学术研究专著 · 信息工程

指挥信息系统安全防护技术

毛永庆 蒲林科 蒲 星◎主编

西北工业大学出版社

学术研究专著·信息工程

ZHIHUI XINXI XITONG ANQUAN FANGHU JISHU

指挥信息系统安全防护技术

主　编　毛永庆　蒲林科　蒲　星

西北工业大学出版社

西安

【内容简介】 本书重点介绍了现代指挥信息系统安全防护技术的发展现状和发展趋势。全书共九章。内容包括指挥信息系统安全防护的主要特征、计算机系统安全防护技术、指挥网络安全防护技术、巡航导弹防御、无人机防御、激光武器防御、反辐射武器防御、电磁脉冲弹/高能微波弹防御和生物武器防御等。

本书是研究指挥信息系统电子战防御、计算机病毒战防御和网络战防御的重要工具，是研制指挥信息系统科研项目的重要参考。本书可作为相关专业科研人员和高等院校师生的教学参考书籍。

图书在版编目(CIP)数据

指挥信息系统安全防护技术/毛永庆，蒲林科，蒲星主编．—西安：西北工业大学出版社，2017.12

ISBN 978-7-5612-5725-8

Ⅰ.①指… Ⅱ.①毛… ②蒲… ③蒲… Ⅲ.①作战指挥系统—信息系统—安全防护—研究 Ⅳ.①E141.1-39

中国版本图书馆 CIP 数据核字(2017)第 284431 号

策划编辑：雷 军
责任编辑：张 潼

出版发行：西北工业大学出版社
通信地址：西安市友谊西路 127 号 邮编：710072
电 话：(029)88493844 88491757
网 址：www.nwpup.com
印 刷 者：兴平市博闻印务有限公司
开 本：710 mm×1 000 mm 1/16
印 张：10.75
字 数：205 千字
版 次：2017 年 12 月第 1 版 2017 年 12 月第 1 次印刷
定 价：42.00 元

前　言

2013年美国的“棱镜门”事件（爱德华·斯诺登曝光了美国情报部门搜集海量国际互联网和电话记录的跟踪程序）骤使全球聚焦国家安全问题，引发了世界多国的恐慌和外交抗议，也使得指挥信息系统安全防护的重要性空前凸显。

《指挥信息系统安全防护技术》一书以前沿的科研和情报信息为依据，以翔实的材料为支撑，以军事发展需求为牵引，以科技创新为主线，力求全面、准确地描述现代指挥信息系统安全防护技术的发展方向。

全书共九章，可分为两大部分：第一章至第三章为第一部分，主要描述指挥信息系统安全防护的主要特征、计算机系统安全防护技术和指挥网络安全防护技术；第四章至第九章为第二部分，主要描述巡航导弹防御、无人机防御、激光武器防御、反辐射武器防御、电磁脉冲弹/高能微波弹防御和生物武器防御技术。

本书是研究指挥信息系统电子战防御、计算机病毒战防御和网络战防御的重要工具，是瞄准世界指挥信息系统安全防护技术发展趋势、制定指挥信息系统发展战略的参考文献。本书也可作为相关专业科研人员和高等院校师生的教学参考书籍。

本书是笔者对多年来从事指挥信息系统研制及课题项目研究报告的汇总和提炼。毛永庆，蒲林科，蒲星负责了全书的编写及统稿工作，崔琳，蒲烨，蒲伟芬，郭琳，蒲伟宁，蒲大卫，蒲健彤，何宁军，蒲伟博，蒲伟洁参与了个别章节的编写和修改。

在本书的编写过程中，笔者得到了中国电科集团公司第28研究所各级领导、有关专家和同事们的指导、支持和帮助，在此一并表示衷心的感谢。

由于所掌握的资料有限，也限于笔者的水平，书中难免有一些值得进一步研究探讨的问题，不妥之处，敬请读者指正。

编　者

2016年12月于南京

目　录

第一章
指挥信息系统安全防护的主要特征

第一节　指挥信息系统是现代战争攻击的首要目标

信息技术的发展，孕育了一种新的战场装备体系；计算机技术的突飞猛进，推动了新一代指挥信息系统的发展。

C^4ISR（指挥、控制、通信、计算机、情报、监视、侦察）系统是第二次世界大战（以下简称“二战”）之后出现的新事物，是以电子装备为基础，集指挥、控制、通信、计算机、情报与电子对抗于一体，能够对部队和武器实施指挥控制的人机系统。它的出现受到各国、各地区的广泛重视，但它的作用，只是在被称为“第一次信息作战”的海湾战争中才突出表现出来。此后，各军事大国，特别是美国开始加强了对 C^4ISR 的研究。有人认为 C^4ISR 系统不仅是“兵力倍增器”，更是现代军事力量的“赋能器”，因为它能使武器系统或武器系统群的效能提高数十倍且具备新功能。俄罗斯军方则把 C^4ISR 系统看作是二战后继核武器、弹道导弹之后的第三次革命性武器。

