

国防信息安全战略

第一编 国防信息安全总论

国防信息安全 是一个国家在政治、经济、军事、外交斗争中取得胜利的重要保证。国防信息安全与国防、军队的安全息息相关。在新的历史时期，尤其是随着信息技术的飞速发展和在军事领域的广泛运用，国防信息安全面临的威胁日益加剧。认真研究新形势下国防信息安全面临的挑战，采取相应的对策努力做好国防信息安全工作，对于维护国家的安全与利益有着深远的历史意义和重要的现实意义。

第一章 国防信息

国防信息，是指为国家防务进行的军事及与军事有关的政治、经济、外交、科技、教育等方面活动的直接或间接的表述。在信息时代，国防信息既是一种直接的战斗力，又是战斗力的倍增器，已成为一种重要的战略资源。国防信息通过操纵和控制战争中的物质资源和能量资源，可以大大提高军队作战效能并减少其它战斗力要素的投入。因此，信息资源在国防建设中的巨大作用，将使未来战争的形态和样式发生深刻变革。

第一节 国防的概念及内容

一、国防的概念

国防是国家的产物。从人类社会有了国家的那一天起，国防问题就成了国家政治生活中的头等大事。

何谓国防？《中国人民解放军军语》作出的释义是：“国家为防备和抵抗侵略，制止武装颠覆，保卫国家的主权、统一、领土完整和安全而进行的军事及与军事有关的政治、经济、外交、科技、教育等方面的活动。是国家生存与发展的安全保障。国家的社会制度和国家政策决定国防的性质。”这一释义总结了我国国防的实践经验，体现了我国社会主义国防的特色，符合当前我国国防建设和斗争的实际。

国防是国家的防务，是立国之本，对此人们不会有怀疑。然而，究竟如何认识国防问题，树立什么样的国防观念，怎样来巩固国防，却是仁者见仁，智者见智。比如传统国防观或者叫做小国防观，将国防基本限定在军事上，甚至认为国防是政治家的事，是军队的事，与老百姓无关。显而易见，从这种小国防观出发的国防是防不住的，是防不胜防的。现代国防观，或者叫做大国防观认为，国防是国家的总体防务，或者叫做综合防务，它不仅仅是军队的事，还需要进行相关的政治、经济、外交、科技、教育等方面的建设和斗争。这种大国防观的出发点，是把中国的国防安全放到世界的政治、经济、军事的大背景、大气候之下来考虑，是全民的、全方位的、立体的、现代化的国防观。

人类历史即将进入二十一世纪，在这世纪之交的重要历史时期，要想建设巩固的国防，就必须树立现代国防观。随着科学技术尤其是信息技术的进步，人们的交往日益频繁、迅捷、方便，地球正在变成一个“小村庄”。大兵压境不再成为威胁的主要标志，攻城掠地不再成为争夺利益的基本手段。政治、军事、科技、文化等方面互为目的、互为手段，军事安全与其它安全之间的传统界线正在变得越来越模

糊。信息时代的国防安全是综合安全概念 包括军事、政治、经济、科技等各方面的安全。其中，信息安全的影响更为突出。由于信息时代的国防比较复杂，偶然性、随机性、不确定性以及不可测事件越来越多。判定各种事件的影响，不能以事态规模的大小作为衡量的标准。对有些“小事”，如果预研或预控不力的话，将可能引起连锁反应。此外，信息时代，新闻传媒手段越来越先进，对整个社会的影响力越来越大，这使能影响民族精神和民族气节的舆论安全问题变得极为迫切。总之，诸领域的安全互相影响，紧紧地交织缠绕在一起，轻视了其中哪一方面，都是对国防安全的片面理解。因此，我们必须对综合安全问题有所研究，有所认识。

