

论我国军事信息安全法规建设

沈 杰

(武警杭州士官学校 训练部,浙江 杭州 310023)

[摘要] 信息技术的迅猛发展及其在军事领域的广泛应用,使信息成为影响战斗力发挥乃至决定战争胜负的关键因素,以军事信息安全为核心的斗争也日趋激烈。当前,我军正处于信息化建设和加速发展的关键时期,应及早做好军事信息安全建设规划,筑牢军事信息安全的防线,确保军事信息领域的绝对安全。

[关键词] 军事;信息安全;法规

[中图分类号] E25 **[文献标识码]** A **[文章编号]** 1003-4145[2014]专辑-0103-02

军事信息安全法规是由国家或军队权威部门制定的与军事信息安全相关的条例和规范。军事信息安全建设,不仅需要各种先进的技术措施来保障,还需要借助技术之外的具有强制性的法律手段来保障。因此,必须制定和完善军事信息安全标准和法规,通过立法手段加强军事信息安全管理,规范和促进军事信息安全建设,使军事信息安全工作有章可循,为军事信息安全建设健康有序发展提供有力的法律依据。

一、建立和完善我军信息安全法规

“凡兵,制必先定;制先定,则士不乱;士不乱,则刑乃明”。这是《尉缭子·制谈》中对制度与军队建设的深刻认识。信息化社会,信息已经成为重要的战略资源,信息能力是构成国家战争潜力和军队战斗力的重要因素,未来战争取胜的关键是夺取制信息权,即限制和剥夺敌方控制和利用信息的能力,同时保障己方信息活动的自由。

(一) 要尽快建立军队信息安全标准体系

学习和借鉴发达国家在信息安全立法方面的成功经验和做法,加快信息安全法制化进程,抓紧制定信息安全管理和技术标准以及配套实施办法,逐步建立与国家标准相衔接、适应军事斗争需要的军队信息安全标准体系。在充分考虑我军实际情况的基础上,应根据新的形势和任务需要,在健全配套国家信息安全相关法规的基础上,制定军事信息安全法规,特别要针对军事信息安全技术性、专业性强的特点,在建立和完善管理法规的同时,制定和完善相关的使用规程。

(二) 要加强标准建设的规划和组织

健全军队信息安全标准管理组织,加强标准建设的规划和组织,对制定和完善我军信息安全法规非常重要。大力抓好信息安全标准的贯彻实施,充分发挥其基础性、规范性和强制性作用。我军近年来十分重视信息安全立法工作,初步形成了我军信息安全法规体系。近年来,先后制定颁发了一系列信息安全法规,主要有《中国人民解放军信息安全保密条例》《中国人民解放军计算机信息系统安全保密规定》《中国人民解放军核心密码管理规定》《关于加强情报保密的规定》《关于军队涉外通信问题的规定》等,还有四总部各部门制定的有关涉及信息安全的规章制度等,都要督导落实,抓出成效。

(三) 要充实完善新的信息安全法规体系

虽然我军在信息安全法规制度的建设方面已经形成了一个比较好的基础,但是与迅猛发展的信息化进程相比,已有的这些信息安全法规制度,尚不足以覆盖信息安全的方方面面,难以完全满足新形势下信息安全的客观需求。比如,针对我军军事训练转型期训练信息网的深入扩大,有必要进一步规范全军军事训练信息安全暂行规定、军事训练信息安全 IP 地址申请管理暂行办法、军事训练信息安全网域名注册管理暂行办法、军事训练信息安全网运行管理工作制度、军事训练信息安全网设备预检维护工作制度、军事训练信息网信息安全管理中心机房工作制度等。此外,还应当进一步完善信息安全法规制度的建设,凡属信息安全所需要的法规制度,应当按照急事急办的原则,抓紧研究拟制,不断建立和完善法规制度。

二、依法实施军事信息安全的监督检查

信息安全监督检查,是指各级信息安全主管部门按照依法行政的职责要求,以有关法规、标准为依据,采用一定的形式和手段(包括技术手段),调查了解所属的涉密单位及其人员是否履行维护信息安全的义务和责任,检验衡量有关的具体行为是否符合安全要求并督促其落实信息安全法规的一种活动。在新的环境和新的形势下,做好信息安全监督和检查是维护信息

收稿日期:2014-05-10

作者简介:沈杰(1972-)男,浙江绍兴人,武警杭州士官学校训练部教授,研究方向:信息系统管理、计算机及应用。

安全的重要措施和有效手段,更加要求加大监督检查力度,全军所有单位和人员必须接受信息安全部门依法实施的监督检查。

(一) 健全保密监督检查机制

在原有信息安全监督机构下,建立健全信息安全监督领导小组,完善严格的信息安全监督检查手段和检查标准,提高发现信息安全方面存在问题的能力和规范化水平,主要检查信息安全工作方针、政策的贯彻落实情况,检查官兵的信息安全意识及对相关知识的掌握程度,检查法规制度的贯彻执行情况,检查组织领导机构的落实及其建设情况,检查信息传递、处理、存储设施的配置和环境的安全情况,检查有无失、泄密事件的发生及其对失、泄密事件的查处情况等。及时发现和消除隐患漏洞,问题严重的要责令整改,必要时信息安全部门可采取强制处置措施。