军队打不赢，一切等于零。在信息化环境中，随着指挥信息系统自动化程度和效率的不断提高，现代战争都无一例外地把攻击敌方指挥信息单元作为作战的首要目标。

网络技术的突飞猛进及其在军事领域的广泛应用已经引发了一场新军事革命。信息战、网络中心战作为全新的作战式样，已在近期发生的几场高科技局部战争中渐露头角，作战双方都把制信息权的夺取和保持作为战役作战的首要任务。作为信息战核心的指挥控制战，即根据统一意图和计划，综合运用心理战、战役伪装、电子战、网络战、作战保密和实体火力摧毁等手段，防止敌方获取信息，攻击敌方 C^4ISR 系统，破坏其信息流，以影响、削弱或摧毁敌方 C^4ISR 系统的指挥控制能力，同时保护己方 C^4ISR 系统。正是由于指挥控制系统的这种极端重要性，决定了它成为信息战优先攻击的目标；而指挥控制系统的脆弱性和易受攻击性，又决定了它将成为未来战争首先遭受打击的对象。

透视最近 20 多年来爆发的几场局部战争，包括 1991 年的海湾战争、1999 年的科索沃战争、2001 年 10 月开始的阿富汗战争和 2003 年的伊拉克战争，这

些战争虽然背景、对象、规模各不相同，但有一点却是完全相同的，那就是战争之初，首先遭到美军攻击的是对方的指挥信息系统，而先发制人的作战方式就是指挥控制战。

海湾战争开始时，美军提前 24 h 发起对伊拉克军队指挥控制中心和通信网络的强大信息战和电子压制，使伊拉克军队的雷达迷盲、通信中断、指挥失灵，为美军尔后的空袭创造了条件。

科索沃战争中，北约军队同样是先从南联盟的指挥信息系统下手的，美军还首次使用了新的电子战武器——电磁脉冲炸弹，轰炸和干扰了南联盟军的指挥信息中心和通信系统。网络战作为一种作战式样用于实战也是从科索沃战争开始的。美、英等国还开设专题网站，对南联盟的网络实施攻击，并利用计算机病毒企图瘫痪南联盟军的指挥信息系统，进而搅乱南联盟的整个金融系统。美军亦通过互联网发布反南联盟政府的宣传材料，丑化米洛舍维奇，为军事打击制造借口。

阿富汗战争中，美军使用先进的电子战手段，侦听、监视“基地组织”和塔利班的活动，打蛇先打头，利用钻地弹等新式武器先后摧毁了 39 处指挥信息中心、设施以及 11 个基地组织的训练营地，其中部分指挥所还设在有数百年历史的洞穴中。美军轰炸机使用的最新目标瞄准技术、激光制导或全球定位系统制导的巨型炸弹都首先定位于恐怖分子的各个指挥部。美军在阿富汗作战的特种部队里还部署了专门的心理战部队。

伊拉克战争中，美军以“斩首行动”拉开了战争的序幕。与此同时，伊军的指挥信息中心、导弹阵地、飞机场即刻遭到了美军巡航导弹的猛烈攻击，使得伊军很快丧失了制空权，也无法实施有效的反击作战。

第二节　指挥信息系统面临的主要威胁

不同层次的指挥控制系统执行不同的任务，其基本功能大都可以概括为下述 3 方面。

1. 情报信息获取和分发

通过各种传感器和不同手段获取敌方的兵力部署、装备配置和数量、作战意图、威胁情况、打击效果等连续不间断的战场态势，经过综合处理后快速分发到上级、下级和友邻部队。

2. 对人员和武器装备的指挥控制

根据瞬息万变的战场态势，合理调动兵力和武器装备，与友邻部队协调一致，保证信息资源和能量资源实现最佳结合，发挥系统整体优势，完成作战任务要求。因此，C^4ISR 系统的中心任务是实现系统诸环节和诸要素的无缝结合，实