二、国防的内容

从现代国防观出发，国防的内容是十分丰富的。其中，捍卫国家的主权、领土完整、维护安全、保障发展是最基本的内容。

（一 捍卫主权

主权是一个国家的根本标志，是一个国家具有按照自己的意愿，根据本国情况 选择自己的社会制度、国家制度 组织政府 独立自主地处理其国内事务而不受他国干预或限制的最高权力。主权有两重性，即对内属性和对外属性。对内属性是指一国范围内对其一切事务的最高统治权。它决定和派生其它一切权力，并通过立法、行政、司法、公安、军事、经济、文化等手段进行自己的统治 而不受其它任何力量的干预和限制。国家主权的对外属性，是指国家在对外事务中独立自主的决定权，不受他国和任何政治实体的干涉。他通过独立自主地决定外交政策，处理国际事务，享受国际权利，承担国际义务，以及国际交往、缔结条约、决定战争与和平等重大问题表现出来。国家主权的两重性是不可分割的统一体，一方面，对内主权决定并派生出对外主权，没有对内的最高统治权，就不可能存在对外的独立权，如果对内主权受到颠覆和破坏，对外主权必然受到侵犯和践踏；对外主权反映并维护对内主权，如果对外独立权受到侵犯，对内主权必然受到侵犯和破坏。如果一个国家的主权被剥夺，其它的一切，包

括国家的独立、领土完整、政治制度、社会准则、生活方式和国家荣辱等，根本就无从谈起了。因此，捍卫国家主权，始终是国防中第一位的、最主要的内容。

（二）保卫领土

领土是国家存在和发展的自然物质前提，是国家行使其主权的空间。《中国人民解放军军语》对领土的解释是：“国家主权所及的全部疆域。包括国家的领陆、领空、领水以及领陆与领水的底土。领土是构成国家的基本要素之一，国家行使主权的地理空间及其人民赖以生存和发展的客观环境。”领土完整是国家主权在地域上的最高表现。任何国家即使是因历史原因造成领土暂时不完整，也应该追求、实现领土完整。领土完整的含义是：凡属本国的领土，决不能丢失、决不允许被分裂、支解和侵占。领土完整与捍卫主权是互相联系的。领土完整是国家行使主权的基础，是构成主权的重要而不可分割的部分，破坏领土完整就是侵犯国家主权。国防必须履行保卫本国领土完整的职能。

（三）维护安全

国家要正常的生存和发展，必须处于和平和稳定的状态，一个国家如果没有和平、稳定的环境，就难以生存，就不能搞好建设和发展。一旦遭到外来的武装侵略和颠覆，安全受到威胁，国家就必须运用自己的国防力量，坚决给以还击，确保国家的和平与稳定。当国内的敌对分子勾结外国敌对势力进行武装暴乱，危及国家安全的时候，国防力量就要采取措施，防止和平息暴乱，保卫国家的安全。

（四）保障发展

国防必须保障国家的发展，而保障国家发展的重点又是国家的经济利益。国家的经济利益表现为国家经济的繁荣发展、科学技术的不断进步、人民生活水平的不断提高。因此，经济发展又是国防建设必不可少的物质基础。没有经济的发展，就不可能从根本上建设强大的国防；反过来，国防建设主要又是经济发展的重要保障，没有强大的国防，也就不可能有经济的发展。在和平时期，国家的安全利

益始终不能放松，但国家利益追求的侧重点首先是经济利益。如我国在新的历史条件下，坚持以经济建设为中心，强调在国民经济发展的基础上逐步实现国防现代化，要求国防建设必须服从、服务于经济建设的大局，并为经济建设创造良好的和平环境，正是上述关系的重要体现。只有经济发展了，国防才能强大，国家的主权、领土、安全和地位、尊严才能得到可靠的保证。

现代国防的根本职能是捍卫国家利益，防备和抵御外来侵略，防备和平息内部与外部势力相互勾结所发生的动乱、暴乱。但是，在现代国防中，经济的强大，科技的发展起着越来越重要的作用，各国都十分重视综合国力的提高。因此，国防的内容决不仅仅限于军事的建设和斗争，而必须包括与之相关的政治、经济、科技、文化、信息、教育、外交等方面的建设和斗争。

第二节 信息的科学概念

“信息”一词不是现代产生的，自从有了人类也就有了信息，并通过语言、文字、形体等方式进行传递和交流。在我国，信息一词古已有之，唐朝诗人李中在《暮春怀古人》一诗中就有“梦断美人沉信息，目穿上路倚楼台”的佳句。信息的英语是 *informati*，我国的台湾译为“资讯”，信息的日语是“情报”。

