作为重要的信息战武器来研究。可以说，计算机病毒是最常见的危害信息系统的手段，防不胜防。

⑤ 信息战。信息战是指为了国家的军事战略而取得信息优势，干扰敌方的信息和信息系统，同时保卫自己的信息和信息系统所采取的行动。这种对抗形式的目标在于，不是集中打击敌方的人员或战斗技术装备，而是集中打击敌方的信息系统，瘫痪其神经中枢的指挥系统。信息技术将根本改变战争的方法，就像坦克的运用引起了第一次世界大战战争艺术的变革一样。继原子武器、生物武器、化学武器的后，信息武器已被列为第四类战略武器。如在海湾战争中，首次将信息武器用于实战，在伊拉克购买的智能打印机中，植入一片带有病毒的集成电路，加上其他因素，最终导致伊拉克指挥系统的崩溃。

二、系统的安全缺陷

本文将网络系统的安全缺陷定义为与系统相关的漏洞或脆弱性，其可以导致系统抵御攻击的能力减弱。下面从几个方面加以分析。

1. 数据处理环节上的安全缺陷

数据处理的各个环节都有可能存在脆弱性。如：

① 数据输入：数据通过输入设备进入系统，输入数据容易被篡改或输入假的数据。

② 数据处理：数据处理部分的硬件容易被破坏或盗窃，并且容易受电磁干扰或由于电磁辐射而造成信息泄露。

③ 数据传输：通信线路上的信息容易被截获，线路容易被破坏或盗窃。

④ 数据输出：输出信息的设备容易造成信息泄露或被窃取。

⑤ 管理控制：系统的安全管理和控制方面的能力还比较弱，问题较多。

⑥ 软件：操作系统、数据库系统和应用程序容易被修改或破坏。

2. 软件上的安全缺陷

由于软件程序的复杂性和编程的多样性，在网络信息系统的软件中很容易有意或无意地留下一些不易被发现的安全漏洞，软件漏洞显然会影响信息系统的安全。

① 陷门：所谓陷门是一个程序模块的秘密的、未写入相关文档的入口。一般情况下，陷门是在程序开发时插入的一小段程序，用于测试这个模块或升级程序，或是为了发生故障后为程序员提供方便，通常在程序开发后期会去掉这些陷门，但由于有意或无意的原因，陷门也可能被保留下来。陷门一旦被原来的程序员利用，或者被无意或有意的人，发现将会带来严重的安全后果。比如，可能利用陷门在程序中建立隐蔽通道，甚至植入一些隐蔽的病毒程序等。利用陷门可以非法访问网络，达到窃取、更改、伪造和破坏的目的，甚至有可能造成信息系统的大面积瘫痪。常见的陷门有：逻辑炸弹、遥控旁路、贪婪程序等。

② 操作系统的安全漏洞：操作系统不安全的首要原因是操作系统结构体制造成的，操作系统的程序是可以动态连接的，包括 I/O 的驱动程序与系统服务，都可以用打补丁的方式进行动态连接。许多 UNIX 操作系统的版本进化开发，都是采用打补丁的方式进行开发的。这种方法厂商可用，“黑客”也可用，这种动态连接也是计算机病毒产生的环境。一个靠渗透与打补丁开发的操作系统是不可能从根本上解决安全问题的。然而，操作系统支持程序动态连接与数据动态交换是现代系统集成和系统扩展的需要，显然，系统集成与系统安全是矛盾的。操作系统不安全的原因还在于可以创建进程，甚至支持在网络的结点上进行远程进程的创建与激活，更为重要的是被创建的进程还继承创建进程的权力。此外，操作系统还有隐蔽信道等。

③ 数据库的安全漏洞：数据库是从操作系统的文件系统基础上派生出来的用于大量数据管理的系统。数据库的全部数据都记录在存储媒体上，并由数据库管理系统（DBMS）统一管理。DBMS 为用户及应用程序提供一种访问数据的方法，并且对数据库进行组织和管理，对

数据库进行维护和恢复。数据库系统的安全策略，部分由操作系统来完成，部分由强化 DBMS 自身安全措施来完成。数据库系统存放的数据往往比计算机系统本身的价值大得多，必须加以特别保护。

④ TCP/IP 协议的安全漏洞：TCP/IP 通信协议，在设计初期并没有考虑到安全性问题，而且用户和网络管理员没有足够的精力专注于网络安全控制，加上操作系统和应用程序越来越复杂，开发人员不可能测试出所有的安全漏洞，连接到网络上的计算机系统就可能受到外界的恶意攻击和窃取。

3. 硬件结构隐患

拓扑逻辑是构成网络的结构方式，是连接在地理位置上分散的各个节点的几何逻辑方式。拓扑逻辑决定了网络的工作原理及信息的传输方法。一旦网络的拓扑逻辑被选定，必定要选择一种适合这种拓扑逻辑的工作方式和信息传输方式。事实上，网络的拓扑结构本身就有可能给网络的安全带来问题，如总线型拓扑结构故障诊断困难、容易被窃听；星型拓扑结构扩展困难、对中央节点的依赖性太强等。

4. 其他方面的安全缺陷

信息系统中除了软件、硬件的外，还包括许多其他要素，其中也存在不同程度上的安全缺陷。如存储密度高，在一张磁盘或一条磁带中可以存储大量信息，很容易放在口袋中带出去，容易受到意外损坏或丢失，造成大量信息的丢失。信息聚生性：当信息以分离的小块形式出现时，它的价值往往不大，但将大量信息聚集在一起时，信息的间的相关特性将极大地显示出这些信息的重要价值，信息的这种聚生性与其安全密切相关。介质的剩磁效应，存储介质中的信息有时是擦除不干净或不能完全擦除掉，会留下可读信息的痕迹，一旦被利用，就会泄密。如许多信息系统中的所谓删除文件仅仅是删除了该文件在目录中的文件名，其内容并没有真正的删除，因此很容易被恢复。甚至是格式化后的磁盘，其信息也可能被恢复。电磁泄露，计算机设备工作时能够辐射出电磁波，任何人都可以借助仪器设备在一定的范围内收到它，尤其是利用高灵敏度仪器可以清晰地看到计算机正在处理的机密信息。电磁泄露是计算机信息系统的一大隐患。此外，电磁泄露还可能干扰其他电磁设备的正常工作等。

5. 中国特色的安全缺陷

鉴于我国目前的情况，系统除了具有上述普遍存在的安全缺陷以外，还有其他一些独具特色的安全缺陷。比如，由技术被动性引起的安全缺陷。首先，芯片基本依赖于进口，即使是自己开发的芯片也需要到国外加工，只有当我国的半导体和微电子技术取得突破性进展的后，才能从根本上摆脱这种受制于人的状态。其次，为了缩小与世界先进水平的差距，我国引进了不少外国设备，但这也同时带来了不可轻视的安全缺陷。如大部分引进设备都不转让知识产权很难获得完整的技术档案。可怕的是，有些引进设备可能在出厂时就隐藏了恶意的“定时炸弹”或者“陷门”。又如由于人员素质问题引起的安全缺陷，法律靠人去执行，管理靠人去实现，技术靠人去掌握。人是各个安全环节中最重要的因素。全面提高人员的道德品质和技术水平

是网络信息安全的最重要保证。当前，系统规模在不断扩大，技术在不断更新，新业务在不断涌现，这就要求人去不断地学习，不断地提高其技术和业务水平。另外，思想品德的教育也是十分重要的，许多安全事件都是由思想素质有问题的内部人员引起的。还有缺乏系统的安全标准所引起的安全缺陷。目前，我国信息安全标准数量远少于现有产品品种，尚未形成较为完整的信息安全标准体系，已颁布的国家标准，绝大多数为框架性基础标准，具有方法论的指导作用，而不是可操作的标准，有限的产品标准技术上滞后，事实上不具有标准的指导作用。缺乏安全标准不但会造成管理上的混乱，对安全技术和产品的研发缺乏指导，而且也会使攻击者更容易得手。

总之，各种不安全因素使得计算机信息系统存在种种漏洞和表现出种种脆弱性。

6.5.3　攻击行为和方法分析

按被攻击的对象划分，可将系统的攻击分为两类：一类是针对信息系统实体的，一类是针对信息的。

对实体的攻击：主要指对系统设备、网络及其环境的攻击，如各种自然灾害与人为的破坏、设备故障、场地和环境因素的影响、电磁场的干扰或电磁泄露、战争的破坏、各种媒体的被盗和散失等。对信息系统实体的攻击，不仅会造成国家财产的重大损失，而且会使信息系统的机密信息严重泄露和破坏。因此，对系统实体的保护是防止针对信息系统攻击的首要一步，也是防止对信息攻击的天然屏障。

对信息的攻击主要有两种，一种是信息的泄露；另一种是信息的破坏。信息泄露就是偶然地或故意地获得（侦收、截获、窃取或分析破译）目标系统中的信息，特别是敏感信息，造成泄露事件。信息破坏是指由于偶然事故或人为破坏，使信息的正确性、完整性和可用性受到破坏，使得系统的信息被修改、删除、添加、伪造或非法复制，造成大量信息的破坏、修改或丢失。