现系统信息和能量的最优化运用，以最小损耗达成最佳的作战效果。

3. 可靠的通信保障

完成报文、话音、数据、图像和视频信号的传输，为情报/信息的传送和分发、武器装备和人员的指挥与控制提供保障条件。

信息战环境下指挥信息系统面临的威胁可分为硬打击和软打击两种。

1. 硬打击

C^4ISR 系统面临的硬打击主要是各种精确制导武器和新概念武器的打击。21世纪武器装备的基本特征是隐身、远程、精确和通用，作为体系对抗的首要目标，C^4ISR 系统面临着几乎所有不同种类精确制导武器的打击，如地地战术导弹、巡航导弹、空地导弹、灵巧弹药等，钻地弹头还可打击地下指挥中心。这些精确制导武器的命中概率多大于 50%，而且突防能力强、作战机动灵活，对 C^4ISR 系统构成了严重的威胁。电磁脉冲弹/高能微波弹和激光武器专门攻击 C^4ISR 系统的信息网络节点，降低系统的使用效能，甚至使系统瘫痪。

2. 软打击

软打击多针对 C^4ISR 系统的传感器、计算机系统和通信网络，主要表现为电子压制、干扰、计算机病毒和网络攻击，其中计算机病毒突发性强、防不胜防，轻则干扰 C^4ISR 系统的正常工作，重则使系统崩溃。

第三节　指挥信息系统安全防护的主要特征

指挥信息系统安全防护有以下几方面的主要特征。

1. 攻击武器和作战方式的先进性

现代战争，用于攻击指挥控制系统的武器装备十分先进，其中以精确制导的巡航导弹、激光制导的钻地弹、新近研制成功的电磁脉冲弹或高能微波武器等各种新概念武器和各式隐形轰炸机、性能先进的联合攻击战斗机为主，还有从事信息破坏的计算机黑客攻击和软件攻击。

这十多年来发生的几场大的局部战争，美军都采用了高超的作战方法。

(1) 打头阵的信息战。这几场局部战争，美军都是首先动用先进的侦察卫星、无人侦察机、空中和地面侦察设备、GPS 卫星导航系统对敌方进行全方位、大纵深的信息侦察与定位。然后采用软硬杀伤手段对敌方的指挥控制中心、通信、雷达等重要军事设施进行硬摧毁和电子软打击。阿富汗战争期间，美军仅第一轮空袭就发射了 50 枚巡航导弹，相当于海湾战争发射总数的 1/6，使阿富汗的军事目标遭到严重摧毁。美军还利用部署在土耳其空军基地和海军航母上的 EA－6B 电子战飞机对预定空域进行强电磁干扰，然后各种作战飞机在 E－3 预

警机的统一指挥下，攻击阿富汗的指挥通信系统、兵器制导系统和地面雷达。在阿富汗战争期间，美军特种部队进入阿富汗，在主要交通要道和秘密地点安装监测仪，监视阿富汗部队的行动，并利用报话机引导美军飞机进行攻击。

早在阿富汗战争开始之前，美军就对个别存有拉登资金的银行账户进行了网络攻击。美国黑客还对阿富汗总统府网站进行了拒绝服务攻击，将许多塔利班网站的主页改成了对拉登的通缉令。

(2)“以空制地”的非对称作战。目前，空中打击已经发展成为现代战争的主要作战方式。在43天的海湾战争中，美英部队进行了39天不接触作战的空中打击和4天“打扫战场”的地面作战。空袭摧毁了伊拉克军队60%的防御能力，对整个战争的结局起到了决定性的作用。而科索沃战争是纯粹的“空袭战争”，在78天的空袭作战中，美军投入了近1 000架飞机和包括3艘航空母舰在内的58艘舰船，投掷各型导弹、炸弹2.3万余枚，对南联盟2 000多个地面军事、民用目标进行了多轮次、多波次的大规模、高强度的狂轰滥炸。同样，在阿富汗战争中，美军通过第一阶段的强大空袭，摧毁了塔利班的防御设施。B-52，B-1轰炸机的机组人员通过掌上电脑和卫星传递的信息与地面特种部队人员联系，投下各种精确制导炸弹，在塔利班和基地组织全然不知的情况下进行空袭。

这几场战争，空袭使美军出尽了风头，充分显示出了它克敌制胜的优越性。依靠先进的侦察卫星、侦察飞机等侦察监视平台和巡航导弹、隐形飞机等远程打击兵器，美军的夜间空袭实现了“我们看得见敌人，敌人看不到我们；我们打得着敌人，敌人打不着我们”的一方打击、一方被动挨打的作战。美军的B-2，B-1B和B-52轰炸机可以从美国本土长途奔袭上万公里，使敌方在不知不觉中遭到空袭。