一、信息的含义

信息是一个具有高度抽象型和普遍性的概念，从不同的角度有不同的解释。所谓“信息”，最简单的解释是“音信、消息”（辞海释义），比较确切的定义是“信息是表征客观事物运动状态和方式、相互联系程度及规律的表述”。

这里所谓的客观事物，是指宇宙事物和世界事物。日月星辰等天体是宇宙事物，随着航天事业的发展，这方面的事物将越来越多。世界事物又分为有形事物和无形事物，有形事物是指看得见、摸得着的物质。人们的思想、认识、意志、情绪、策划、方法等都是无形事物，

虽然看不见摸不着,但也有一定的表达方式和状态,如语言、文字、行动等;所谓事物的运动状态、相互联系程度及其规律,是指事物的形状、颜色、功能及变化,以及各种事物相互间联系、作用的结果。在客观世界中,任何事物都不是孤立存在的,都是与其它事物相互联系的,而事物间的联系,本质就是物质、能量和信息的交流。或者说,在客观世界中,事物、系统之间相互作用的三种基本方式是物质流、能量流和信息流。在三者中,物质、能量是基础,没有物的存在与运动,就没有信源。由此可见,信息是具体的不是抽象的,反映物质世界的信息如此,反映精神世界的信息也是如此,如某一计划的披露,都表达了具体内容;所谓表述,是说事物的运动状态和方式,只有通过直接或间接的表述反映出来,才能成为信息。表述和反映的方法很多,如语言、文字、数字、符号、图象以及动作表情等。信息可以直接表述,也可以间接表述。

二、信息传播的三大要素

——信源,也叫信息源,是信息的发源地。信息是客观事物的反映,信息来源于信源,信源没有虚假的,它所发出的信息都是真实的。

——信宿,是信息的归宿,是接收信息者对信息判断后作出的处理结果。信宿决定着信息的价值,因此,当信息被有关者获取后,要对其进行筛选分类、综合分析、判断处理,以便保留有价值的、摒弃无价值的,利用有价值的,充分发挥信息的作用。

——信道,即传递信息的通道,是信源与信宿之间联系的纽带。信道有自然信道,如空气、风、水等;人的本能信道,如人的感官、躯体和语言等;技术信道,如通信系统、计算机网络系统等。

三、信息的基本特征

信息具有以下特征:

1 客观性。信息是客观存在的,是除物质、能量之外存在于世界的第三要素。在客观世界中,事物之间相互作用的三种基本方式:物质流、信息流和能量流。信息的客观性,并不意味着信息本身就是一种物质,而是说它是事物的状态、特征及其变化的客观反映。既然

事物的状态、特征及其变化是不以人的意志为转移的客观存在，反映这种客观存在的信息，就不能不同样带有客观性。

2、有用性。信息能满足人们某些方面的需求，用来为社会服务。因此，信息具有使用价值。信息通过一定载体反映出来，被人们知道和理解，即可产生利用价值。特别是经过人类加工、社会取舍及组合后，使用价值更大。信息不是过了时的已知的东西，而必须是具有新内容的东西。此外，信息是否有用，要看它能不能作用于接收对象。

3、共享性。信息作为现代社会的一种重要资源，可供人类共同享用。但是同一则信息，由于人们对其认识程度的不同，必然会导致对其利用程度的不同。比如，在战场上，对一些信息的不同判断和利用，可以出现不同的战斗结果。信息的共享性，往往引发人们对信息的独占欲，于是便采取一些措施进行保密，如电报密码、计算机的特殊命令等。

4、可控性。此特征主要反映在三个方面：一是可扩充。人的知识不断增加，能力不断提高，信息技术不断发展，使信息量不断在扩充；二是可压缩。由于信息量大，人们可在庞大的信息量中压缩取舍 择其有用者而取之；三是可处理。如分类、存储、搜索、增删、消除和修改等。信息的可控性，既增加了信息技术的可操作性，又增加了信息技术利用的复杂性。

