基础理论篇

该篇通过对军事信息安全概念、精神、属性、范畴、模型及其展望的论述，主要回答军事信息安全“是什么”、“做什么”的问题。

基础理论篇

第一章　军事信息安全概述

军事信息安全，是巩固国防、促进经济发展、确保国家繁荣、推动社会进步，以及提高人们的工作水平和生活质量的重要保证。解析军事信息安全的原理，必先诠释其概念内涵。

一、军事信息安全概念

（一）安 全

“安全”并没有一个统一的定义，但对该词有四种代表性的解释。如：

一是远离危险的状态或特性；

二是客观上不存在威胁，主观上不存在恐惧；

三是没有危险，平安的，不必害怕或焦虑；

四是为防范间谍活动或蓄意破坏、犯罪、攻击等而采取的措施。

这四种解释基本上涵盖了安全的本义。

（二）信 息 安 全

信息安全同样没有公认和统一的定义，也有众多之说，有代表性的解释是：

一是为了防止未经授权就对知识、事实、数据或能力进行使

用、滥用、修改或拒绝使用而采取的措施；

二是信息安全是对信息、系统以及使用、存储和传输信息的硬件的保护。

三是信息安全的含义是通过各种计算机、网络和密钥技术，保证在各种系统和网络中传输、交换和存储的信息的机密性、完整性和真实性。

（三）军事信息安全

“军事信息安全”的定义更是五花八门，不一而足。如：

军事信息安全，主要是指“秘密与关键信息产生、传输、存储过程中不被对方获悉或破坏，确保信息的可用性、保密性和完整性”。

军事信息安全，主要是指军事“信息不受威胁，即保证信息的完整性、可用性、机密性、可靠性和真实性，保证采集信息、传输信息、处理信息、存取信息和使用信息的安全”。

军事信息安全，主要是指军事“信息系统的软、硬件资源受到破坏、信息失泄（窃）或遭受攻击而采取物理的、逻辑的，以及行为管理的方法与措施，以保证信息系统可靠运行与数据存储、处理的安全”。

以上，罗列了“安全”、“信息安全”、“军事信息安全”的有关定义，从这些含义中可以看出，不管是宏观的还是微观的信息安全定义，都是从各自业务系统的角度，从不同的层面上来论述信息安全的。但共性的含义有两点：一是强调信息系统的整体保护。即确保信息处理系统安全、可靠与不间断地运行，为信息系统的所有用户提供有效的服务；二是强调信息系统的信息保护，即确保信息系统中的信息免遭泄露、破坏或篡改，为系统中的各信息提供应有的保护。

为此，军事信息安全就是保障军事信息、系统与机构免遭威胁与侵害，而在分析风险的基础上，制定安全策略，进行主动防

护、深透检测、安防认证、动态响应与灾难恢复等行为过程。

该定义反映出：为抵抗军事信息系统因人为失误、恶意破坏以及各种自然灾害所造成军事系统和机构正常业务中断的能力。

二、军事信息安全属性

（一）军事信息安全是一个相对抽象的概念

军事信息安全，就是关注军事信息本身的安全，而不管应用计算机或什么处理手段，也不是要求达到的绝对量。军事信息安全的任务是保护军事信息资源，以防止偶然的或未授权者恶意泄露、修改或破坏军事信息，从而导致军事信息可靠性差或无法处理。因为这种偶然性或恶意行为的不确定性，使军事组织利用军事信息无法保障不招致损失，而只求损失最小。再则，因为各军事信息系统处在不同层次、担负不同工作、执行不同任务（战斗）的信息系统，其安全要求、标准与指数也不尽相同，所以说军事信息安全只是一个相对而抽象概念。

（二）军事信息安全是个相当广泛的领域

军事信息安全所涉及的领域相当广泛。从技术角度上看，军事信息安全研究的内容主要包括通信安全、计算机安全、操作安全、资源保护和实体安全等；从通信专业来看，包括移动通信安全、数据通信安全、卫星通信安全、网络（计算机网络、多媒体网络和智能化网络）安全等；从信息系统的设备上看，包括质量可靠、性能先进和物理安全等；从管理层次上看，包括人员可信、协议完善，规章制度健全等。