(3)“指哪打哪”的超视距精确战。美军的全球定位系统制导武器、激光制导武器已经把命中误差缩小到了1～3 m的范围。指挥控制系统指到哪里，精确制导武器就能打到哪里。精确打击的前提条件是精确探测和精确定位。美军靠一整套由空间卫星、侦察飞机等组成的高效能探测手段，及时准确地发现目标。美军的探测范围可达攻击国的大部分战略、战役目标，探测距离可达数百、数千公里。海湾战争中，美军的一架F-117隐形轰炸机隐蔽突入巴格达上空，只发射了一枚激光制导炸弹，便准确击中并摧毁了伊拉克的电话电报大楼。科索沃战争中，美军在战前一年多时间里就已对包括我国驻南联盟大使馆在内的各类目标进行了定位，为开战后的精确打击提供保障。被美军称为“人类历史上最精确的战争”的阿富汗战争，美军共投掷了2.2万枚导弹和炸弹，其中约75%的弹药击中并摧毁或部分破坏了目标。美军可在几千公里之外实施超视距（远程）攻击，超视距精确作战的好处就在于能在敌方武器系统的有效杀伤距离之外通过精确制导武器摧毁目标。

但美军的精确制导武器也常常会失准，在阿富汗战争期间，大约有1/4的炸

弹偏离目标。2001年12月，一枚精确制导炸弹偏离目标，不但炸死了3名美国陆军特种兵，还差点伤及阿富汗临时政府主席卡尔扎伊。在对付移动目标、洞穴或地下目标时，美军的超视距精确战也常常显得无能为力。

(4)“来去无踪”的隐形战。隐形战正在成为美军进行局部战争的看家本领。这十多年间的几次战争中，B-2，B-1B隐形战略轰炸机、F-117隐形轰炸机都担纲了作战的主角。据《美军海湾战争总结报告》称，在海湾战争中美军空袭的第一个晚上，被攻击战略目标任务的35%是由F-117A隐形轰炸机承担的；在海湾战争全过程中，F-117A出动架次只占全部轰炸机出动架次的2%，却承担了被攻击战略目标40%的任务；它不需要各种空中支持力量，如战斗机和电子战飞机的支援。巡航导弹是专为躲避雷达探测而研制的超低空飞行的导弹，由于地球曲率对电波的遮挡，雷达只能在很短距离之内才能发现它，往往还来不及做出射击反应，巡航导弹就已飞出了雷达的探测范围。“战斧”巡航导弹也不需要空中预警机、战斗机和电子战飞机的协助，是接到通知就能实施攻击的唯一一种武器。反辐射导弹是专门对付雷达系统的导弹。海湾战争中美军发射了2 151枚昂贵的高速反辐射导弹，使伊拉克的每部雷达均遭受到4～8枚反辐射导弹的袭击，几乎摧毁了全部伊拉克的雷达。雷达的被摧毁导致了伊拉克整个防空系统的瘫痪，使居世界第6位的伊拉克空军失去了战斗力（见图1.1）。

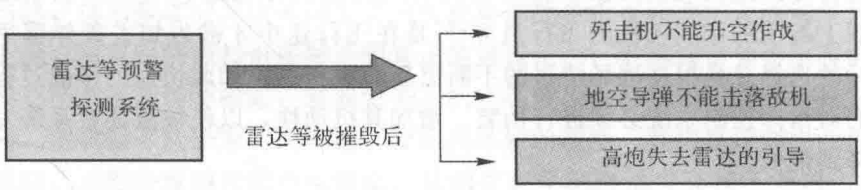

图1.1 美军隐形战使伊拉克整个防空系统瘫痪示意图

2002年3月，美国总统布什、国务卿鲍威尔和国防部长都曾表示，美军特别是空军装备将要向全方位隐形化方向发展。最近几年之内，美空军将装备3 000多架隐形战机，并计划近期组建一支由12架B-2隐形轰炸机和48架F-22隐形战斗机组成的能够快速部署且能在一天之内摧毁270多个目标的小型“全球隐形打击特遣部队”，担负摧毁敌方指挥控制中心、防空导弹系统等重要目标的作战任务。

(5)“攻城先攻心”的心理战。“攻心为上，攻城为下”自古以来就是军事家们心往神追的信条。信息时代，心理战不再单单是一种辅助的作战手段和样式，已成为在全时空、全方位、多层次发挥作用的战略行动。心理战在削弱和瓦解敌军战斗意志，降低己方作战人员伤亡等方面起了十分重要的作用。因此，美军十分重视心理战部队的建设。目前，美军的心理战部队作为特种部队的一部分，由一个现役心理战大队、两个后备役心理战大队和一个心理战战略研究中心组成。