根据攻击的方式进行分类，可将攻击行为分为被动攻击和主动攻击两类。

被动攻击：是指一切窃密的攻击，它是在不干扰系统正常工作的情况下进行侦收、截获、窃取系统信息。利用观察信息、控制信息的内容来获得目标系统的设置、身份。利用研究机密信息的长度和传递的频度获得信息的性质。被动攻击不容易被用户察觉出来，它的攻击持续性和危害性都很大。被动攻击的主要方法有：

① 直接侦听。利用电磁传感器或隐藏的收发信息设备，直接侦收或搭线侦收信息系统的中央处理机、外围设备、终端设备、通信设备或线路上的信息。

② 截获信息。系统及设备在运行时，散射的寄生信号容易被截获。如离计算机显示终端（CRT）百米左右，辐射信息强度可达 30 dB(uV)以上，因此可以在那里接收到稳定、清晰可辨的信息图像。此外，短波、超短波、微波和卫星等无线电通信设备有相当大的辐射面，市话线路、长途架空明线等电磁辐射也相当严重，因此可利用系统设备的电磁辐射截获信息。

③ 合法窃取。利用合法用户身份，设法窃取未授权的信息。例如，在统计数据库中，利用多次查询数据的合法操作，推导出不该了解的机密信息。

④ 破译分析。对于已经加密的机要信息，利用各种破译分析手段获得机密信息。

⑤ 从遗弃的媒体中分析获取信息。如从信息中心遗弃的打印纸、各种记录和统计报表、窃取或丢失的软盘片中获得有用信息。

主动攻击：是指篡改信息的攻击，它不仅是窃密，而且威胁到信息的完整性和可靠性。它是以各种各样的方式，有选择地修改、删除、添加、伪造和复制信息内容，造成信息破坏。主动攻击的主要方法有：

① 窃取并干扰通信线中的信息。

② 返回渗透。有选择地截取系统中央处理机的通信，然后将伪信息返回系统用户。

③ 线间插入。当合法用户已占用信道而终端设备还没有动作时，插入信道进行窃听或信息破坏活动。

④ 非法冒充。采取非常规的方法和手段，窃取合法用户的标识符，冒充合法用户进行窃取或信息破坏。

⑤ 系统人员的窃密和毁坏系统数据、信息的行为等。

主要的计算机网络攻击技术和方法有：网络数据侦听、计算机病毒、特洛伊木马、IP 欺骗、WEB 欺骗、拒绝服务攻击、缓冲区溢出攻击等。

6.5.4 防御行为和方法分析

计算机网络信息系统的保护和防御应该是多层、多剖面的综合体，目前还不能做到这一点。计算机网络信息系统的安全保护可以从技术和管理两大方面来考虑，从管理角度注重信息系统的安全管理（包括人员、设备、日常等多方面的管理活动）。从技术角度来讲包括信息实体、信息、信息系统等多方面的安全保护，具体方法和技术主要有：防火墙技术、入侵检测技术、反计算机病毒技术、身份认证及权限控制技术、安全管理、电磁防护、实体安全技术、快速反映和灾难恢复技术、信息隐藏技术、数据加密解密技术以及系统开发实施过程中的安全控制技术等，还有针对于网络传输系统的 SSL、SET、VPN、IPSEC 等技术。

6.5.5 攻击与对抗过程分析

一、攻击行为过程分析

如图 6.4 所示为一般攻击行为过程示意图，一个攻击行为的发生一般有三个阶段，即攻击

准备、攻击实施和攻击后处理。当然这种攻击行为有可能对攻击目标未造成任何损伤或者说攻击未成功。下面简介各阶段的主要内容及特点。

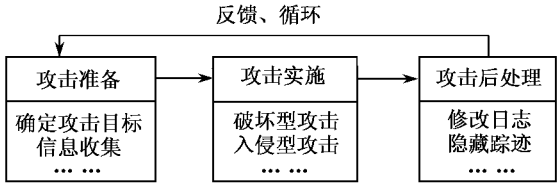


图 6.4　攻击行为过程示意图

1. 攻击准备

攻击的准备阶段可分为确定攻击目标和信息收集两个子过程。攻击前首先确定攻击目标，而后确定要达到什么样的攻击目的，即给对方造成什么样的后果，常见的攻击目的有破坏型和入侵型两种。破坏型攻击指的破坏目标，使其不能正常工作，而不是控制目标系统的运行。另一类是入侵型攻击，这种攻击是要获得一定的权限达到控制攻击目标或窃取信息的目的。入侵型攻击较为普遍，威胁性大，因为一旦获得攻击目标的管理员权限就可以对此服务器做任意动作，包括破坏性质的攻击。此类攻击一般利用服务器操作系统、应用软件或者网络协议等系统中存在的漏洞进行。在确定攻击目标的后，最重要的是收集尽可能多的关于攻击目标的信息，以便实施攻击。这些信息主要包括：目标的操作系统类型及版本，目标提供的服务类型，各服务器程序的类型、版本及相关的各种信息等。

2. 攻击实施

当收集到足够的信息后，攻击者就可以实施攻击了，对于破坏型攻击只需利用必要的工具发动攻击即可。作为入侵型攻击，往往要利用收集到的信息找到系统漏洞，然后利用该漏洞获得一定的权限，有时获得一般用户的权限就足以达到攻击的目的。一般攻击者都想尽办法获得系统最高权限，这不仅为了达到入侵的目的，在某种程度上也是为了显示攻击者的实力。系统漏洞一般分为远程和本地漏洞两种，远程漏洞是指可以在别的机器上直接利用该漏洞进行攻击并获得一定的权限，这种漏洞的威胁性相当大，攻击行为一般是从远程漏洞开始。利用远程漏洞不一定获得最高权限，往往获得一般用户的权限。只有获得了较高的权限（如管理员的权限）才可以进行入侵行为（如放置木马程序）。

3. 攻击后处理

如果攻击者完成攻击后，立刻离开系统而不做任何后续工作，那么他的行踪将很快被系统管理员发现，因为所有的网络操作系统都提供日志记录功能，会把系统上发生的事件记录下来，所以攻击者发动完攻击后，一般要做一些后续工作。对于破坏型攻击，攻击者隐匿踪迹是为了不被发现，而且还有可能再次收集信息以此来评估攻击后的效果。对于入侵型攻击最重要的是隐匿踪迹，攻击者可以利用系统最高管理员身份随意修改系统上文件的权利。隐匿踪

迹最简单的方法是删除日志，但这样做虽然避免了系统管理员根据日志的追踪，但也明确地告诉管理员系统已经被入侵了，一般采用的方法是修改日志中与攻击行为相关的那一部分日志，而不是删除日志。只修改日志仍不够，有时还会留下蛛丝马迹，高级攻击者可以通过替换一些系统程序的方法进一步隐藏踪迹。此外，攻击者在入侵系统后还有可能再次入侵该系统，所以为了下次进入的方便，攻击者往往给自己留下后门，如给自己添加一个账号、增加一个网络监听的端口、放置木马等。还有一种方法，即通过修改系统内核的方法可以使管理员无法发现攻击行为的发生，这种方法需要较强的编程技巧，一般的攻击者较难完成。

二、防御行为过程分析

一般情况下被攻击方几乎始终处于被动局面，他不知道攻击行为在什么时候、以什么方式、以什么样的强度来攻击，故而被攻击方只有沉着应战才有可能获取最佳效果，把损失降到最低。单就防御来讲，相应于攻击行为过程，防御过程也可分为三个阶段，如图 6.5 所示，即确认攻击、对抗攻击、补救和预防。防御方首先要尽可能早地发现并确定攻击行为、攻击者，所以平时信息系统要一直保持警惕，收集各种有关攻击行为的信息，不间断地进行分析、判定。系统一旦确定攻击行为的发生，无论是否具有严重的破坏性，防御方都要立即、果断的采取行动阻断攻击，有可能的情况下以主动出击的方式进行反击（如对攻击者进行定位跟踪）。此外，尽快修复攻击行为所产生的破坏性，修补漏洞和缺陷来加强相关方面的预防，对于造成严重后果的还要充分运用法律武器。

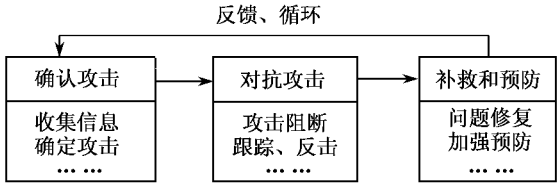


图 6.5　防御行为过程示意图

1. 确认攻击

攻击行为一般会产生某些迹象或者留下踪迹，可根据系统的异常现象发现攻击行为：如异常的访问日志；网络流量突然增大；非授权访问（如非法访问系统配置文件）；正常服务的中止；出现可疑的进程或非法服务；系统文件或用户数据被更改；出现可疑的数据等。发现异常行为后，要进一步根据攻击的行为特征，分析、核实入侵者入侵的步骤，分析入侵的具体手段和入侵目的。一旦确认出现攻击行为，即可进行有效的反击和补救。总的，确认攻击是防御、对抗的首要环节。