第三节 国防信息的存在方式

国防信息所呈现的形态是千差万别、各具特色的，似乎看不到有什么规律性，但仔细辩解其存在的形式，它可以区分为有形的国防信息和无形的国防信息两大类。有形国防信息主要包括与国防建设有关的各种文书、资料、图书、音像制品以及军事禁区、军队活动场地、军事行动和国防科技重要研究成果、样品等有关内容的表述。有形国防信息是以依附于某种载体的形式表现的。另一种是无形的，是人们在通常情况下看不见、摸不着的。如传递在通信系统或计算机

系统中的各类国防信息、传播在空中的电磁波以及人们与其相关的意识、思维等。比如，指挥员对某一重大军事行动作出决策前的思考、分析，人们通过阅、听有形国防信息而被大脑摄取并储存的信息等。

有形国防信息与无形国防信息有着密切的联系，而且在一定的条件下又相互转化。比如，当人们阅、听某份秘密文件时，就可以把它的内容储存到头脑中，这时，有形的信息就变成无形的信息。又如，某人参加某一次军事新装备论证会议时，既不发文件，也不准记录和录音、录像，会议内容全靠脑子记忆。但根据工作的需要，今后需将头脑中记忆的内容整理出来，这时，无形的信息又转化为有形的信息。

国防信息的两种存在方式，客观上要求我们不仅要重视保护有形的信息安全，更要重视无形的信息安全。国防信息被泄露，并不一定是因为信息载体失去控制，更多的是通过言谈话语或是通过载密的电波、声波泄露出去的。这同样会给国防信息造成危害。然而，在平时工作中，人们更多地想到的是秘密文件、资料、密码电报等表现为有秘密载体的有形国防信息，并注意对其采取多种防范措施，实施有效控制。但对无形国防信息，因为它看不见，摸不着，往往不易引起人们的重视，疏与防范。比如，在信息社会里，电话已成为人们工作、生活以及社交活动中不可缺少的通信联络工具。在通常情况下，打电话既有公事也有私事，涉及的问题不仅有经济工作、科学技术、日常生活方面的内容，而且还必然要涉及到军事工作、政治工作、国防建设以及隐蔽斗争等方面的重要信息。因此，各国情报机构都把窃听电话作为他们获取国防情报的重要手段之一。因此，不仅要十分重视有形信息的安全，也要重视落实无形信息的防范措施，以防国防信息通过有形与无形的各种渠道泄露出去。

第四节 国防信息的范围

国防信息的范围，是国防信息这一概念所指对象的总和。国防信息的范围非常广泛，包括为国家防务进行的军事及与军事有关的政治、经济、外交、科技、教育等方面活动的表述。本课题所研究的国防信息，主要是关系国防和军队的安全与利益、在一定时间内只限一定范围的人员知悉的信息，即国防涉密信息。

国防涉密信息的基本范围主要包括：国防和军队建设中各项工作的规划及实施情况；作战部署、部队调动、输送及各项勤务保障事项 秘密情报及其来源、手段、能力 秘密通信的密码、资料 电子对抗及其它特种技术、手段、能力等情况 军事禁区、设防地域和重要军事设施的情况；战备演习、部队训练情况，院校不宜公开的专业和技术、学术研究成果；军队的组织编制、实力，军以下部队及特殊单位的番号；国防科学技术研究的重要成果，先进的、我军特有的军事装备的战术技术性能和核心部位的技术资料；预备役人员的储备、战时动员计划及可供国家动员的人力、物力等有关情况；政治工作策略、部队政治素质和不宜公开的政治活动、涉外事件、重要案件；国防经费的预、决算 国防工业的分布 重要军事物资装备的生产、调拨、储备 以及战略、战役后方基地的情况；高级干部和负有特殊使命人员的驻地、行动和重要会议的内容、时间和场所等情况；不宜对外公开的文件、资料、书报、刊物、影视资料等。

国防涉密信息的具体范围，包括在国防和军队建设的各项具体工作中。例如，总参谋部印发的《中国人民解放军军事工作中军事秘密范围及其密级划分规定》中，将军事工作中的秘密区分为作战、情报、通信、训练、军队院校教育、军务、装备、动员、炮兵、装甲兵、工程兵、防化兵、电子对抗、雷达、机要、测绘、外事、陆军航空兵等方面 并划定各方面工作中秘密的具体范围。为便于实际工作中操作和掌握，同一业务系统秘密的范围及其密级，由各级依据规定，列出具