（三）军事信息安全是一个不断更新完善的过程

军事信息安全的静态含义，是创建计算机系统、数据处理系统等军事信息系统时所采取的技术以及管理的保护措施，防止造成军事信息系统的硬件、软件和数据有意无意泄露、破坏、丢失

等问题的发生。

军事信息安全的动态含义，是军事信息系统能连续正常工作。军事信息系统在规划、设计和运行的过程中，安全只是相对的，不安全因素则是绝对的。另外，对原有不安全因素的排除，并不等于遏制了新的不安全因素的出现，也可能刺激了新的不安全因素的产生。所以，在新军事变革的今天，信息对抗愈演愈烈，军事信息安全的周期越来越短，更新——完善——再更新——再完善，由此周而复始才是军事信息安全的真正要义。

三、军事信息安全特征

研究军事信息安全的目的就是保护军事信息资源免受威胁与侵害。根据国际标准化组织（ISO）的定义，以及部分国家政府有关信息安全的规定和专家学者的观点，军事信息安全的内在属性就是实现保密性、完整性、可用性、可控性、占用性和可信性等“六性”安全。

（一）保密性

信息保密性是指静态军事信息防止未授权访问和动态军事信息防止非法截取、解密与利用。

军事信息的保密性是确保拥有权限和特权的人才允许其访问，而那些未获授权的人则被禁止访问的特性。为此，应根据不同的数据类型和应用需求，对具体数据和用户进行分类，并配置不同的访问模式，以此保护静态军事信息的安全。

由于军事系统无法以确认是有未授权用户窃听网上数据，若随保障动态（传输中）信息的安全，应采取数据加密技术来实现这一目标。因加密后的军事信息能保证在传输、转换和使用过程中不被未授权者非法获取与使用。同时，也限制了非法用户对军事信息的访问，从而维护了军事信息的保密性。

（二）完整性

军事信息完整性是指军事信息在存储、传输过程中未被腐蚀、毁损、篡改、丢失的特性。信息的完整性是军事信息的基础。该特性的目的，就是保证军事信息系统上的数据处于一种完整和未受损的状态，也不会因有意或无意的事件而改变或丢失其系统中的信息。

许多计算机病毒的创建都有侵蚀数据的功能。为此，可采用检测病毒，观察文件大小的改动情况来判断文件的完整性。采用散列函数，更是确保信息完整性的极好方法。散列函数也被译为杂凑函数、哈希函数。通常表示为：函数 h＝H（M），其输入 M 为任意长度的消息，输出 h 为长度固定的消息摘要。

当然，一个文件受损并不总是来自黑客、病毒等原因，传输媒体中的噪音也能引起数据失真。一个低功率的信号，可使接收系统记录下不精确的数据。这可通过冗余位与校验位来弥补对军事信息完整所构成的威胁。同时，在数字传输过程中，加密算法、散列函数以及纠错码都可以保障信息的完整性。

（三）可用性

军事信息可用性是指可被合法用户访问并按其需求使用的特性。该特性能保证授权者按自己的需要而存取信息，任何攻击者都不能占用所有的信息资源而妨碍授权者的访问。在网络环境下，拒绝服务、干涉、阻碍与破坏网络及有关系统的正常运行都是对可用性的攻击行为。

可用性并不针对任何用户而是针对合法用户的。信息可用性应对用户进行鉴别技术验证，确认身份后才决定是否提供访问服务。为保证军事系统和网络提供正常的访问服务，应该进行必要的备份和冗余的配置。

备份的安全位置可以是现场的防火隔间，通常是采取远程地点安放的安全措施。所以，备份可以提供信息的可用性，但不一

定能够提供及时的可用性。冗余系统可以位于现场中，以便随时解决主要系统出现的故障。

（四）可控性

军事信息可控性是指对军事信息内容、流向及行为方式具有控制能力的特性。美国政府提供并采用的“密钥托管”、“密钥恢复”等方式方法，就是实现信息安全可控性的例子。

为保证军事信息可控性，首先，军事系统能够控制访问系统或网络上数据的用户，以及访问权限（是只读还是可以修改等），一般通过访问控制列表等方法实现。其次，需要对网络上的用户经过握手协议和鉴别进行身份验证。最后，应将用户的所有活动记录下来便于查询审计。