2. 对抗攻击

一旦发现攻击行为就要立即采取措施以免造成更大的损失，同时在有可能的情况下给予迎头痛击，追踪入侵者并绳之以法。具体地，可根据获知的攻击行为手段或方式采取相应的措施。比如，针对于后门攻击及时堵住后门；针对病毒攻击利用杀毒软件或暂时关闭系统以免扩大受害面积等。还可采取反守为攻的方法，追查攻击者，复制入侵行为的所有影像作为法律追查分析、证明的材料，必要时直接通过法律武器解决或报案。

3. 补救和预防

一次攻击和对抗过程结束后，防御方应吸取教训，及时分析和总结问题所在，对于未造成损失的攻击要修补漏洞或系统缺陷；对于已造成损失的攻击行为，被攻击方应尽快修复，尽早使系统工作正常，同时修补漏洞和缺陷，关闭不用的端口，必要的情况下运用法律武器追究攻击方的责任。总的，无论是否造成损失，防御方均要尽可能的找出原因，并适时进行系统修补（亡羊补牢），而且要进一步采取措施（管理和技术）加固系统和加强预防。

三、攻击与对抗过程的“共道”—“逆道”抽象模型

如图 6.6 所示为根据第四章所讲的抽象“共道”—“逆道”模型建立的计算机网络的系统对抗过程的“共道—逆道”模型。

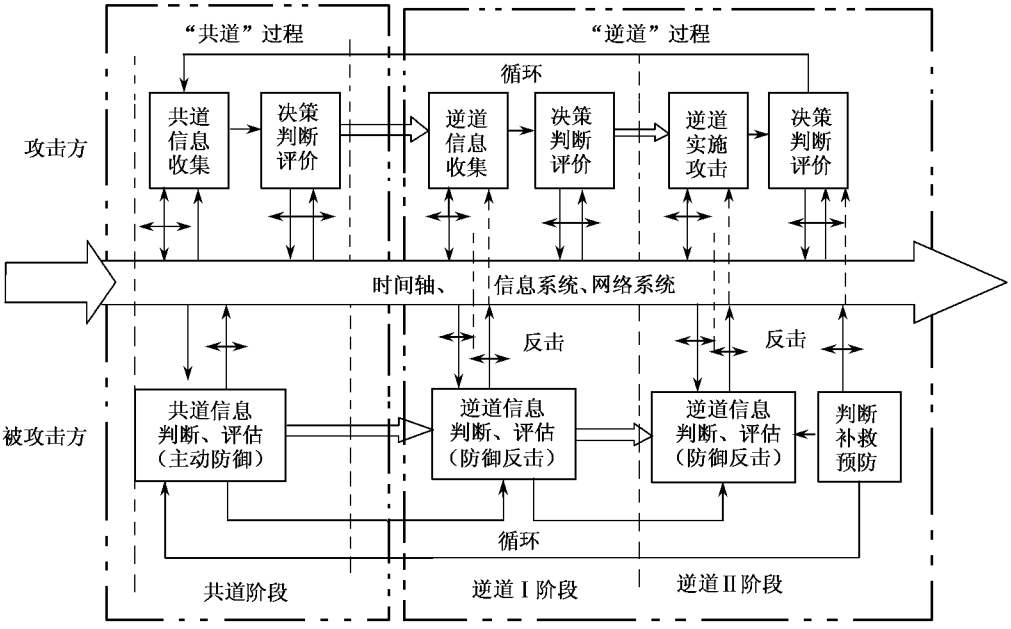


图 6.6　信息系统攻击与对抗过程“共道—逆道”模型

攻击与对抗首先是一个过程，对于整个系统以及时间轴来讲，这个过程随着人类社会的发展而不断连续，即攻击与对抗过程贯穿于人类社会发展的整个过程。过程是相对于时间而言的，网络攻击与对抗过程模型应以时间轴为基准，把整个攻击和对抗行为映射于相对位置的时间轴上，其时间关系对于双方在不透明情况下的对抗斗争以及获得对抗信息很重要，即获得信息越及时、越早越好，行动也要尽早、尽快，要力争在对方来不及反应前动手，即“攻其不备”，时间拖得越长信息越容易暴露，行动就越易于失败，同时也会丧失主动权，这些是攻守双方都力求避免的局面。

综合考虑时间因素、过程因素以及“道”的因素，便形成了具有串联结构的网络系统对抗过程的“共道–逆道”抽象模型（如图 6.6 所示）。从图中可以明显得出，总体上讲，对于一次对抗过程可分为三个阶段，即“共道”阶段、“逆道Ⅰ”阶段和“逆道Ⅱ”阶段。前面分析中，攻击方和被攻击方行为也分为三个阶段，但这与对抗过程模型中的三个阶段的划分有所不同，即对抗过程模型不是攻击和防御过程三阶段的简单堆砌或拼凑。模型以时间轴为基准，攻击方和被攻击方的行为有较严格的时间对照关系。很明显，被攻击方一般情况下处于被动局面，虽然能提供主动防御措施，但很难预测得出攻击行为的发生（虽然通过统计可以发现某些类型的攻击，但大多数据情况下这种方法并不能起作用）。攻击方始终处于主动，能在任何时间、任意地点以任何方式实施攻击（注：图中的横向双箭头是指该“行为”在时间轴上的移动）。

下面对对抗过程模型进行具体分析、运用：

“共道”阶段：对于攻击方而言，在“共道”阶段将主要利用共有的信息（如 TCP/IP 协议、操作系统类型、应用软件、防火墙类型、杀毒软件类型、CPU 类型等）进行信息收集，当收集到足够信息后便可做出决策，是否需要进一步收集“逆道”信息（如操作系统的漏洞、系统开放的端号、应用软件的漏洞、防火墙的缺陷等）或实施攻击。如果欲立即实施攻击，其过程便可直接转至“逆道Ⅱ”阶段，即实施攻击阶段（如拒绝服务攻击，它并不需要收集逆道信息便可直接实施攻击），这种情况下整个攻击与对抗过程就分为两个阶段，即“共道”和“逆道Ⅱ”阶段。对于被攻击方而言，在“共道”阶段很难获得攻击行为所表现的信息，这主要是因为“共道”阶段攻击行为无显著特征（攻击方在收集信息的过程中可能会不留下任何踪迹，如在端口或漏洞扫描时采用不同的策略使被攻击方很难感觉到扫描事件的发生），故很难采取必要的反击措施，但这个阶段被攻击方可以采取必要的措施进行主动防御技术（如更新操作系统，更新杀毒软件，关闭不用的端口，使用物理隔离技术，使用入侵检测系统，使用蜜罐技术，定期查看和分析日志等），尽可能消除系统的缺陷和漏洞。同时，加强管理手段和措施，以使攻击方无机可乘。“共道”阶段，对于被攻击方而言，只是对后续的攻击提供信息积累作用，为反击提供支持，该阶段很难实施对抗反击行为。

“逆道”过程总体上分为两个阶段，即“逆道Ⅰ”和“逆道Ⅱ”阶段。这两个阶段对于一次具体的攻击和对抗过程，也有可能只存“逆道Ⅱ”阶段，而不存在“逆道Ⅰ”阶段，这种情况下，攻击方通过“逆道Ⅱ”阶段便达到了攻击的目的，而不需要实施“逆道Ⅰ”阶段的信息收集，这种攻击

行为一般属于破坏型攻击(如前面提到的拒绝服务攻击)。大多数情况下,对于攻击者来说必须通过“逆道Ⅰ”信息收集才有可能达到攻击目的。没有通过“逆道Ⅰ”过程收集到足够的“逆”信息,无法实施具体的攻击,不能达到最终的攻击目的(如木马攻击),这种情况下“逆道”两个阶段都需要,缺一不可。对于被攻击方而言,如果在“逆道Ⅰ”阶段确认了攻击行为或实施了有效的反击,则是对攻击方的一种沉重打击,攻击方有可能就此停止攻击行为,被攻击方也不会造成大的损失。若被攻击方对“逆道Ⅰ”阶段未引起足够的重视,则于“逆道Ⅱ”阶段的反击将会受到很大影响,有可能造成很大的损失。此外,“逆道Ⅰ”阶段也许是被攻击方采取主动的机会,被攻击方可以采取诱骗和陷阱技术给攻击者以致命的打击。总之,攻防双方谁在时间上占有优势,谁就有可能占有主动,被攻击方才有可能从被动转为主动。

一次攻击与对抗过程完成后,便循环进入下一轮对抗。对于被攻击方来讲,要充分总结经验、亡羊补牢,加强预防措施(进一步加固系统),或变被动为主动,主动追击攻击者(如迅速跟踪定位,通过法律手段惩戒攻击方)。对于攻击方来讲,要对攻击行为产生的后果进行评估,判断是否达到了攻击目的,是否隐藏了自己的踪迹,是否需要进入下一轮的攻击……

关于对抗过程的进一步说明:

