

# 论军事信息安全的特殊性

梅宪华

(南京政治学院上海分院, 上海 200433)

**摘要:** 军事信息安全是军队信息化建设的基础性工程, 与一般意义上的信息安全相比, 军事信息安全具有特殊性。把握军事信息安全的特殊性, 对于构建军事信息安全防范体系有着重要意义。

**关键词:** 信息安全; 军事信息安全; 国家安全; 信息战

**中图分类号:** E0-059 **文献标识码:** A **文章编号:** 1001-9774 (2006) 01-0087-03

随着我军信息化建设的发展, 军事信息安全问题日益凸显。如何从国家战略的高度构建军事信息安全防范体系, 已成为亟待解决的一个紧迫问题。本文从军事信息安全内涵、面临的威胁等方面分析其特殊性, 在此基础上就发达国家构建信息安全保障体系的主要做法作一梳理。

## 一、军事信息安全内涵的特殊性

随着信息网络的兴起与广泛应用, 信息安全问题已不仅仅是传统的信息保密, 还包括信息的完整性(即保证信息的来源、去向、内容真实无误)、不可否认性(即保证信息的发送和接收者无法否认自己所做过的操作行为), 以及可靠性(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早恢复正常)、可控性(即保证运营者对网络和信息系统有足够的控制和管理能力)、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。<sup>[1]</sup>可以说, 信息网络的普及应用, 深化了人们对信息安全内涵的认识。军事信息安全的内涵除了包含一般信息安全的共性, 还具有自身的特殊性。

第一, 严格的保密性。在很长一段时期, 信息的重要性常常与军事机密联系在一起, 信息安全就是保守军事秘密。随着世界新军事变革的蓬勃兴起,

各类信息系统在军队日益普及, 并渗透到军事领域的各个方面, 对军事信息的产生、承载、传播的方式和途径产生了革命性影响。由于海量的军事信息储存在“盘”内、流动在网上、传播于空中, 从而使泄密的隐患和漏洞大为增加, 造成的危害也越来越大。以抵御技术侦察与破坏, 保护涉密信息与信息系统安全, 防止窃密、泄密为主要目的的信息安全保密, 不可避免地成为军事信息安全中的核心内容。做好信息安全保密, 成为我军积极应对新军事变革挑战的客观要求。

第二, 地位的战略性和价值的广泛性。信息时代, 信息资源在社会资源中的地位、作用和价值越来越大, 国家的发展和人们生活水平的提高, 越来越取决于对信息资源的开发、控制、利用和保护。信息作为特殊的战略资源, 与国家利益、民族尊严息息相关。同时, 信息也成为军事力量构成的关键要素, 成为直接的、决定性的作战要素。信息不仅是一种作战手段, 而且是战斗力的倍增器。部队战斗力的形成和发挥以及实施有效的指挥和控制, 依赖于信息的获取、处理、传输、控制和使用。交战双方紧紧围绕争夺信息优势而展开行动, 采取一切手段利用、瘫痪和破坏对方的信息系统; 同时, 又千方百计地保护己方的信息系统。由此, 信息争夺、信息控制已经突破传统范围, 一跃上升为综合国力、军事实力间的较量。

第三, 超强的技术性。在高技术群的支撑下, 信

收稿日期: 2005-11-17

作者简介: 梅宪华(1954—), 男, 江西南昌人, 南京政治学院上海分院军事信息管理系副教授。

息网络技术以前所未有的广度和深度向战争诸要素渗透,极大地改变着现代高技术战争的物质基础和战斗力的技术构成,使战争形态、作战样式、战斗力性质实现了从机械化向信息化的质的飞跃。由于信息优势决定了作战的主动权,进而成为战争制胜的决定性因素,为夺取制信息权,取得信息优势,必须首先在信息技术上取得优势地位,这样才能确保在有效打击敌方的同时,有效地保护己方。因此,各国为保障军事信息安全,都把信息技术列为最核心、最关键的技术。

## 二、军事信息安全面临的挑战与威胁

同一般信息安全一样,网络环境下影响军事信息安全的因素,包括黑客入侵、病毒破坏、逻辑炸弹及因自身失误、恶意访问、信息泄密、服务干扰、网络固有缺陷等等。但同时,军事信息安全面临的威胁又具有特殊性。