范围和对象。

国防涉密信息按其内容的重要程度和对国防建设的利害关系，分为绝密、机密、秘密三级。绝密是核心秘密，如被敌人获悉，将对国防的安全和利益造成特别严重的危害；机密是较为重要的秘密，如被敌方获悉，会给国防的安全和利益造成严重危害；秘密属于一般的部分，如果泄露，也会造成一定的危害。

国防信息涉密的基本范围和具体范围具有一定的时间性和可变性。保护信息安全的目的是服务于政治斗争、军事斗争及国防建设的，即服务于国家安全利益的。保密的内容是随着国内外形势的发展和国家的利益需要不断地发展变化的，该保的不保，会使国防安全和利益受到损害，该变的不变，同样会使国防利益遭受损失。片面地强调信息安全，人为地制造神秘感，则会给工作带来不必要的麻烦。因此，在确保信息安全的前提下，对于有些工作中确需了解的秘密信息，应当准许有关人员接触，以便更好地为国防和军队建设服务。

第二章 国防信息安全

国防信息安全，是一个国家在政治、军事、经济斗争中取得成败的重要因素。我国是一个发展中的社会主义国家，是保卫世界和平的重要力量，在国际事务中发挥着越来越大的作用。我国的政治、经济、军事、科技等方面在世界范围内均处于重要地位，许多国家的情报机构都把我国的国防信息作为他们活动的重要目标。因此，维护国防信息安全的任务相当艰巨。

第一节 国防信息安全的含义

国防信息安全，主要是指国防信息不受威胁，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。

国防信息安全所涉及的范围非常广泛，几乎无法界定。从信息的含义来看，包括信息的完整性（即保证信息没有残缺）、可用性（即保证信息具有使用价值）、机密性（即保证信息不会被非法扩散）；从信息网络来看，包括可靠性（即保证网络和信息系统随时可用，运行过程中不出现故障，若遇意外打击能够尽量减少损失并尽快恢复正常运转）、可控性（即保证操作者对网络和信息系统的控制和管理能力）、互操作性（即保证协议和系统能够互相联接）、可计算性（即保证准确跟踪实体运行达到审计和识别的目的）等；从信息系统的设备来看，包括质量可靠、性能先进、物理安全等；从管理层次来看，包括人员可靠、规章制度健全等。如果再从专业上来分，那么所包含的内容就更广泛了。象安全移动通信、安全数据通信、安全卫星通信、安全智能网、安全计算机网络、安全多媒体网络、安全数据库、安全路由器、安全浏览器等等。

第二节 国防信息安全的地位作用

在新的历史条件下，国防信息安全在维护国防安全和利益，保障军队建设和作战的顺利进行中，处于非常重要的地位。

一、国防信息安全工作是党、国家和军队工作的重要组成部分

国家利益是一个主权国家在总的国际关系格局中生存与发展需求的总和。国家安全是国家的最 高利益 维护国防 信息安全是维护国家利益的最重要的内容。因为国防信息安全与国家的生存、发展是直接相关的。国防信息安全与不安全的问题，实质上是国家间阶级斗争的一种反映。只要国家和阶级还存在着维护信息安全就必然是党、国家和军队工作中不可缺少的重要组成部分。

国防信息安全工作贯穿于国家工作的各系统、各部门。这是因为国防工作要通过许多职能部门进行，各个部门，特别是高级领导部门在履行职责的过程中 必然要不断产生、传递、使用和存储大量的

秘密信息。这些信息一旦泄露或被敌人窃取，就会直接影响国防建设的进行，给国家安全带来威胁或危害。在整个国家机器中，任何一个部门的失泄密，都会给国家带来损失。信息安全工作做好了，不仅有利于国家的安全和利益，而且会直接保障和促进各项工作的顺利进行。