① 就共性和本质而言,“共道—逆道”模型是攻击与对抗过程的一种基础模型,在攻击与对抗过程中,“共道”和“逆道”环节缺一不可,是必然的环节,否则不能称为对抗过程,这也正是矛盾对立统一规律的体现。

② 对于信息网络系统,其功能越多、应用越广,其重要性越大,则可能遇到的攻击种类和次数越多,这就是信息系统的“道”,同样反其“道”也就越多、越广。从这一角度来讲,单项或单元攻击与对抗的研究是必要的,但远远不够,应从系统的角度,综合地、整体地分析、讨论,即考虑到它的特殊性又要考虑到它的普适性。

③ 防御反击即可以采用单项技术又可以采用综合性技术(技术、组织、管理、法律等)。针对单项技术攻击采用相应单项或综合性反击措施,对综合性攻击只有采用综合性反击措施。

④ 信息攻击与对抗的系统性研究极为必要。攻击即是防御,防御也可为攻击,二者辩证统一。但攻击行为可以以任意时间、任意地点、任意方式进行,特别是随着当前信息系统、信息网络的快速发展,全球已逐渐形成一个整体,其安全与对抗问题的研究就更为重要,系统地研究攻击与对抗行为过程可以实现更为有效攻击和防御。

6.5.6　存在问题分析

尽管目前针对于计算机网络系统的安全技术很多,但都是针对性较强的技术,如果能从系统的角度来考虑信息及信息系统的安全技术,从整体上统一考虑,根据信息安全与对抗的基础层次、系统层次定理、原理、方法与技术,研究、设计综合计算机网络信息系统的安全系统将会更有效。

6.6 本章小结

本章以通信、雷达、计算机网络三种典型信息系统为例，说明信息安全与对抗基本原理、方法、技术的应用。分析了通信信息系统的抗攻击的安全考虑内容、安全措施和特点，同时讨论了高安全要求的移动无缝隙广域通信系统的对抗问题；分析了地基和卫星广播电视系统的安全性；详细分析了计算机网络信息系统的不安全因素、系统本身的脆弱性，以及攻击和防御对抗行为和过程。

习　题

1. 分析和讨论通信系统的安全与对抗体系。
2. 分析和讨论雷达系统的安全与对抗体系。
3. 典型计算机网络系统的不安全因素主要有哪些？
4. 以典型计算机网络系统为例说明其攻击与防御过程。
5. 以“共道”—“逆道”博弈模型分析计算机网络系统的攻击与防御过程。

附　录

附录 1　《中华人民共和国刑法》节选

（1997 年 7 月 1 日第八届全国人民代表大会第五次会议修正通过，1997 年 10 月 1 日实施）

第一百一十一条　为境外的机构、组织、人员窃取、刺探、收买、非法提供国家秘密或者情报的，处五年以上十年以下有期徒刑；情节特别严重的，处十年以上有期徒刑或者无期徒刑；情节较轻的，处五年以下有期徒刑、拘役、管制或者剥夺政治权利。

第一百二十四条　破坏广播电视设施、公用电信设施，危害公共安全的，处三年以上七年以下有期徒刑；造成严重后果的，处七年以上有期徒刑。过失犯前款罪的，处三年以上七年以下有期徒刑；情节较轻的，处三年以下有期徒刑或者拘役。

第二百一十九条　有下列侵犯商业秘密行为之一的，给商业秘密的权利人造成重大损失的，处三年以下有期徒刑或者拘役，并处或者单处罚金；造成特别严重后果的，处三年以上七年以下有期徒刑，并处罚金：（一）以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密的；（二）披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密的；（三）违反约定或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密的。明知或者应知前面条款所列行为，获取、使用或者披露他人商业秘密的，以侵犯商业秘密论罪。本条所称商业秘密，是指不为公众所知悉，能为权利人带来经济利益，具有实用性并经权利人采取保密措施的技术信息和经营信息。本条所称权利人，是指商业秘密的所有人和经商业秘密所有人许可的商业秘密使用人。

第二百八十二条　以窃取、刺探、收买方法，非法获取国家秘密的，处三年以下有期徒刑、拘役、管制或者剥夺政治权利；情节严重的，处三年以上七年以下有期徒刑。非法持有属于国家绝密、机密的文件、资料或者其他物品，拒不说明来源与用途的，处三年以下有期徒刑、拘役或者管制。

第二百八十三条　非法生产、销售窃听、窃照等专用间谍器材的，处三年以下有期徒刑、拘役或者管制。

第二百八十四条　非法使用窃听、窃照等专用间谍器材，造成严重后果的，处二年以下有期徒刑、拘役或者管制。

第二百八十五条　违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

第二百八十六条　违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造

成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役，后果特别严重的，处五年以上有期徒刑。违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

第二百八十七条　利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

第二百八十八条　违反国家规定，擅自设置、使用无线电台（站），或者擅自占用频率，经责令停止使用拒不停止使用，干扰无线电通讯正常进行，造成严重后果的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金。单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照前款的规定处罚。

第三百六十三条　以牟利为目的，制作、复制、出版、贩卖、传播淫秽物品的，处三年以下有期徒刑、拘役或者管制，并处罚金；情节严重的，处三年以上十年以下有期徒刑，并处罚金；情节特别严重的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。为他人提供书号，出版淫秽书刊的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；明知他人用于出版淫秽书刊而提供书号的，依照前款的规定处罚。

第三百六十四条　传播淫秽的书刊、影片、音像、图片或者其他淫秽物品，情节严重的，处二年以下有期徒刑、拘役或者管制。组织播放淫秽的电影、录像等音像制品的，处三年以下有期徒刑、拘役或者管制，并处罚金；情节严重的，处三年以上十年以下有期徒刑，并处罚金。制作、复制淫秽的电影、录像等音像制品组织播放的，依照第二款的规定从重处罚。向不满十八周岁的未成年人传播淫秽物品的，从重处罚。

第三百六十七条　本法所称淫秽物品，是指具体描绘性行为或者露骨宣扬色情的淫秽性的书刊、影片、录像带、录音带、图片及其他淫秽物品。有关人体生理、医学知识的科学著作不是淫秽物品。包含有色情内容的有艺术价值的文学、艺术作品不视为淫秽物品。

附录 2　全国人民代表大会常务委员会关于维护互联网安全的决定

（2000 年 12 月 28 日第九届全国人民代表大会常务委员会第十九次会议通过）

我国的互联网，在国家大力倡导和积极推动下，在经济建设和各项事业中得到日益广泛的应用，使人们的生产、工作、学习和生活方式已经开始并将继续发生深刻的变化，对于加快我国国民经济、科学技术的发展和社会服务信息化进程具有重要作用。同时，如何保障互联网的运行安全和信息安全问题已经引起全社会的普遍关注。为了兴利除弊，促进我国互联网的健康发展，维护国家安全和社会公共利益，保护个人、法人和其他组织的合法权益，特作如下决定：

一、为了保障互联网的运行安全，对有下列行为之一，构成犯罪的，依照刑法有关规定追究刑事责任：

（一）侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统；

（二）故意制作、传播计算机病毒等破坏性程序，攻击计算机系统及通信网络，致使计算机系统及通信网络遭受损害；

（三）违反国家规定，擅自中断计算机网络或者通信服务，造成计算机网络或者通信系统不能正常运行。

二、为了维护国家安全和社会稳定，对有下列行为之一，构成犯罪的，依照刑法有关规定追究刑事责任：

（一）利用互联网造谣、诽谤或者发表、传播其他有害信息，煽动颠覆国家政权、推翻社会主义制度，或者煽动分裂国家、破坏国家统一；

（二）通过互联网窃取、泄露国家秘密、情报或者军事秘密；

（三）利用互联网煽动民族仇恨、民族歧视，破坏民族团结；

（四）利用互联网组织邪教组织、联络邪教组织成员，破坏国家法律、行政法规实施。

三、为了维护社会主义市场经济秩序和社会管理秩序，对有下列行为之一，构成犯罪的，依照刑法有关规定追究刑事责任：

（一）利用互联网销售伪劣产品或者对商品、服务作虚假宣传；

（二）利用互联网损害他人商业信誉和商品声誉；

（三）利用互联网侵犯他人知识产权；

（四）利用互联网编造并传播影响证券、期货交易或者其他扰乱金融秩序的虚假信息；

（五）在互联网上建立淫秽网站、网页，提供淫秽站点链接服务，或者传播淫秽书刊、影片、音像、图片。

四、为了保护个人、法人和其他组织的人身、财产等合法权利，对有下列行为之一，构成犯罪的，依照刑法有关规定追究刑事责任：

（一）利用互联网侮辱他人或者捏造事实诽谤他人；

（二）非法截获、篡改、删除他人电子邮件或者其他数据资料，侵犯公民通信自由和通信秘密；

（三）利用互联网进行盗窃、诈骗、敲诈勒索。

五、利用互联网实施本决定第一条、第二条、第三条、第四条所列行为以外的其他行为，构成犯罪的，依照刑法有关规定追究刑事责任。

六、利用互联网实施违法行为，违反社会治安管理，尚不构成犯罪的，由公安机关依照《治安管理处罚条例》予以处罚；违反其他法律、行政法规，尚不构成犯罪的，由有关行政管理部门依法给予行政处罚；对直接负责的主管人员和其他直接责任人员，依法给予行政处分或者纪律处分。