第一,由信息窃取带来的威胁。在信息化战争形态下,夺取并保持信息优势,成为打赢信息化战争的基础和保证。现代高技术局部战争表明,通过攻击敌方的信息系统,可以直接影响甚至破坏敌方的指挥决策。“发现即意味着摧毁”,重要信息一旦被泄露,就有可能遭受毁灭性打击。因此,对军事信息安全构成的威胁既包括利用传统的手段窃取军事信息,又包括对信息网络的攻击。目前我国信息基础设施的网络、硬件、软件等产品几乎完全建立在外国的核心技术上,这些核心技术和专用设备往往存在着严重的安全隐患,而且在诸多已建成的信息系统中普遍缺乏安全机制、防范措施和自卫能力,给我军信息安全带来了严峻挑战。

第二,由主动攻击带来的威胁。对军事信息安全构成最危险的威胁是以获取军事信息或破坏军事信息系统为目的,针对计算机网络信息系统而实施的主动攻击。计算机信息网络是现代战争中实施远程打击、精确制导、预警防空、反潜反舰、电子对抗、侦察、定位、指挥、通信等领域必不可少的信息系统基础设施。因此,在信息化战争中,信息网络必然是敌方精确打击和信息攻击的首要目标。目前外军已经研制出具有超强破坏能力的计算机病毒、芯片病毒固化技术和计算机病毒无线输送装备,正在研究以无线电方式、卫星辐射注入方式,将病毒植入计算机或各类传感器、网桥中。同时,一些国家不但成立了专门的信息作战部队,而且还在国内外招聘了大量黑客。另外,用于主动攻击的网络入侵技术手段也向综合化、复杂化发展,快速寻找网络漏洞,通过网络连接安全薄弱部件,对信息网络进行破坏的能力不断提高。在

信息对抗“不对称”条件下,落后一方的信息网络会出现防护失效、性能降低等问题,从而失去制信息权。

第三,由信息战带来的威胁。信息战已成为信息时代的主要作战样式,并成为信息时代军事信息安全面临的最大威胁。信息战要求在信息的占有量、获取信息和鉴别信息能力、利用信息能力以及信息的对抗能力上获得优势。由于信息战的重要地位,世界各主要国家都把发展信息战能力作为国家安全战略和军事战略的重点,特别是重点开发计算机网络攻防武器和手段。美国从20世纪80年代初期就开始研究以计算机网络攻防对抗为中心的信息战,并将信息战作为夺取信息优势进而在21世纪继续保持军事优势的关键要素。俄罗斯将信息战置于仅次于核战争的重要位置,其《1996~2000年行动计划》强调,在适当保持核潜力的同时,把注意力放在广泛开发信息战手段上<sup>[2]</sup>。以摧毁敌方重要信息网络、保护己方重要信息网络为目标的信息战的出现,凸显了军事信息安全的极端重要性。

## 三、发达国家构建军事信息安全保障体系的主要做法

近年来,世界各国尤其是发达国家为切实保障军事信息安全,高度重视军事信息安全保障体系方面的构建,其主要做法是:

第一,从国家战略的高度,制定军事信息安全的战略规划。鉴于军事信息安全直接关系到国家安全,世界各国在构建军事信息安全保障体系时,都将其纳入国家战略体系中加以研究并制定信息安全的国家战略规划,以指导军事信息安全保障体系建设。美国自20世纪80年代以来,从信息战的高度对军事信息安全问题进行了大规模、有组织的研究,形成了系统的信息安全和信息战理论。在此基础上,美国制定了一系列信息安全国家战略规划,如《关于通信和自动化信息系统安全的国家政策》(即NSDD-145,1984年9月17日)、《联邦政府信息资源管理通告》(即A-130通告,1985年12月)、《信息安全发展战略与发展计划》(2000年)、《信息时代保护关键基础设施的行政命令》(2001年10月16日)、《国防信息保障纲要》以及《信息保障技术框架》(1998年)等。2002年,美国政府提出未来美国网络安全领域的十大重要措施,其中重要一项即制订《保护Cyberspace安全的国家战略》。俄罗斯自20世纪90年代初即关注信息安全问题,此后,俄安全会议组织有关部门专家、学者着手制定俄联邦信息安全学说,并于2000年出台了作为信息安全国家战略规划《国家信息安全学说》。