（五）占有性

军事信息占有性是指对军事信息资源具有所有权或控制权的独享性。即用户获得信息，则称信息为其所有。若存储军事信息的磁盘、光盘等信息载体被盗用，传输信息的呼号、频率、通信代码等资源被窃取，这都将造成丧失信息占有权的威胁。

保护军事信息占有性的方法很多，一般是提供物理和逻辑的存取控制方法；维护和检查有关文件访问的审记记录，使用标示与签名；严格通信纪律与管理等。

（六）责任性

军事信息责任性是指信息的行为人要对自己的信息行为负责任。责任性要求信息行为人不能抵赖自己曾有过发送信息的行为，也不能否认曾经接收过他人的信息事实。

责任性往往被人们忽略，其主要原因是：责任性安全服务本身不提供针对攻击的保护，没有刺激性；它增加了复杂程度，但没有提高价值；它还必须与数字签名和公证机制等一同使用，才能识别和认证用户执行与访问的合法性。由此，责任性增加了投资和降低了系统的可用性。但如果无责任性服务，那么保密性和

完整性机制就无法发挥作用。

四、军事信息安全范畴

由于信息网络的开放性、互联性和多样化等特征，致使军事信息网络易受间谍、黑客、病毒程序和不轨行为的攻击，所以军事信息的安全是个至关重要的问题。无论是军事信息机构中的单机还是站点，军事网还是因特网的系统中，都存在着人为的与自然的等诸多因素的脆弱性和潜在威胁。为此，应在物理、通信、辐射、计算机、网络和数据等方面，实施全方位的保护措施，才能确保军事网络信息及系统的安全。主要体现在：

(一)物理安全

早先，所有的财产都是物理的，信息也是物理的。信息都是刻在石头上、竹简上，或写印在布帛上、纸张上。但重要的、关键的信息，都是以“永久”的形式保留着。再则，为了保护这些物理资源，利用箱柜、房屋、城池、护城河等物理安全措施。另外，如果传递这些重要而关键的秘密信息，一般由信任的使者来完成。军事信息安全的物理防护亦如此。

军事信息物理安全除设备本身的问题外，还包括设备的位置安全、物理环境和地域安全因素等。

物理设备的位置安全。所有军事信息设施都应该放置在一个物理上安全的地点，严格限制来访人员，以杜绝未经授权而对军事信息系统主要设施所在地的访问。同时，并注意冗余备份。

物理的环境安全。军事信息系统选置应避开地震环、雷击区、火山体外，还应避开山体滑坡的高发区。同时，应做好温度、湿度、灰尘、供电系统的环境防护工作，以免自然灾害对军事信息系统造成破坏等。

物理的地域安全。不要说因特网络跨越洲际、国际的地理环

境，就是我军的军事网络也是跨越城际、县际和省（市、自治区）际，其地理位置错综复杂，通信线路质量难以保证，一方面会给通信线路上传输的军事信息造成损坏、丢失等不必要的灾害外，还会给那些“搭线窃听”的间谍、黑客和不法分子以可乘之机，增添更多的失、泄密隐患。

（二）通信安全

通信安全既是一个古老问题又是一个新兴问题。自从有战争以来，军事通信就一直受到高度重视，并在战争中扮演着十分重要的角色。古往今来，经过无数次的战争实践，军事家们得出了机密、及时、准确和不间断这一军事通信的四原则。从中不难看出，没有安全措施的军事通信，无疑是向敌人“通风报信”。故信息数据加密技术被广泛应用。

随着计算机网络事业的发展，过去相对封闭的军事通信网络正在迅速地与开放的公共网络融合，过去相对封闭的军事通信终端正在转变为智能型的开放式终端。如电话机、传真机等。

1. 电话通信安全

电信固定网（PSTN）就是传统的电话网。截止 2002 年 5 月底，我国固定电话用户数为 2 亿户；互联网用户 4580 万。电脑电话、智能电话迅速进入市场，加之这些电话广泛地使用嵌入式操作系统等先进技术，已具备了计算机操作的基本特征。这种计算机技术在电话业务中的应用是一柄双刃剑，在使得电话功能获得革命性变化的同时，也使计算机领域存在的安全危险步入电信固定网。这无疑危及军事网络系统的安全。

2. 移动通信安全

移动通信作为世界性的通信系统，它不仅能适应信息社会发展的要求，而且能够满足军事通信的特殊要求。因此，在移动通信系统中如何保证军事信息的安全性已成为迫切而重要的课题。