利用互联网侵犯他人合法权益，构成民事侵权的，依法承担民事责任。

七、各级人民政府及有关部门要采取积极措施，在促进互联网的应用和网络技术的普及

过程中，重视和支持对网络安全技术的研究和开发，增强网络的安全防护能力。有关主管部门要加强对互联网的运行安全和信息安全的宣传教育，依法实施有效的监督管理，防范和制止利用互联网进行的各种违法活动，为互联网的健康发展创造良好的社会环境。从事互联网业务的单位要依法开展活动，发现互联网上出现违法犯罪行为和有害信息时，要采取措施，停止传输有害信息，并及时向有关机关报告。任何单位和个人在利用互联网时，都要遵纪守法，抵制各种违法犯罪行为和有害信息。人民法院、人民检察院、公安机关、国家安全机关要各司其职，密切配合，依法严厉打击利用互联网实施的各种犯罪活动。要动员全社会的力量，依靠全社会的共同努力，保障互联网的运行安全与信息安全，促进社会主义精神文明和物质文明建设。

附录 3　计算机信息网络国际联网安全保护管理办法

（1997 年 12 月 11 日国务院批准，1997 年 12 月 30 日公安部发布）

第一章　总　则

第一条　为了加强对计算机信息网络国际联网的安全保护，维护公共秩序和社会稳定，根据《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》和其他法律、行政法规的规定，制定本办法。

第二条　中华人民共和国境内的计算机信息网络国际联网安全保护管理，适用本办法。

第三条　公安部计算机管理监察机构负责计算机信息网络国际联网的安全保护管理工作。

公安机关计算机管理监察机构应当保护计算机信息网络国际联网的公共安全，维护从事国际联网业务的单位和个人的合法权益和公众利益。

第四条　任何单位和个人不得利用国际联网危害国家安全、泄露国家秘密，不得侵犯国家的、社会的、集体的利益和公民的合法权益，不得从事违法犯罪活动。

第五条　任何单位和个人不得利用国际联网制作、复制、查阅和传播下列信息：

（一）煽动抗拒、破坏宪法和法律、行政法规实施的；

（二）煽动颠覆国家政权、推翻社会主义制度的；

（三）煽动分裂国家、破坏国家统一的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）捏造或者歪曲事实，散布谣言，扰乱社会秩序的；

（六）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；

（七）公然侮辱他人或者捏造事实诽谤他人的；

（八）损害国家机关信誉的；

（九）其他违反《宪法》和法律、行政法规的。

第六条　任何单位和个人不得从事下列危害计算机信息网络安全的活动：

（一）未经允许，进入计算机信息网络或者使用计算机信息网络资源的；

（二）未经允许，对计算机信息网络功能进行删除、修改或者增加的；

（三）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；

（四）故意制作、传播计算机病毒等破坏性程序的；

（五）其他危害计算机信息网络安全的。

第七条　用户的通信自由和通信秘密受法律保护。任何单位和个人不得违反法律规定，利用国际联网侵犯用户的通信自由和通信秘密。

第二章　安全保护责任

第八条　从事国际联网业务的单位和个人应当接受公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

第九条　国际出入口信道提供单位、互联单位的主管部门或者主管单位，应当依照法律和国家有关规定负责国际出入口信道、所属互联网络的安全保护管理工作。

第十条　互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应当履行下列安全保护职责：

（一）负责本网络的安全保护管理工作，建立健全安全保护管理制度；

（二）落实安全保护技术措施，保障本网络的运行安全和信息安全；

（三）负责对本网络用户的安全教育和培训；

（四）对委托发布信息的单位和个人进行登记，并对所提供的信息内容按照本办法第五条进行审核；

（五）建立计算机信息网络电子公告系统的用户登记和信息管理制度；

（六）发现有本办法第四条、第五条、第六条、第七条所列情形之一的，应当保留有关原始记录，并在二十四小时内向当地公安机关报告；

（七）按照国家有关规定，删除本网络中含有本办法第五条内容的地址、目录或者关闭服务器。

第十一条　用户在接人单位办理入网手续时，应当填写用户备案表。备案表由公安部监制。

第十二条　互联单位、接入单位、使用计算机信息网络国际联网的法人和其他组织（包括跨省、自治区、直辖市联网的单位和所属的分支机构），应当自网络正式联通之日起三十日内，到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。

前款所列单位应当负责将接入本网络的接入单位和用户情况报当地公安机关备案，并及

时报告本网络中接入单位和用户的变更情况。

第十三条　使用公用账号的注册者应当加强对公用账号的管理，建立账号使用登记制度。用户账号不得转借、转让。

第十四条　涉及国家事务、经济建设、国防建设、尖端科学技术等重要领域的单位办理备案手续时，应当出具其行政主管部门的审批证明。

前款所列单位的计算机信息网络与国际联网，应当采取相应的安全保护措施。

第三章　安全监督

第十五条　省、自治区、直辖市公安厅（局），地（市）、县（市）公安局，应当有相应机构负责国际联网的安全保护管理工作。

第十六条　公安机关计算机管理监察机构应当掌握互联单位、接入单位和用户的备案情况，建立备案档案，进行备案统计，并按照国家有关规定逐级上报。

第十七条　公安机关计算机管理监察机构应当督促互联单位、接入单位及有关用户建立健全安全保护管理制度。监督、检查网络安全保护管理以及技术措施的落实情况。

公安机关计算机管理监察机构在组织安全检查时，有关单位应当派人参加。公安机关计算机管理监察机构对安全检查发现的问题，应当提出改进意见，作出详细记录，存档备查。

第十八条　公安机关计算机管理监察机构发现含有本办法第五条所列内容的地址、目录或者服务器时，应当通知有关单位关闭或者删除。

第十九条　公安机关计算机管理监察机构应当负责追踪和查处通过计算机信息网络的违法行为和针对计算机信息网络的犯罪案件，对违反本办法第四条、第七条规定的违法犯罪行为，应当按照国家有关规定移送有关部门或者司法机关处理。

第四章　法律责任

第二十条　违反法律、行政法规，有本办法第五条、第六条所列行为之一的，由公安机关给予警告，有违法所得的，没收违法所得，对个人可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，并可以给予六个月以内停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格；构成违反治安管理行为的，依照《治安管理处罚条例》的规定处罚；构成犯罪的，依法追究刑事责任。

第二十一条　有下列行为之一的，由公安机关责令限期改正，给予警告，有违法所得的，没收违法所得；在规定的限期内未改正的，对单位的主管负责人员和其他直接责任人员可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，并可以给予六个月以内的停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格。

（一）未建立安全保护管理制度的；

（二）未采取安全技术保护措施的；

（三）未对网络用户进行安全教育和培训的；

（四）未提供安全保护管理所需信息、资料及数据文件，或者所提供内容不真实的；

（五）对委托其发布的信息内容未进行审核或者对委托单位和个人未进行登记的；

（六）未建立电子公告系统的用户登记和信息管理制度的；

（七）未按照国家有关规定，删除网络地址、目录或者关闭服务器的；

（八）未建立公用账号使用登记制度的；

（九）转借、转让用户账号的。

第二十二条　违反本办法第四条、第七条规定的，依照有关法律、法规予以处罚。

第二十三条　违反本办法第十一条、第十二条规定，不履行备案职责的，由公安机关给予警告或者停机整顿不超过六个月的处罚。

第五章　附　则

第二十四条　与香港特别行政区和台湾、澳门地区联网的计算机信息网络的安全保护管理，参照本办法执行。

第二十五条　本办法自发布之日起施行。

附录 4　《互联网信息服务管理办法》节选

（2000 年 9 月 20 日国务院第 31 次常务会议通过，2000 年 9 月 25 日公布实施）

第一条　为了规范互联网信息服务活动，促进互联网信息服务健康有序发展，制定本办法。

第二条　在中华人民共和国境内从事互联网信息服务活动，必须遵守本办法。

本办法所称互联网信息服务，是指通过互联网向上网用户提供信息的服务活动。

第十五条　互联网信息服务提供者不得制作、复制、发布、传播含有下列内容的信息：

（一）反对宪法所确定的基本原则的；

（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

（三）损害国家荣誉和利益的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）破坏国家宗教政策，宣扬邪教和封建迷信的；

（六）散布谣言，扰乱社会秩序，破坏社会稳定的；

（七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

（八）侮辱或者诽谤他人，侵害他人合法权益的；

（九）含有法律、行政法规禁止的其他内容的。

第十六条　互联网信息服务提供者发现其网站传输的信息明显属于本办法第十五条所列内容之一的，应当立即停止传输，保存有关记录，并向国家有关机关报告。

第十七条　经营性互联网信息服务提供者申请在境内境外上市或者同外商合资、合作，应当事先经国务院信息产业主管部门审查同意；其中，外商投资的比例应当符合有关法律、行政法规的规定。