英、法、德等国均非常重视从国家战略的高度,研究军事信息安全问题并制定有关的国家战略规划。

第二,加强立法,制定专门的军事信息安全法规。军事信息安全保障的重要性及其复杂性,决定了必须制定专门的法律规范。世界各国都十分重视通过立法保障军事信息安全。自20世纪80年代以来,美军在国家信息安全法律体系框架下,先后制定了一系列信息安全的军事法规、条例、操作规程和技术标准。美国陆军1996年8月颁布的FM-6号野战条令《信息作战》,成为美军指导信息战的“纲领性文件”,其中对信息安全工作提出了具体要求。此外,《陆军信息资源管理方案》、《陆军部信息安全方案》、《美国陆军通讯电子操作指导方案》、《通讯安全管理》、《信息系统安全》、《信息系统安全管理》、《国防部信息安全方案》等一系列条例,为美军全面加强信息安全工作提供了统一的法规依据。特别是《美军信息安全管理条例》,明确提出了军事信息安全面临的主要威胁,并对军事信息安全等级进行了划分,详细规定了各等级军事信息安全保障的措施和法律责任。俄罗斯关于军事信息安全的政策法规,以国家有关信息安全的政策法规为基础。1995年,俄罗斯颁布了《联邦信息、信息化和信息保护法》,强调国家在建立信息资源和信息化中的责任是“旨在为完成俄联邦社会和经济发展的战略、战役任务,提供高效益、高质量的信息保障创造条件”。法规中明确界定了信息资源开放和保密的范畴,提出了保护信息的法律责任。1997年出台的《俄罗斯国家安全构想》强调了信息安全对于国家安全的重要性<sup>[3]</sup>;2000年,普京总统批准的《国家信息安全学说》,对军事信息安全问题作了全面阐述,提出了保障军事信息安全的具体措施。在《国家信息安全学说》等国家信息安全政策法规框架体系下,俄罗斯军方制定了一系列法规、条令等,构成了军事信息安全的法律保障体系<sup>[4]</sup>。

第三,成立专门的军事组织机构,加强军事信息安全保障的制度建设。为切实维护军事信息安全,发达国家依据有关军事法规,着眼于制度建设,设置了专门的军事信息安全组织机构。美军依据《信息安全条例》的规定,建立了职责明确的信息系统安全管理专门机构。其中,国防部下属的国家安全局负责“国家安全系统”的信息安全工作,包括涉及情报(intelligence)活动的信息安全、涉及与国家安全有关的隐蔽(crypto-logic)活动的信息安全、涉及军队指挥与控制、涉及武器和武器系统的设备或对于完成军事任务至关重要的设备等。此外,美国还先后成立了国家信息战预警中心、国家安全委员会的“国家信息基础设

施安全保护办公室”,分别负责战略目标和全国信息系统的安全防护工作。2002年,美国国防部将原来的航天司令部和战略司令部合二为一,成立了新的战略司令部,负责计算机网络对抗、C<sup>4</sup>ISR保密系统管理、导弹防御和全球作战计划。美国国防部还成立了“网络信息安全司令部”,负责三军网络安全防护的总体指导、规划与监督。在陆军一级司令部和陆军部长助理办公室设有信息系统安全计划管理人,下属机关以至基层单位分别设有信息系统安全管理员,具体负责其相应层次的系统、网络、中继站、工作站、计算机群,乃至每台计算机和每个终端接口的安全。海军成立了“空间和信息战指挥与控制局”和“网络战司令部”,加强对海军网络系统的规范、监视和控制,统一协调情报技术、情报处理、空间需求和信息安全问题。空军成立了“网络危险评估小组”,设立互联网保密监审专员。现在,美军已形成了“自上而下、分区划片”的网络防护管理体制<sup>[5]</sup>。

第四,加强信息网络与信息技术研究,确保信息优势。军事信息安全保障体系建设,法规、管理与技术三者缺一不可,技术在其中具有举足轻重的作用。为取得信息优势,夺取制信息权,必须首先在信息技术上具有优势地位。为此,发达国家军队纷纷加强了信息技术的研究,包括加强C<sup>4</sup>ISR保密系统建设;研究各种新技术在加密和破译能力方面的应用;开发检测和抵御网络攻击的智能软件系统;研制和改进保密终端,等等<sup>[5]</sup>。

信息安全问题是全球性的问题。尤其在信息战的影响下,军事信息安全决定着国防与军队战斗力,决定着国家的安全状态。我们必须切实把维护军事信息安全放到保护国家安全、保障军队建设、保证战争胜利的战略高度来认识,加快军事信息安全保障体系的建设,以确保我军在未来信息战中能够克敌制胜。

〔责任编辑 杜永吉〕

#### 参考文献:

- [1]杨义先,林晓东,邢育森.信息安全综论[J].电信科学,1997,13(12):2-5.
- [2]孙永强.信息战与计算机网络攻防[N].科技日报,2000-08-24(4).
- [3]宫小雄,公晓燕.俄罗斯〈国家信息安全学说〉刍议[J].现代国际关系,2000,(8):28-30.
- [4]胡慧平.美、日、俄信息安全的政策保障[J].中国信息报,2003,(2):50-51.
- [5]周保太.2002年回顾:外军信息安全发展综述[EB].  
<http://www.syt.edu.cn/gwwq/cankao/zb801.html>.