根据移动通信系统安全威胁的位置可分为：一是无线链路威

胁。即终端设备与服务网之间的无线接口可能受到非授权访问、拒绝服务攻击和对完整性的威胁。二是服务网络威胁。即非授权访问数据、对完整性的威胁、拒绝服务攻击、否认和非授权访问服务等。三是终端威胁。即攻击者利用窃取的终端设备访问、修改、删除和插入系统资源与数据，获取更多的访问权限及破坏终端数据的完整性等。

3. 电子邮件安全

电子邮件服务是互联网上一种最为流行的信息服务方式。用户通过电子邮件可以方便、快捷地与其他用户通信，包括简单的电子文件和信函的传输等。但是，我们一定要清醒地认识到，网络上的电子邮件都是明文传输的，这对于需要机密、及时、准确和不间断的军事通信来说，必须引起足够的重视，开展研究，以利军事邮件的安全性得到保证。

（三）辐射安全

只要加密方法科学先进，并在使用加密系统时不犯错误，秘密信息就很难破解。但随着科学技术的发展，在 20 世纪 50 年代，人们认识到所有电子系统都会产生电子辐射。就是加密器和电传打印机上加密过的消息，一旦经过电话线上发送，人们经过检查电话线上的电信号，也可获得代表原始消息的电子信号，并使用先进的设备就可将消息还原。如图 1—1 所示。

自 1831 年法拉第发现电磁感应现象，总结出电磁感应定律以来，特别是在第二次世界大战中，电磁兼容理论进一步发展，逐步形成一门独立的学科。现在，信息泄漏防护技术（Tempest 技术）已经成熟。 它包括泄漏信息的分析预 测、接收、识别、复原、防护、测试、安全评估等项技术，涉及到众多个学科领域。

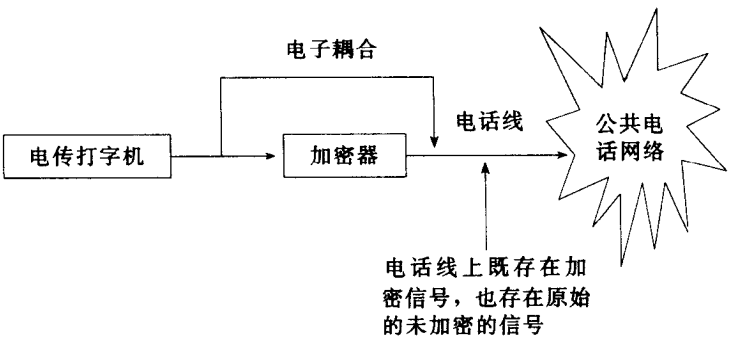

图1—1　电子信号绕过加密系统

在不泄漏有用电频信号的基础上，一般应保护好显示器的视频信号、打印机打印头的驱动信号、磁头读／写信号、键盘输入信号及信号线上的输入／输出信号等。具体的防护电磁泄漏措施，其他章节里还要详叙，在此就不叙述了。

（四）计算机安全

计算机安全，即是指计算机硬件与软件的防护问题，以及组成容错计算机系统。计算机系统，分为硬件系统和软件系统两部分，即人们常讲的计算机硬件和软件。

1. 硬件安全

硬件是计算机系统的基础。计算机硬件的安全，一般是指对全机、显示器、软盘、软驱、打印机、扫描仪、硬盘的防护措施或增加硬件来防护。如计算机加 锁，加专 的信息卡（如防病毒卡、防拷贝卡），加插座式的数据变换硬件（如在并行接口上加密等），输入／输出通道控制，以及对内存单元进行保护等。

随着科学技术的发展，计算机更新换代也越来越快。由于硬件安全防护的价格昂贵，且不易随计算机设备的更新而换代。为

此，许多计算机安全保护功能是由软件实现的。软件保护措施灵活，但它占用内存资源多，并且还会影响计算机运行的性能，同时，软件的一些保护手段（如磁盘程序加密）易被破译，故在软件保护的基础上，再增强硬件防护措施才能确保安全。