第十八条　国务院信息产业主管部门和省、自治区、直辖市电信管理机构，依法对互联网信息服务实施监督管理。

新闻、出版、教育、卫生、药品监督管理、工商行政管理和公安、国家安全等有关主管部门，在各自职责范围内依法对互联网信息内容实施监督管理。

第十九条　违反本办法的规定，未取得经营许可证，擅自从事经营性互联网信息服务，或者超出许可的项目提供服务的，由省、自治区、直辖市电信管理机构责令限期改正，有违法所得的，没收违法所得，处违法所得 3 倍以上 5 倍以下的罚款；没有违法所得或者违法所得不足 5 万元的，处 10 万元以上 100 万元以下的罚款；情节严重的，责令关闭网站。

违反本办法的规定，未履行备案手续，擅自从事非经营性互联网信息服务，或者超出备案的项目提供服务的，由省、自治区、直辖市电信管理机构责令限期改正；拒不改正的，责令关闭网站。

第二十条　制作、复制、发布、传播本办法第十五条所列内容之一的信息，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由公安机关、国家安全机关依照《中华人民共和国治安管理处罚条例》、《计算机信息网络国际联网安全保护管理办法》等有关法律、行政法规的规定予以处罚；对经营性互联网信息服务提供者，并由发证机关责令停业整顿直至吊销经营许可证，通知企业登记机关；对非经营性互联网信息服务提供者，并由备案机关责令暂时关闭网站直至关闭网站。

附录 5　中华人民共和国电子签名法

（2004 年 8 有 28 是第十届全国人民代表大会常务委员会第十一次会议通过）

2004 年 8 月 28 日，中华人民共和国第十届全国人民代表大会常务委员会第十一次会议通过了《中华人民共和国电子签名法》。作为我国电子商务领域的第一部法律，《电子签名法》的出台，第一次从法律上把数字化活动推到了实际操作的阶段，开启了中国电子商务立法的大门，它为解决司法实践中亟待回答的问题，扫清网络交易行为的障碍提供了立法保障，为互联网从单纯的媒体时代过渡到全面应用时代奠定了基础，并将进一步规范网上行为，净化网络环境，消除网络信用危机，保障用户的各项权利，为我国的网络立法与国际立法的接轨起到了示范性作用。

第一章　总　则

第一条　为了规范电子签名行为，确立电子签名的法律效力，维护有关各方的合法权益，制定本法。

第二条　本法所称电子签名，是指数据电文中以电子形式所含，所附用于识别签名人身份并表明签名人认可其中内容的数据。

本法所称数据电文，是指以电子、光学、磁或者类似手段生成、发送、接收或者储存的信息。

第三条　民事活动中的合同或者其他文件、单证等文书，当事人可以约定使用或者不使用电子签名、数据电文。

当事人约定使用电子签名、数据电文的文书，不得仅因为其采用电子签名、数据电文的形式而否定其法律效力。

前款规定不适用下列文书：

（一）涉及婚姻、收养、继承等人身关系的；

（二）涉及土地、房屋等不动产权益转让的；

（三）涉及停止供水、供热、供气、供电等公用事业服务的；

（四）法律、行政法规规定的不适用电子文书的其他情形。

第二章　数据电文

第四条　能够有形地表现所载内容，并可以随时调取查用的数据电文，视为符合法律、法规要求的书面形式。

第五条　符合下列条件的数据电文，视为满足法律、法规规定的原件形式要求：

（一）能够有效地表现所载内容并可供随时调取查用；

（二）能够可靠地保证自最终形成时起，内容保持完整、未被更改。但是，在数据电文上增加背书以及数据交换、储存和显示过程中发生的形式变化不影响数据电文的完整性。

第六条　符合下列条件的数据电文，视为满足法律法规规定的文件保存要求：

（一）能够有效地表现所载内容并可供随时调取查用；

（二）数据电文的格式与其生成，发送或者接收时的格式相同，或者格式不相同但是能够准确表现原来生成发送或者接收的内容；

（三）能够识别数据电文的发件人、收件人以及发送接收的时间。

第七条　数据电文不得仅因为其是以电子、光学、磁或者类似手段生成、发送、接收或者储存的而被拒绝作为证据使用。

第八条 审查数据电文作为证据的真实性，应当考虑以下因素：

（一）生成、储存或者传递数据电文方法的可靠性；

（二）保持内容完整性方法的可靠性；

（三）用以鉴别发件人方法的可靠性；

（四）其他相关因素。

第九条　数据电文有下列情形之一的，视为发件人发送：

（一）经发件人授权发送的；

（二）发件人的信息系统自动发送的；

（三）收件人按照发件人认可的方法对数据电文进行验证后结果相符的。

当事人对前款规定的事项另有约定的，从其约定。

第十条　法律、行政法规规定或者当事人约定数据电文需要确认收讫的，应当确认收讫。发件人收到收件人的收讫确认时，数据电文视为已经收到。

第十一条　数据电文进入发件人控制之外的某个信息系统的时间，视为该数据电文的发送时间。

收件人指定特定系统接收数据电文的，数据电文进入该特定系统的时间，视为该数据电文的接收时间；未指定特定系统的，数据电文进入收件人的任何系统的首次时间，视为该数据电文的接收时间。

当事人对数据电文的发送时间、接收时间另有约定的，从其约定。

第十二条　发件人的主营业地为数据电文的发送地点，收件人的主营业地为数据电文的接收地点。没有主营业地的，其经常居住地为发送或者接收地点。

当事人对数据电文的发送地点，接收地点另有约定的，从其约定。

第三章　电子签名与认证

第十三条　电子签名同时符合下列条件的，视为可靠的电子签名：

（一）电子签名制作数据用于电子签名时，属于电子签名人专有；

（二）签署时电子签名制作数据仅由电子签名人控制；

（三）签署后对电子签名的任何改动能够被发现；

（四）签署后对数据电文内容和形式的任何改动能够被发现。

当事人也可以选择使用符合其约定的可靠条件的电子签名。

第十四条　可靠的电子签名与手写签名或者盖章具有同等的法律效力。

第十五条　电子签名人应当妥善保管电子签名制作数据。电子签名人知悉电子签名制作数据已经失密或者可能已经失密时，应当及时告知有关各方，并终止使用该电子签名制作数据。

第十六条　电子签名需要第三方认证的，由依法设立的电子认证服务提供者提供认证服务。

第十七条　提供电子认证服务，应当具备下列条件：

（一）具有与提供电子认证服务相适应的专业技术人员和管理人员；

（二）具有与提供电子认证服务相适应的资金和经营场所；

（三）具有符合国家安全标准的技术和设备；

（四）具有国家密码管理机构同意使用密码的证明文件；

（五）法律、行政法规规定的其他条件。

第十八条　从事电子认证服务，应当向国务院信息产业主管部门提出申请，并提交符合本法第十七条规定条件的相关材料。国务院信息产业主管部门接到申请后经依法审查，征求国务院商务主管部门等有关部门的意见后，自接到申请之日起四十五日内作出许可或者不予许可的决定。予以许可的，颁发电子认证许可证书；不予许可的，应当书面通知申请人并告知理由。

申请人应当持电子认证许可证书依法向工商行政管理部门办理企业登记手续。

取得认证资格的电子认证服务提供者，应当按照国务院信息产业主管部门的规定在互联网上公布其名称、许可证号等信息。

第十九条　电子认证服务提供者应当制定、公布符合国家有关规定的电子认证业务规则，并向国务院信息产业主管部门备案。

电子认证业务规则应当包括责任范围、作业操作规范、信息安全保障措施等事项。

第二十条　电子签名人向电子认证服务提供者申请电子签名认证证书，应当提供真实、完整和准确的信息。

电子认证服务提供者收到电子签名认证证书申请后应当对申请人的身份进行查验，并对有关材料进行审查。

第二十一条　电子认证服务提供者签发的电子签名认证证书应当准确无误，并应当载明下列内容：

（一）电子认证服务提供者名称；

（二）证书持有人名称；

（三）证书序列号；

（四）证书有效期；

（五）证书持有人的电子签名验证数据；

（六）电子认证服务提供者的电子签名；

（七）国务院信息产业主管部门规定的其他内容。

第二十二条　电子认证服务提供者应当保证电子签名认证证书内容在有效期内完整、准确，并保证电子签名依赖方能够证实或者了解电子签名认证证书所载内容及其他有关事项。

第二十三条　电子认证服务提供者拟暂停或者终止电子认证服务的，应当在暂停或者终止服务九十日前，就业务承接及其他有关事项通知有关各方。

电子认证服务提供者拟暂停或者终止电子认证服务的，应当在暂停或者终止服务六十日前向国务院信息产业主管部门报告，并与其他电子认证服务提供者就业务承接进行协商，作出

妥善安排。

电子认证服务提供者未能就业务承接事项与其他电子认证服务提供者达成协议的，应当申请国务院信息产业主管部门安排其他电子认证服务提供者承接其业务。

电子认证服务提供者被依法吊销电子认证许可证书的，其业务承接事项的处理按照国务院信息产业主管部门的规定执行。

第二十四条　电子认证服务提供者应当妥善保存与认证相关的信息，信息保存期限至少为电子签名认证证书失效后五年。

第二十五条　国务院信息产业主管部门依照本法制定电子认证服务业的具体管理办法，对电子认证服务提供者依法实施监督管理。

第二十六条　经国务院信息产业主管部门根据有关协议或者对等原则核准后，中华人民共和国境外的电子认证服务提供者在境外签发的电子签名认证证书与依照本法设立的电子认证服务提供者签发的电子签名认证证书具有同等的法律效力。