军队是国家机器的重要组成部分，它的基本职能是保卫国家的安全，是国防信息安全的重点和要害。军队的各级机关和部门，特别是高级领导机关和要害部门，掌管着大量秘密信息，其中作战、情报、通信、机要、战勤等方面的信息都属核心秘密，具有全军性、长远性和战略性，与国家和军队的根本利益关系最大，一旦被敌方获悉，将会对国家和军队造成特别严重的危害。因此，军事核心秘密信息是敌人不顾一切代价窃取的重点目标。这种对国防建设或作战行动特别重大的利害关系，在战争年代和非常时期，表现得极为突出和明显，也容易引起人们的重视。而在平时时期，特别是对外开放以来，许多过去不公开的情况都对外公开了。有些人以此为根据，认为没有什么信息秘密可保了。这种认识是极其有害的。尽管当前国际形势趋向缓和，大仗一时打不起来。但是我们必须清醒地认识到，战争的根源并没有根除，国防工作对内反颠覆、对外反侵略，保卫国家安全利益的根本职能没有变。在平时时期，信息安全不能有丝毫的放松。历史教训告诉我们，平时时期不重视国防信息安全，战时就会吃大亏。因此，国防涉密信息的安全总是与国防与军队的建设紧密联系着，保守军事信息安全不仅是国防和军队建设自身的需要，而且是国家安全利益的需要，是一项不可缺少、无比重要的工作。

国防科技直接反映着一个国家实力的强弱，同时也决定着它在国际上的地位、作用和影响。在科学技术突飞猛进、日新月异、激烈竞争的今天，国防科技的发达与否，直接关系到国家的兴衰乃至存亡。国防科技战线一些重要尖端技术外泄，事实上就等于把“屠刀”交给别人。因此，国防科技战线上的情报与反情报斗争日益尖锐复杂，并已成为各国维护国家安全利益的核心问题。当今，国际竞争激

烈万分，失去一项领先技术就是失去一份优势，而失去优势就要受到别人的控制、敲诈和威胁，国家在世界战略格局中的地位作用也就受到影响。在国防科技情报战线上，我们的对手强大而狡猾，形势非常严峻。因此，在严酷的斗争面前，国防科技战线的人员要为国家的安全和民族利益尽心、尽力、尽职、尽责 这是历史赋予我们的神圣职责。

在国际和平力量日益增长的情况下，我们将会与更多的国家建立友好关系，一些过去是敌对的国家也可能会转为友好。但是，只要国家和阶级还存在，信息安全工作就不能放松。何况在间谍与反间谍问题上 多数国家始终奉行“只有对手、没有朋友”的原则。一些国家不仅搞敌国的情报，也搞友好国家的情报，甚至连自己的军事盟国也不放松。因而，无论国际形势怎样变化，维护国防信息安全的工作都必须常抓不懈。

二、国防信息安全领域是对敌军事斗争的重要战线

随着科学技术的进步和发展，国家之间在政治、军事、经济上的角触竞争越来越激烈，国际上间谍与反间谍的斗争也日趋尖锐复杂，隐蔽斗争已成为国际斗争的重要战线。近年来，西方一些国家不惜花费巨资，大力加强情报工作，并且把我国的国防信息作为他们活动的重要目标。因此，国防信息安全在对敌斗争，特别是对敌军事斗争中占有特殊重要的地位。

纵观人类战争的历史，有无数战例说明，交战双方谁能千方百计地获取对方的重要军事情报并有效地保住自己的军事秘密，在一定意义上说，谁就取得了战争的主动权，从而赢得战争的胜利。反之，就可能丧失战争的主动权而招致失败，甚至国家灭亡。如第一次世界大战期间，德军的一位高级参谋在华沙的一次宴会与同僚谈论战争和时局时 他嘲笑美国人说：“美国支持英国与法国的政策 没有什么用处。因为不久德国将在凡尔登发动一个有决定性的全面攻势，这个战役必将结束这场战争”。这番话被同桌的一个美国商人听到后，立即转告了美国驻英大使馆的有关部门，使馆又迅速转告法军。

由于法军周密做好了各项战役准备，结果使德军在凡尔登战役中惨败。第二次世界大战中这方面的事例更是屡见不鲜，如日本联合舰队司令山本五十六的座机被美军飞机拦截并击落、日美中途岛之战中日海军精华几乎被全歼，都是因秘密信息泄露而造成的。