战争中，各军种都有实施心理战的具体任务。海湾战争开始前，美军的心理战部队在伊拉克边境就已大肆渲染美军的作战能力和新式武器的威力，对伊军形成巨大的心理威慑，使其不敢轻举妄动。战争中，美军除了利用传统的心理战手段之外，还广泛使用卫星定位、测向和电视转播、计算机信息处理、信号模拟技术等高科技手段开展心理战活动。心理战部队并且深入伊拉克境内，将反对伊政府和宣传美军实力、战果的录音带散发到巴格达地区。地面战争期间，伊军共有 8.7 万名官兵投降，其中绝大多数投诚、逃亡或投降的伊军手里都持有美军的心理战宣传品。这一战果被称为美军的“心理战奇迹”。阿富汗战争中，美军的心理战部队很好地配合了军事打击行动。心理战部队通过空投传单、发放食品、战场喊话、无线电广播等活动分化瓦解塔利班的士气，促使一批又一批塔利班士兵投降。这些成果表明，美军正在从过去倚重的“物理暴力打击”向以军事实力为基础、发展“心理暴力打击”的方向转变。

2. 军事伪装欺骗的必要性

指挥控制系统作为现代战争的大脑和神经中枢，其重要作用已显得越来越突出。在这个“发现了就意味着摧毁”的时代，一旦被敌方发现可能还来不及做出反应就遭到了摧毁，根本没时间对对方实施反击。在阿富汗战争期间，美英部队从发现目标到战机飞临头顶实施攻击的时间大多没有超过 10 min，从基地或航空母舰上起飞的作战飞机的飞行员 80％是在飞行途中才被告知去轰炸哪里，因为目标的选择总是根据战场情报的不断更新而更新的。如此快速的作战过程，促使我们对指挥控制系统必须进行伪装、增加其机动性，以使被敌侦察系统发现的概率降到最低。

3. 作战空间的无界性

美军的远程打击能力已达到了数千甚至上万千米，B－2 隐形轰炸机可以从美国本土长途奔袭 1.8 万千米进行作战。目前，美军已经有能力选择打击目标，即对“先打谁，后打谁，重点打击谁”提前作出规划，由此彻底突破了传统的“战线”和“战场”的概念。美军的空中打击打到哪里，哪里就有战线；美军的夜间空袭打到哪里，哪里就变成了战场。美军还可根据作战需要对打击手段和作战武器进行调整组合，如可使用空中、海上、地面的不同发射平台发射炸弹，以增强打击效果。美军还可根据不同目标，使用不同炸弹进行攻击，以形成最佳的作战能力。

网络战已没有了战区的概念，它构制了新的作战空间。除了在传统的物理战场上抗争之外，网络战更多的是在以电磁空间、网络空间为主的虚拟战场进行着“没有硝烟的战斗”。

4. 攻击过程的突然性

美军的精确打击实现了真正意义上的“全纵深作战”“立体作战”和“瘫痪

作战”。由于超视距精确打击的突然性，战争已没有了绝对的后方、纵深和安全区。只要被侦察系统发现，美军即会在瞬间对目标发起攻击，美军最新研制成功并首次部署于阿富汗战场的“全球鹰”无人侦察机，能在发现目标之后 5 min 之内发动攻击。而网络战，无论是无线耦合攻击还是有线因特网攻击，都会在几秒或几分钟的瞬间完成。

5. 作战目的的损毁性

现代战争的作战目的已从过去的“杀人、掠地”逐步发展到现在“毁物、换首脑”的“零伤亡战争”。从 1991 年海湾战争起，美国一直致力于推翻伊拉克萨达姆政权。科索沃战争中，北约 78 天的狂轰滥炸迫使南联盟总统米洛舍维奇下台并将他投入设在海牙的监狱。阿富汗战争中，美军军事革命所强调的战果不是占领土地而是获得信息，美军在阿富汗所使用的许多新的技战术的目的并非用于摧毁而是为了获取情报。美国通过战争剥夺了塔利班的政权并摧毁了基地组织对阿富汗的控制。这些战争，美军依靠大量先进的武器装备和战略、战术，依靠“大量的钢铁和计算机，少量的参战人员”取得了各次战争的胜利，而美军的人员伤亡每次都微乎其微。