2. 软件安全

软件是指程序、数据及其相关文档的完整集合。硬件是躯体，软件是支配计算机硬件进行工作的“灵魂”。

软件安全就是采用技术和管理等手段，保障计算机软件、数据不因偶然或恶意的原因而遭破坏、更改、显露、盗版、非法复制及正常运行的安全措施。其具体内容是：

一是软件自身安全。防止软件丢失、被破坏、被篡改、被伪造，其核心要保证软件的完整性。即保证操作系统、数据库管理软件、网络软件、应用软件及相关资料的完整。

同时，因软件和数据可以存放在一张软盘上，所以必须采取严格的防范措施，以确保计算机软件不被偷窃，不会丢失。

二是软件存储安全。保证计算机软件的可靠存储，即保密存储、压缩存储和备份存储。

三是软件通信安全。软件通信安全是指软件的安全传输、加密传输、网络安全下载等。包括输入／输出、识别用户、审计等。

四是软件使用安全。软件使用安全主要是合法使用的问题，即防止软件被窃取、被非法复制和滥用。

五是软件运行安全。软件运行安全就是确保软件运行功能正常。包括电源、环境、机房与运行管理等。

3. 容错计算机

容错计算机系统是由故障检测、隔离、恢复和动态冗余切换等模块组成，其目的是为了数字化信息存储在计算机并通过网络传输中的安全。

容错计算机的基本特点是：预知故障、保证数据的完整性、数

据备份与恢复等。即当出现操作错误和电源掉电等之类的故障时，容错计算机系统能及时发现、迅速补救，保护与恢复文件数据，并保障其正常运行等。

（五）网络安全

网络安全就是对军事网络系统的硬件、软件及其系统中的数据实施保护，以确保军事网络系统正常运行。即要求军事网络应保证其信息系统资源的完整性、准确性和向所有合法用户提供各自应得到的服务。其具体内容包括：

一是逻辑安全。防止网络计算机的黑客入侵，主要是依赖计算机的逻辑安全。为了计算机上的军事信息数据的安全，通常是将各计算机隔离，严格控制所有高度机密数据的存取。同时，有些安全软件包可以跟踪可疑、未授权的存取企图。如限制试登录的次数或对试登录操作加上时间限制，试登录次数或时间超出，系统就自动退出，使非法用户难以进入军事网络的计算机。

二是操作系统安全。操作系统是计算机的核心，它控制计算机系统的资源。虽然通用的 UNIX 等操作系统，都具有一定程度的访问控制、安全内核和系统设计等安全功能。但从国家安全、军事安全的角度考虑，应独立开发使用我国我军自己的安全操作系统。依靠别国公司开发研制的操作系统，都存在着潜在的、陷阱门式的威胁。

三是联网安全。联网安全性，主要通过访问控制服务、通信安全服务两个方面来体现。即用来保护军用计算机和网络资源不被非授权使用和认证军事数据的保密性、完整性和可信性的各种军事通信。