在近期世界局部战争中，各国更加重视信息安全工作，因为严格保密，出奇制胜，以少胜多，决战告捷的战例不胜枚举。如 1981 年 6 月 7 日，以色列对伊拉克核反应堆偷袭成功就是一个典型的例子。70 年代末，以色列人得到了法国为伊拉克建造核反应堆的情报。因为核反应堆的建成标志着伊拉克将拥有制造核武器的能力，显然伊拉克的核反应堆对以色列构成了巨大威胁。1980 年初以色列人制定了一个“巴比伦”行动计划，决定偷袭伊拉克的核反应堆。为此以色列情报人员采用各种手段刺探到不少有用的情报，其中包括约旦飞机随时可使用沙特阿拉伯领空运送军用物资前往伊拉克。与此同时，他们在一个偏僻的沙漠里建造了一个水泥模型核反应堆，让飞行员反复进行了模拟轰炸训练。偷袭之前，把所有要出动的轰炸机全部改头换面，涂上约旦军用飞机的标志。当 14 架轰炸机进入伊拉克领空时，以色列人诡称“我们是约旦飞机”，因此骗过了阿拉伯国家地面雷达的跟踪，径直地向着进攻目标扑去，一举摧毁了伊拉克的核反应堆。以色列的“巴比伦”行动计划，从策划到实施，前后长达 18 个月。由于采取了严格的保密措施，没有走漏丝毫风声，阿拉伯国家对他们的行动计划毫无察觉。

在和平时期，国防涉密信息的泄露一时不会造成兵败人亡的惨痛后果，然而，它却会造成一种巨大的潜在危险。一旦战争爆发，它就会以狰狞的面目让泄密方付出沉痛的代价。因为，和平时期的许多情报活动，都是为未来战争服务的。可以预料，在信息化战争中，国防秘密信息的“泄”与“藏”对于战争的胜负将起着举足轻重的作用。

三、国防信息安全工作是适应改革开放新形势的需要和促进社会主义建设的重要手段

党的十一届三中全会以来，我国实行了改革、开放、搞活的基本政策。毫无疑问，这一国策的实施，是我国走向富强的必由之路。但我们必须清醒地看到，国外情报机构利用我对外开放的便利条件，以种种公开合法的身份对我进行谍报活动，使维护国防信息安全的斗争更加尖锐复杂。

近年来，我国与世界各国的联系发生了巨大变化，相互间的人员交往日益频繁。来华探亲访友、旅游观光、技术交流、洽谈贸易以及讲学、考察等活动日益增多，有些外国及台湾情报机关乘机派遣特务混杂其中，大摇大摆地进入我境内搜集情报。加之我国的开放地区不断扩大。一些军用机场、军港、码头改为民用，准许外国人活动的范围大大放宽。此外，现在我国每年有近百万种科技杂志和报纸，近千万份专利在全世界范围流动。这些也在很大程度上给敌特搜集情报信息提供了便利条件，增大了国防信息泄露的可能性。

在改革开放的新形势下，我们内部的一些人，盲目追求高消费，甚至贪财好色，想不劳而获。国外情报机关正是利用了这一点，拉拢、腐蚀、收买我内部人员的活动十分猖獗。如海军一名干部，为了追求资产阶级生活方式，被台湾特务收买，先后向其提供我军各类战斗条令及机密资料几十份，被判处有期徒刑 12 年。某部一名副连长先后将 87 张军用地图、90 多本军事教材出卖给外国情报机关，被判处有期徒刑 13 年。在我军内部发生这类事件虽属于个别现象，但它不仅会对国防安全造成很大危害，而且影响部队正常的工作和生活秩序及军队内部的纯洁和稳定。

总之，改革开放对国防信息安全带来了许多新情况、新问题。很多政策放宽了，权限下放了，但却给间谍、特务的活动打开了方便之门。我们对来华洽谈业务、投资经商的外国人、港、澳、台同胞和华侨是欢迎的，他们的正常活动和合法权益历来受到我国法律的保护。但我们也要看到确有少数别有用心的人混杂其中，在公开合法的名义下拉拢收买我内部人员，窃取我机密信息。如果我们的同志缺乏警惕，就会中人家的圈套，就会给国防安全造成危害，甚至自己也堕