信息战的作战目的就是使敌人的指挥失灵、系统瘫痪、通信中断、信息失效、武器失控、人员丧失战斗意志，并最终使其减弱或丧失整个作战能力。

当然，这十多年间，由美国发动的历次局部战争也存在着很大的局限性：从技术上说，超视距精确打击还做不到真正的智能化。一旦掌握了美军空袭的规律性，只要经常变动伪装模式，就能使美军的空袭效果大打折扣。例如，科索沃战争期间，南联盟军队经常运用帐篷、废旧汽车轮胎改变一些指挥控制中心周围的地貌地物，或燃烧废旧轮胎产生浓烟，从而使美军的巡航导弹找不到攻击目标，只好最后燃料烧尽坠地。目前，美军对复杂地形上的目标、隐蔽良好的目标和机动目标的攻击效果还都难以奏效。而且，打击效果评估受技术的局限，也还没有完全解决。比如空袭南联盟的效果究竟如何，美军说摧毁了南联盟 90％的指挥控制中心和军事设施，而南联盟说仅损失了 30％的部队装备，双方各执一词，因此至今谁也搞不清楚。

这些年，美军选择的打击对象都是些经济落后、军力无法与美军相抗衡的弱小国家。自 1975 年历时 12 年的越南战争以美军的失败而宣告结束之后，美国为了维护其“世界警察”的地位，到处挑起战争，但每次都选择弱小国家作为自己的对手。1983 年美军入侵格林纳达、1986 年美军空袭利比亚、1989 年美军入侵巴拿马，而这些小国在美军的眼里都是些“软柿子”。近十几年间，美军遇到最大的作战对手是伊拉克，持续 12 年的军事打击和经济封锁使伊拉克的经济和军事实力遭受重创，2003 年的伊拉克战争才使得萨达姆政权被推翻。

第二章
计算机系统安全防护技术

第一节　计算机病毒战的基本特点

进攻性信息行动和防御性信息行动都把信息作战核心的指挥控制单元作为打击的重点和打击的中心。指挥控制单元包括指挥控制系统、武器控制系统、通信系统、侦察探测系统和后勤保障系统。指挥控制系统主要以计算机系统为神经中枢组成。

指挥控制系统面临的威胁分为硬打击和软打击两个方面。其硬打击主要包括各种精确制导武器（如巡航导弹、精确制导导弹、钻地弹）以及各种新概念武器（如电磁脉冲弹/高能微波弹、强激光武器、粒子束武器、生物武器、纳米武器）的打击。软打击多针对 C^4ISR 系统的计算机系统、传感器和通信网络，主要表现为电子压制、电子干扰、计算机病毒和“黑客”攻击。

C^4ISR 系统是以计算机系统为核心的技术装备与指挥人员相结合，对部队和武器实施指挥控制的人机系统。信息战和战场数字化都以指挥控制系统为中心，以计算机平台为基本，使现代战争的战场景象为之一新。海湾战争之后的历次战争，美军的整个作战系统都极度依赖计算机，其预警机、电子战飞机、侦察机、遥控飞行器、导弹、制导炸弹以及海陆空三军的所有军事行动都在 C^4ISR 系统的统一指挥控制下进行。最典型的要算美国陆军从 1994 年开始实施的数字化部队建设，其目的是通过计算机和通信系统把战场上的单兵、单个作战平台和战场指挥控制系统联为一体，形成一个巨型的作战信息网络系统。

有人说，21 世纪是计算机战的世纪。计算机对战争的影响越来越大，一旦遭受攻击后果不堪设想。

计算机战可分作计算机病毒战和计算机网络战。据统计，我国目前有 55% 以上的计算机受到病毒的感染。2001 年世界发生的十项重大事件中，位列 9·11 之后的第三大事件，就是“红色代码”计算机病毒攻击事件，因此，有人也把 2001 年定名为“计算机病毒年”。

计算机病毒实际上就是专门用来破坏计算机正常工作的特殊程序。它以计算机能够运行的代码方式隐藏在计算机硬盘、软盘、光盘、网络或其他外部设备

中，能够自我复制和侵入其他有用程序之中，以篡改、损坏程序的有效功能。当用户运行一个带病毒的可执行文件时，首先执行的是病毒程序。病毒程序在执行过程中，如果驻留内存，它首先会修改中断向量，使这个中断向量指向病毒，以便及时获得控制权。如果不驻留内存，它将寻找感染对象进行传染。