除此之外，还应实现物理安全和进行保密教育等。

（六）信息安全

军事信息安全就是物理安全、通信安全、辐射安全、计算机安全和网络安全所组成。有的专家学者还把物理安全、通信安全、

辐射安全、计算机安全、网络安全和信息安全作为安全性简史的发展六个阶段来看待。如图 1—2 所示。

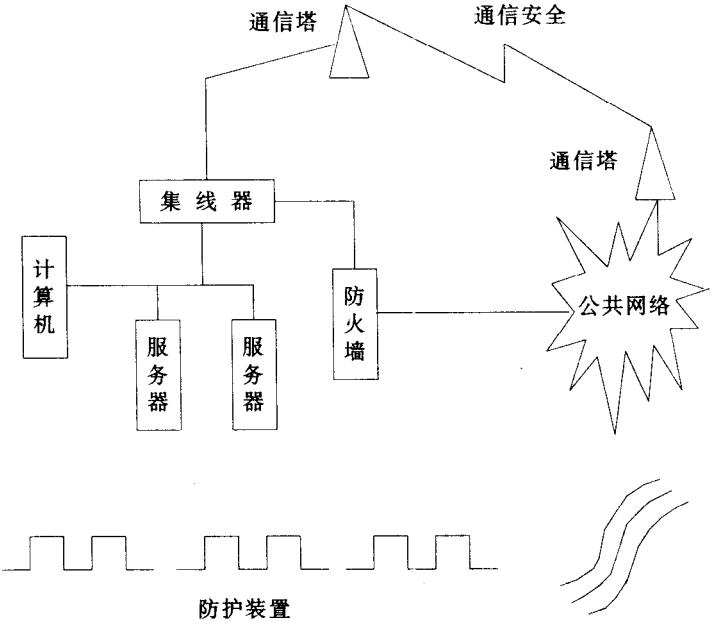

图1—2　军事信息安全总体概示

总之，物理安全，是保护实体资产安全的必须手段；通信安全，是保护传输中信息安全的必须手段；辐射安全，是防止敌人读取计算机系统电子辐射信号的必须手段；计算机安全，是控制合法访问和抵制非法访问的必须手段；而网络安全，是控制各级军事领域网络安全的必须手段。这些防护概念的综合体，就构成了军事信息安全的框架。

五、军事信息安全模型

军事信息安全不仅是防护技术，还是动态的循环过程。单纯地强调信息安全防护技术，就会导致军事信息系统的盲目建设，这不仅造成安全设备投入过大，反而没有真正抓住安全的关键环节。军事信息安全涉及到安全技术、管理控制和法规支撑等诸方面的工作，是一个动态的系统保护与防御体系。

信息安全保障体系模型的研究一直在不断地发展与完善中，现今还在继续进行。综合国内外专家学者的论述，军事信息安全保障模型应由风险分析、保障策略、主动防护、深透检测、安防认证、动态响应和灾难恢复等七个环节组成。这七个环节，也就是军事信息安全的七大原理。如图 1—3 所示。

现将军事信息安全保障模型的基本内涵简述如下。

（一）风险分析

风险分析是军事信息安全的起点，亦是制定安全策略的基础。风险分析主要是回答军事信息安全工作“为什么”的问题。即通过风险分析，认清军事信息安全的严峻性、紧迫性和目的性。

（二）保障策略

它为军事信息系统的安全保障提供指导性策略。根据风险分析而制定的安全策略是军事系统安全的核心，所有的军事信息系统的防护、检测、认证、响应与恢复都是依据安全策略实施的。

（三）主动防护

主动防护环节的主要功能，就是主动、自觉地做好一切军事系统的安全防护工作。防护可分三大类：军事信息系统物理安全防护、网络安全防护和数据信息安全防护。主动采用数据加密、防火墙、访问控制等技术功能，做好物理安全、通信安全、软件安全、网络安全。

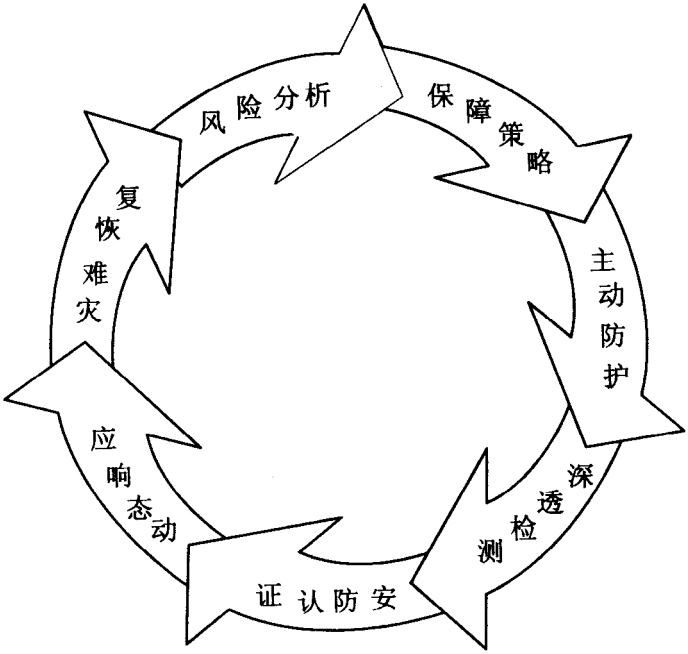

图 1—3　军事信息安全的循环过程模型

(四)深透检测

深透检测是主动防护和动态响应的依据。该系统的主要功能即是检测军事信息系统的安全防护程度。通过采用基于物理的渗透性检测和基于网络的入侵检测系统、电磁过滤等手段来发现外部威胁和军事系统存在的安全隐患。

(五)安防认证

安防认证环节的主要功能即是测评认证军事信息系统安全防