第四章　法律责任

第二十七条　电子签名人知悉电子签名制作数据已经失密或者可 能已经失密未及时告知有关各方，并终止使用电子签名制作数据，未向电子认证服务提供者提供真实、完整和准确的信息，或者有其他过错，给电子签名依赖方、电子认证服务提供者造成损失的，承担赔偿责任。

第二十八条　电子签名人或者电子签名依赖方因依据电子认证服务提供者提供的电子签名认证服务从事民事活动遭受损失，电子认证服务提供者不能证明自己无过错的，承担赔偿责任。

第二十九条　未经许可提供电子认证服务的，由国务院信息产业主管部门责令停止违法行为；有违法所得的，没收违法所得，违法所得三十万元以上的，处违法所得一倍以上三倍以下的罚款；没有违法所得或者违法所得不中三十万元的，处十万元以上三十万元以下的罚款。

第三十条　电子认证服务提供者暂停或者终止电子认证服务，未在暂停或者终止服务六十日前向国务院信息产业主管部门报告的，由国务院信息产业主管部门对其直接负责的主管人员处一万元以上五万元以下的罚款。

第三十一条　电子认证服务提供者不遵守认证业务规则、未妥善保存与认证相关的信息，或者有其他违法行为的由国务院信息产业主管部门责令限期改正；逾期未改下正的，吊销电子认证许可证书，其直接负责的主管人员和其他直接责任人员十年内不得从事电子认证服务。吊销电子认证许可证书的，应当予以公告并通知工商行政管理部门。

第三十二条　伪造、冒用、盗用他人的电子签名，构成犯罪的，依法追究刑事责任；给他人造成损失的，依法承担民事责任。

第三十三条　依照本法负责电子认证服务业监督管理工作的部门的工作人中员，不依法

履行行政许可、监督管理职责的，依法给予行政处分；构成犯罪的，依法追究刑事责任。

第五章　附　则

第三十四条　本法中下列用语的含义：

（一）电子签名人，是指持有电子签名制作数据并以本人身份或者以其所代表的人的名义实施电子签名的人；

（二）电子签名依赖方，是指基于对电子签名认证证书或者电子签名的依赖从事有关活动的人；

（三）电子签名认证证书，是指可证实电子签名人与电子签名制作数据有联系的数据电文或者其他电子记录；

（四）电子签名制作数据，是指在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据；

（五）电子签名验证数据，是指用于验证电子签名的数据，包括代码、口令、算法或者公钥等。

第三十五条　国务院或者国务院规定的部门可以依据本法制定政务活动和其他社会活动中使用电子签名、数据电文的具体办法。

第三十六条　本法自 2005 年 4 月 1 日起施行。

附录 6　电子认证服务管理办法

中华人民共和国信息产业部令　第 35 号

《电子认证服务管理办法》已经 2005 年 1 月 28 日中华人民共和国信息产业部第十二次部务会议审议通过，现予发布，自 2005 年 4 月 1 日起施行。

部 长：王旭东

二〇〇五年二月八日

第一章　总　则

第一条　为了规范电子认证服务行为，对电子认证服务提供者实施监督管理，依照《中华人民共和国电子签名法》和其他法律、行政法规的规定，制定本办法。

第二条　本办法所称电子认证服务，是指为电子签名相关各方提供真实性、可靠性验证的公众服务活动。

本办法所称电子认证服务提供者，是指为电子签名人和电子签名依赖方提供电子认证服务的第三方机构（以下称为“电子认证服务机构”）。

第三条　在中华人民共和国境内设立电子认证服务机构和为电子签名提供电子认证服务，适用本办法。

第四条　中华人民共和国信息产业部（以下简称“信息产业部”）依法对电子认证服务机构和电子认证服务实施监督管理。

第二章　电子认证服务机构

第五条　电子认证服务机构，应当具备下列条件：

（一）具有独立的企业法人资格；

（二）从事电子认证服务的专业技术人员、运营管理人员、安全管理人员和客户服务人员不少于三十名；

（三）注册资金不低于人民币三千万元；

（四）具有固定的经营场所和满足电子认证服务要求的物理环境；

（五）具有符合国家有关安全标准的技术和设备；

（六）具有国家密码管理机构同意使用密码的证明文件；

（七）法律、行政法规规定的其他条件。

第六条　申请电子认证服务许可的，应当向信息产业部提交下列材料：

（一）书面申请；

（二）专业技术人员和管理人员证明；

（三）资金和经营场所证明；

（四）国家有关认证检测机构出具的技术设备、物理环境符合国家有关安全标准的凭证；

（五）国家密码管理机构同意使用密码的证明文件。

第七条　信息产业部对提交的申请材料进行形式审查，依法作出是否受理的决定。

第八条　信息产业部对决定受理的申请材料进行实质审查。需要对有关内容进行核实的，指派两名以上工作人员实地进行核查。

第九条　信息产业部对与申请人有关事项书面征求中华人民共和国商务部等有关部门的意见。

第十条　信息产业部自接到申请之日起四十五日内作出许可或者不予许可的书面决定。不予许可的，说明理由并书面通知申请人；准予许可的，颁发《电子认证服务许可证》，并公布下列信息：

（一）《电子认证服务许可证》编号；

（二）电子认证服务机构名称；

（三）发证机关和发证日期。

电子认证服务许可相关信息发生变更的，信息产业部应当及时公布。

《电子认证服务许可证》的有效期为五年。

第十一条　取得电子认证服务许可的，应当持《电子认证服务许可证》到工商行政管理机关办理相关手续。

第十二条　取得认证资格的电子认证服务机构，在提供电子认证服务之前，应当通过互联网公布下列信息：

（一）机构名称和法定代表人；

（二）机构住所和联系办法；

（三）《电子认证服务许可证》编号；

（四）发证机关和发证日期；

（五）《电子认证服务许可证》有效期的起止时间。

第十三条　电子认证服务机构在《电子认证服务许可证》的有效期内变更法人名称、住所、注册资本、法定代表人的，应自完成相关变更手续之日起五日内按照本办法第十二条的规定公布变更后的信息，并自公布之日起十五日内向信息产业部备案。

第十四条　《电子认证服务许可证》的有效期届满要求续展的，电子认证服务机构应在许可证有效期届满三十日前向信息产业部申请办理续展手续，并自办结之日起五日内按照本办法第十二条的规定公布相关信息。

第三章　电子认证服务

第十五条　电子认证服务机构应当按照信息产业部公布的《电子认证业务规则规范》的要求，制定本机构的电子认证业务规则，并在提供电子认证服务前予以公布，向信息产业部备案。

电子认证业务规则发生变更的，电子认证服务机构应当予以公布，并自公布之日起三十日内向信息产业部备案。

第十六条　电子认证服务机构应当按照公布的电子认证业务规则提供电子认证服务。

第十七条　电子认证服务机构应当保证提供下列服务：

（一）制作、签发、管理电子签名认证证书；

（二）确认签发的电子签名认证证书的真实性；

（三）提供电子签名认证证书目录信息查询服务；

（四）提供电子签名认证证书状态信息查询服务。

第十八条　电子认证服务机构应当履行下列义务：

（一）保证电子签名认证证书内容在有效期内完整、准确；

（二）保证电子签名依赖方能够证实或者了解电子签名认证证书所载内容及其他有关事项；

（三）妥善保存与电子认证服务相关的信息。

第十九条　电子认证服务机构应当建立完善的安全管理和内部审计制度，并接受信息产业部的监督管理。

第二十条　电子认证服务机构应当遵守国家的保密规定，建立完善的保密制度。

电子认证服务机构对电子签名人和电子签名依赖方的资料，负有保密的义务。

第二十一条　电子认证服务机构在受理电子签名认证证书申请前，应当向申请人告知下列事项：

（一）电子签名认证证书和电子签名的使用条件；

（二）服务收费的项目和标准；

（三）保存和使用证书持有人信息的权限和责任；

（四）电子认证服务机构的责任范围；

（五）证书持有人的责任范围；

（六）其他需要事先告知的事项。

第二十二条　电子认证服务机构受理电子签名认证申请后，应当与证书申请人签订合同，明确双方的权利义务。

第四章　电子认证服务的暂停、终止

第二十三条　电子认证服务机构在《电子认证服务许可证》的有效期内拟终止电子认证服务的，应在终止服务六十日前向信息产业部报告，同时向信息产业部申请办理证书注销手续，并持信息产业部的相关证明文件向工商行政管理机关申请办理注销登记或者变更登记。