计算机病毒不同于一般程序而独具特殊性：①传染性，它具有强再生和传染机制。②潜伏性，寄生于其他程序之中的计算机病毒往往需要等待特定的时间或事件才会触发。③隐蔽性，计算机病毒破坏其他程序和数据的过程不易被察觉。④突发性，计算机病毒具有难以防备的突然性。⑤破坏性，它会给用户造成灾难性和长久的危害。

世界上现有多少种计算机病毒，是几十万种还是上百万种，谁也无法说得清。2001 年，美军投资 2 500 万美元继续悬赏、招募软件专家编写可用作武器的计算机病毒，并试验通过无线方式向敌方信息设备强行注入病毒，意在战争条件下用它“摧毁敌指挥控制系统和通信线路，在敌人内部传递经篡改的信息”。1999 年，第一代“病毒固化”微型芯片技术在美军问世，一旦需要，这些平时发现不了的“固化病毒”便被有线或无线方式遥控激活，使装备这类产品的军队不打自瘫。据称美军于 1990 年 12 月已成功地将这一技术用于海湾战争：他们暗地里用一套带有“固化病毒”的微型芯片取代伊军进口用于控制和协调防空炮兵部队行动的计算机打印系统中的芯片，从而使伊拉克军队在海湾战争中丧失了对空防御作战的能力。伊朗布什尔核电站中，美国在德国西门子的控制卡件的硬件上植入病毒，报废了整个伊朗核设施的控制系统和设备，使伊朗核计划整整推后一年多。最近，美军研制的“计算机病毒枪”能从遥远的距离“送毒”上门，使敌方的指挥控制中心、飞机、坦克和舰艇中的电子系统“患病”。

1999 年某国有关部门发现，一旦联入国际互联网，CPU 奔腾Ⅲ芯片序列号功能会自动向 Intel 公司发回用户信息。奔腾系列的某种处理芯片也存在一种缺陷（bug），这种处理器对非法指令不作任何响应，而是直接导致死机。1997 年澳大利亚海军发现 Windows 95 会自主地向微软公司发送本机的配置信息。Windows 98 也预留了会泄露用户个人资料的“秘密通道”。微软公司的 IE 浏览器有能力在用户浏览域名时辨认出用户身份。另外，某版本 Windows NT 也存在一种缺陷，当计算机收到一个空数据包时，会导致不明的死机现象。就连 2001 年最新推出的 Windows XP 也存在类似的“后门”问题。

总之，在各种对计算机系统进行攻击的武器当中，与生俱来的计算机病毒、谈之色变的黑客攻击、防不胜防的计算机“后门”问题等，不仅严重危害着计算机系统的安全，而且对我国国防和国民经济的安全也构成了巨大威胁。各种计算机攻击武器如图 2.1 所示。