落为人民的罪人。我们必须牢固树立敌情观念，保持清醒的头脑，在实际工作中采取积极预防措施，有效地做好信息安全工作。

第三节 影响国防信息安全的主要因素

影响国防信息安全的因素，涉及信源安全、信道安全、信宿安全的各个环节，涉及人为因素、技术因素、环境因素等各个方面。

一、信息战因素

所谓信息战，是指敌对双方在信息领域的对抗活动。主要是通过争夺信息资源，掌握信息的生产、传递、处理等的主动权，破坏敌方信息传输，为遏制或打赢战争创造条件。信息战是信息技术发展的必然结果。

随着以信息技术为核心的高新技术越来越广泛地向军事领域渗透和在武器装备中的应用，整个战争机器越来越依赖于信息技术。信息技术不仅已成为各种战争资源发挥效能的基本保证，而且本身就是重要的作战武器。比如，信息的收集、存储、传递、处理、显示、识别等技术，大大提高了指挥效能。全面争夺“制信息权”的斗争促进了把指挥、决策、控制、通信、情报、作战、支援保障、设施及武器装备联结为一个有机整体的自动化信息网络的产生。总之，信息技术使武器装备进入信息化武器系统阶段，奠定了信息化战争的物质基础。信息系统的网络化又促进了信息化战场的形成，为信息化战争提供了可靠的依托，使信息化战争成为未来战争的主要战争形态。

信息技术在对作战能力作出巨大贡献的同时，也对其造成了空前威胁。一方面，信息技术的广泛应用，是部队以及各类武器装备等对于信息与信息系统的依赖程度达到了“不可离之须臾”的地步，任何先进的武器装备一旦信息失灵，就如同废物一般。另一方面，信息对抗技术的高度发展，为有效的干扰、削弱、破坏和压制信息化武器与信息系统提供了手段。近年来，计算机病毒、逻辑炸弹、高功率微波武器、电子袭击工具等信息攻击武器层出不穷，对信息与信息系统

造成了空前威胁。比如，人类进入信息时代的重要标志之一，是全球网络环境的形成。作为信息技术重要内容的计算机网络技术已走过了 30 余年的历程。近年来，多媒体技术、新的传输与处理技术的发展与融合使卫星通信网、移动通信网、开发分布网得以广泛应用，极大地提高了网络的效率，并促使 80 年代后期国际互联网的形成。到目前为止，该网已联接 170 多个国家和地区，拥有 5 万多个计算机局域网和 6 百多万台电脑 5 千多万用户，而且其主机还在以每小时 100 余台的速度增长。与此同时，其它名目繁多的区域网、局域网、广域网以及内部网也在蓬勃发展。发达国家的微机联网率已达到 60%。政府网络、商业网络、军事网络与电力网络通过互联网络连结在一起，使军事行动、政府日常工作、国内与国际贸易等基本的社会活动对网络化的依赖程度日益增强。网络化已经成为一个国家竞争力的重要标志。然而，网络化对社会贡献的增大是以其易毁性为代价的。

在信息时代，极具讽刺意味的是，信息化程度越高的国家越容易受到攻击。随着全球互联网的不断发展，计算机空间不断膨胀，几乎覆盖了世界的每一个角落。在这日益复杂的网络环境中，已不能区分哪里是网络的开始，哪里是网络的终结。计算机空间为信息战进攻一方提供了一个广阔的、无国界的“隐藏”空间。进攻者只要从一处进入网络，就可通过各种途径实施对世界各地任何入网的计算机及信息系统实施信息攻击，并在发起攻击前几天、几个月、甚至几年的时间来部署信息战进攻。近年来，计算机和网络系统遭到“侵入”和“攻击”的事件屡屡发生。可以肯定，未来的信息战，在硬杀伤将继续发挥作用的同时，计算机空间上的争夺将象机械化战争中争夺“制空权”那样激烈。

二、人为因素

影响信息安全的人为因素，是指由于人的主、客观行为而导致的对信息安全的破坏或威胁。它主要是指来自敌方的危害，来自“黑客”行动的破坏，来自自己方人员违纪造成的损失等。