第二十四条　电子认证服务机构拟暂停或者终止电子认证服务的，应在暂停或者终止电子认证服务九十日前，就业务承接及其他有关事项通知有关各方。

电子认证服务机构拟暂停或者终止电子认证服务的，应当在暂停或者终止电子认证服务六十日前向信息产业部报告，并与其他电子认证服务机构就业务承接进行协商，做出妥善安排。

第二十五条　电子认证服务机构拟暂停或者终止电子认证服务，未能就业务承接事项与其他电子认证服务机构达成协议的，应当申请信息产业部安排其他电子认证服务机构承接其业务。

第二十六条　电子认证服务机构被依法吊销电子认证服务许可的，其业务承接事项的处理按照信息产业部的规定进行。

第二十七条　电子认证服务机构有根据信息产业部的安排承接其他机构开展的电子认证服务业务的义务。

第五章　电子签名认证证书

第二十八条　电子签名认证证书应当准确载明下列内容：

（一）签发电子签名认证证书的电子认证服务机构名称；

（二）证书持有人名称；

（三）证书序列号；

（四）证书有效期；

（五）证书持有人的电子签名验证数据；

（六）电子认证服务机构的电子签名；

（七）信息产业部规定的其他内容。

第二十九条　有下列情况之一的，电子认证服务机构可以撤销其签发的电子签名认证证书：

（一）证书持有人申请撤销证书；

（二）证书持有人提供的信息不真实；

（三）证书持有人没有履行双方合同规定的义务；

（四）证书的安全性不能得到保证；

（五）法律、行政法规规定的其他情况。

第三十条　有下列情况之一的，电子认证服务机构应当对申请人提供的证明身份的有关材料进行查验，并对有关材料进行审查：

（一）申请人申请电子签名认证证书；

（二）证书持有人申请更新证书；

（三）证书持有人申请撤销证书。

第三十一条　电子认证服务机构更新或者撤销电子签名认证证书时，应当予以公告。

第六章　监督管理

第三十二条　信息产业部对电子认证服务机构进行年度检查并公布检查结果。

年度检查采取报告审查和现场核查相结合的方式。

第三十三条　取得电子认证服务许可的电子认证服务机构，在电子认证服务许可的有效期内不得降低其设立时所应具备的条件。

第三十四条　电子认证服务机构应当按照信息产业部信息统计的要求，按时和如实报送认证业务开展情况及有关资料。

第三十五条　电子认证服务机构应当对其从业人员进行岗位培训。

第三十六条　信息产业部根据监督管理工作的需要，可以委托有关省、自治区和直辖市的信息产业主管部门承担具体的监督管理事项。

第七章　罚　　则

第三十七条　电子认证服务机构向信息产业部隐瞒有关情况、提供虚假材料或者拒绝提供反映其活动的真实材料的，由信息产业部依据职权责令改正，并处警告或者五千元以上一万元以下罚款。

第三十八条　信息产业部和省、自治区和直辖市的信息产业主管部门的工作人员，不依法履行监督管理职责的，由信息产业部或者省、自治区和直辖市的信息产业主管部门依据职权视情节轻重，分别给予警告、记过、记大过、降级、撤职、开除的行政处分；构成犯罪的，依法追究刑事责任。

第三十九条　电子认证服务机构违反本办法第十六条、第二十七条的规定的，由信息产业部依据职权责令限期改正，并处警告或一万元以下的罚款，或者同时处以以上两种处罚。

第四十条　电子认证服务机构违反本办法第三十三条的规定的，由信息产业部依据职权责令限期改正，并处三万元以下罚款。

第八章　附　则

第四十一条　本办法施行前已从事电子认证服务的机构拟继续从事电子认证服务的，应在2005年9月30日前依照本办法取得电子认证服务许可；拟终止电子认证服务的，应当对终止业务的相关事项作出妥善安排。自2005年10月1日起，未取得电子认证服务许可的，不得继续从事电子认证服务。

第四十二条　经信息产业部根据有关协议或者对等原则核准后，中华人民共和国境外的电子认证服务机构在境外签发的电子签名认证证书与依照本办法设立的电子认证服务机构签发的电子签名认证证书具有同等的法律效力。

第四十三条　本办法自2005年4月1日起施行。

参考文献

1 (美)埃里克·詹奇．自组织宇宙观．曾国屏等译．北京:中国社会科学出版社，1992

2 曾国屏．自组织的自然观．北京：北京大学出版社,1996

3 (德)赫尔曼·哈肯．协同学．上海:上海译文出版社,1995

4 谢龙．现代哲学观念．北京：北京大学出版社，1990

5 李秀林，王于，李淮春．辩证唯物主义和历史唯物主义原理．北京：中国人民大学出版社，1995

6 韩民青．物质进化论的人本哲学．南宁:广西人民出版社,1994

7 谢龙．中西哲学与文化比较新论．北京：人民出版社，1995

8 吴彤．自组织方法学研究．北京：清华大学出版社，2001

9 张禾瑞．近世代数基础．上海：商务印书馆，1952

10 谭跃进,高世楫，周曼殊．系统学原理．长沙:国际科技大学出版社，1996

11 Michel Mouly，Marie－Bernadette Pautet. The GSM system fro Mobile Communications. Cell &Sys，1993

12 宋健．钱学森科学贡献暨学术思想研讨会论文集．北京:中国科学技术出版社，2001

13 张维明，邓芳，罗雪山，肖卫东．信息系统建模技术与应用．北京：电子工业出版社，1997

14 胡晓峰，吴玲达，李国辉等．多媒体系统原理与应用．北京：人民邮电出版社，1995

15 张贤达．现代信号处理．北京:清华大学出版社，2002

16 谢希仁．计算机网络(第二版)．北京：电子工业出版社，1999

17 钟义信．信息科学原理．北京：北京邮电大学出版社，1996

18 N. Wiener. Cybenetics and Scociety. MIT Press，1961

19 C. E. Shannon. The Bandwagon. IEEE trans. On Information Theory,1956,vol. 2,No. 2,p3

20 金德文，陈建亚,纪江．现代交换原理．北京:电子工业出版社，2000

21 徐端颐．高密度光盘数据存储．北京:清华大学出版社，2003.

22 何新贵，唐常杰，李霖，刘云生．特种数据库技术．北京:科学出版社,2000

23 张贤达,保铮．通信信号处理．北京:国防工业出版社，2000

24 李长坤，朱铁军．网络犯罪评析——从比较法的角度观察．网络安全技术与应用，2002，No. 11

25 李春华．计算机犯罪的法律防治措施．网络安全技术与应用，2002，No. 12

26 蔡谊，沈昌祥．安全操作系统发展现状及对策．信息安全与通信保密，2001，No. 7

27 赵战生．信息安全是信息化社会可持续发展之保障．计算机安全，2001，No. 3

28 刘建军，于阳．计算机犯罪的原因及其现场勘察．网络安全技术与应用，2002，No. 12

29 余产峰．数字证据及其取证技术．网络安全技术与应用，2002，No. 12

30 吕诚昭．信息安全保障体系研究．信息安全与通信保密，2001，No. 2

31 高庆狮．关于网络安全的一些看法．信息安全与通信保密，2001，No. 5

32 张建军．对信息安全观念的新思考．信息安全与通信保密，2001，No. 12

33 何德全．提高网络安全意识构建信息保障体系．信息安全与通信保密，2001，No. 1

34 徐光辉．随机服务理论．北京：科学出版社,1980

35 王红卫．建模与仿真．北京：科学出版社，2002
36 袁震东，洪源，林武忠，蒋鲁敏．数学建模．上海：华东师范大学出版社，1999
37 （前苏联）A. G. 亚历山大洛夫等．数学——它的内容、方法和意义（第三卷）．北京：科学出版社，1962
38 朱成喜．测度论基础．北京：科学出版社，1991
39 刘晨，张滨．黑客与网络安全．北京：航空工业出版社，1999
40 高文等．数字图书馆——原理与技术实现．北京：清华大学出版社，2000
41 吴秋新等．信息隐藏技术——隐写术与数字水印．北京：人民邮电出版社，2001
42 卿斯汉．密码学与计算机网络安全．北京：清华大学出版社，2001
43 中国信息安全产品测评认证中心．信息安全与法律法规．北京：人民邮电出版社，2003
44 罗森林．信息系统安全与对抗技术．北京：北京理工大学出版社，2005
45 熊华，郭世泽，吕慧勤等．网络安全取证与密罐．北京：人民邮电出版社，2003
46 常建平．网络安全与计算机犯罪．北京：中国人民公安大学出版社，2002
47 张越今．网络安全与计算机犯罪勘查技术学．北京：清华大学出版社，2003
48 （美）Bruce Schneier. Applied cryptography protocols algorithms and source code in C（Second edition）. John & Sons Inc.，1996
49 凌雨欣．网络安全技术与反黑客．北京：冶金工业出版社，2001
50 戴宗坤等．信息系统安全．金城出版社，2000
51 李海泉等．计算机系统安全技术．北京：人民邮电出版社，2001
52 杨义先等．网络信息安全与保密．北京：北京邮电大学出版社，1999