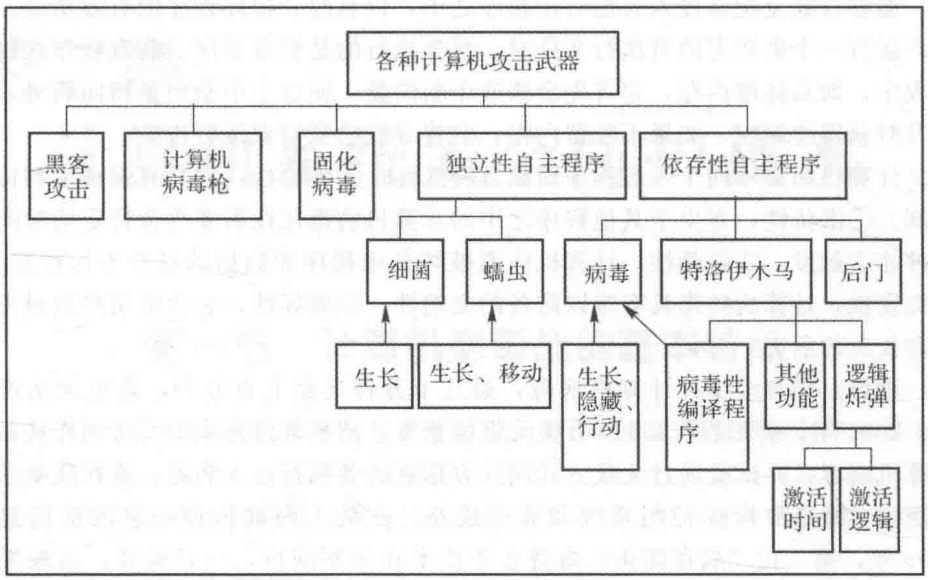

图 2.1　各种计算机攻击武器

1. 计算机病毒的严重危害

(1) 计算机病毒能直接攻击敌指挥信息系统。C^4ISR 系统是由成百上千台计算机和巨大的网络构成的，只要计算机病毒成功地攻击其中的某一部位或某个环节，就会使其无法正常工作，从而导致整个系统工作不畅。1995 年 9 月美军进行了一场代号为“联合勇士”的军事演习：一名年轻的上尉军官把从普通商店中购得的计算机和调制解调器与当地的互联网相联通，将有病毒的电子邮件发向一支海上舰队，不一会儿，一艘停泊在海面上的价值千万美元的军舰的指挥权就落入了他的手中，而舰长竟浑然不知。随着计算机病毒在各军舰计算机中的不断复制，海上的军舰一艘接一艘地拱手交出了指挥权，使整个舰队在一个人操纵的计算机面前不战而败。

(2) 计算机病毒可扰乱敌国国家经济。一位美国专家曾经说：“用计算机进行战争比用核武器进行战争更为有效。现在敌对国家若要摧毁美国，只需扰乱美国银行的计算机系统，几分钟就能盗走上千亿美元。这足以使美国的经济彻底崩溃。”1985 年 11 月 21 日，纽约银行的软件程序由于染上计算机病毒，该银行的电脑不能接受进账，却可以给所有账单付款，仅在那一天，纽约银行就短缺了 230 亿美元。

(3) 计算机病毒能破坏敌民用系统。现在各国的电信业、电力、银行和交通系统的庞大电子信息系统更易遭受计算机病毒的攻击，任何敌人对上述系统的攻击都会给该国带来巨大的损失。1998 年 11 月，美国康奈尔大学计算机专业研究

生莫里斯把自己研制的病毒注入计算机网络，使 8 500 台计算机陷入瘫痪，一半以上的计算机关机达 36 h。整个事件造成的经济损失不少于 9 700 万美元。

2. 计算机病毒的攻击方式

（1）无线方式。可以通过无线电把病毒码发射到敌方电子系统之中，这是计算机病毒战的最佳方式。可能的途径有：①通过通信频谱侦察、信道参数分析、通信格式剖析、通信密码破译等步骤，可直接对敌方电子系统的无线电接收器或设备发射病毒，使接收器对其进行处理并把它传染到目标机上。如计算机病毒枪，可发射带病毒的电磁波，使计算机程序错乱而丧失作战能力。美军声称，一支合格的计算机病毒枪就能使像“米格-29”那样世界一流的战斗机在 10 s 内变成一块空中废铁。②冒充合法无线传输数据。试验表明，只要事先掌握了敌方计算机系统之间的通信规则，就可以通过发射很高能量的电磁信号，利用敌方系统的各种接口、端口或缝隙，将计算机病毒程序注入其中。计算机病毒也可以冒充敌方计算机间的通信数据或程序，使接收方将其当作正确的内容接收下来，进入 C^4ISR 系统内部。③寻找敌电子信息系统防护最差的节点进行病毒注入，或通过敌方未加保护的数据链路将病毒传染到目标之中。

（2）有线方式。现在大部分的计算机系统是靠有线网络相互连接的，因此可以从民用网络的入口、敌有线网络的开口或与之相连的其他线路的开口直接将病毒注入线路上，使其扩散到与网络相连的众多计算机和传感器之中。

（3）“固化式”方式。由于目前全世界所有计算机系统使用的高功率芯片、集成电路板、显示器、不间断电源及通用软件等产品，大多是由少数几个发达国家生产制造的，他们完全有能力把计算机病毒预先设置或固化在产品当中。这些计算机病毒平时处于休眠状态，并不产生危害，但可以繁殖蔓延，使其他信息设备感染病毒。一旦爆发战争，只要向敌国的信息系统发射特定的无线电信号，就能激活病毒，使敌方信息系统和武器系统产生意想不到的故障而失效。

（4）借助于外围配套设备方式。在天线系统、电源系统、传感系统、驱动系统等这些直接与计算机相连的配套设备中注入病毒，也可以实现使病毒向主设备传播的目的。

（5）直接方式。即通过派遣间谍或买通敌方人员，直接把病毒传染到敌计算机系统当中。

第二节 计算机系统安全防护策略

计算机战属战术范畴，而且随着人类科技的发展和其关键技术的不断突破将愈演愈烈。它将逐步进入各国军队正规的战役作战序列，成为指挥控制战的重要组成部分，成为信息战的一种主要作战形式。