(二) 加大执法监督力度

目前,我军出现的军事信息内部泄密事件大都是由于法规执行不严、监督不力造成的,必须认真贯彻各项法规,严格按照法规的要求约束、规范人们在军事信息活动中的行为。各军事主管单位要结合本单位实际,突出重点,及时完善信息安全规章制度和防范措施,把军事信息安全的各项法规落到实处。同时,要采用分级管理的方法,即区分军事信息、信息系统、涉密人员等环节对信息安全影响的重要程度,对重要的信息、系统、涉密人、涉密载体以及物理环境等,加强信息安全防护,提高信息安全管理等级,进而从制度上明确区分不同信息安全级别的保护方式和保护程度。

(三) 严格奖惩和监督监察制度

信息安全监督检查部门与政法机关要加强协作,进一步明确违规、泄密行为的法律责任及追究办法。要根据信息安全事件造成损失的大小来确定向上问责的级别以及行政问责的方式、内容、程序和尺度;要畅通泄密举报渠道,充分发挥群众监督作用;要严格执法执纪监督,依法严办泄密案件,要实行问责制,做到有漏必查、有责必问、有错必究,要做到对违反信息安全法规的个人和单位,严格按照规定进行处理,消除在信息安全方面的侥幸心理,进而形成以军事行政主官为重点的军事信息安全问责制度。

三、强化官兵严守信息安全法规的意识

随着信息获取技术越来越发达,信道越来越流畅,人们获取的信息越来越多,速度越来越快。信息来源上更为广泛,新技术使信息以前所未有的速度传播。通过现代化传播手段,几乎不受任何限制把信息有效地传到世界各国,具有非常强大的穿透力和自由度。然而,军事信息网络的规划与建设、运行与管理、数据的收集与存储以及军事信息的获取、传输、处理、使用的各个环节均可能涉及信息安全问题,甚至少数官兵因不懂军事信息安全法规而侵犯军事信息系统的各种资源包括硬件、软件、系统中存储和传输的数据而犯罪。因此,在完善法规建设的同时,要不断强化官兵严守信息安全法规的意识。

(一) 要加强舆论宣传引导

军队应采取综合措施,在建立和完善有关信息领域的法律和道德规范准则的基础上,在拓展信息获取空间和传递自身信息的同时,筛选和梳理所获得信息,剔除和拒绝破坏型信息,弘扬国家和民族思想文化,确保自身最大限度地利用有效信息,维护国家独立和民族特色。在特定的地点、时间、环境等条件下,为了维护国家利益,使传媒有利于己方,应对媒体加强控制,防止因传媒的滥用造成混乱,甚至被敌方利用。

(二) 要广泛开展信息安全教育

通过开展深入持久的信息安全教育,不断提高官兵的信息安全意识,使全体官兵充分认识到维护信息安全是自己的职责和义务,树立敌情观念、纪律观念和法制观念,形成自觉维护军事信息安全的良好风尚,使广大官兵充分认清新形势下加强军事信息安全工作的重大意义和艰巨任务,以及当前军事信息安全面临的复杂环境和严峻挑战,明确保证军事信息安全的重要性和我们肩负的重大责任。通过教育,提高官兵信息安全知识水平,了解掌握安全保密基本技能,使官兵既有强烈的信息安全意识,又具备过硬的计算机应用和信息安全保密技术,防止出现因知识缺乏和技能不精造成的泄密,增强官兵的信息安全防范能力。

(三) 要建立传媒监督机制

包括制定新闻工作者的行为准则,监督其遵守情况,审查上传媒体原始材料,并建立执法机构来惩罚违规者,单位个人应该有选择地摄取信息,抵御具有危害性的信息侵蚀;树立保卫国家信息疆域和信息边界的观念,自觉筑起无形的精神防线,维护国家信息主权的尊严。四要通过正规院校进行信息安全培训。全军院校要开设信息安全与保密课程,开展专业教学,规范教育内容、目标和要求,区分教育层次,突出重点对象,逐步实行分类施教,注重利用信息失密案例搞好教育,大力宣传信息安全与保密工作的政策、法规;中高级干部培训要把信息安全与保密知识作为必修内容;保密工作部门要加强对重要涉密岗位人员的教育;要加强对重要涉密人员的保密管理,选拔领导干部和选调机关工作人员,要把信息安全素质作为必备条件。对进入重要涉密岗位的人员要严格审查,发生过泄密问题的人员,不得安排在涉及信息安全的重要岗位工作。

(责任编辑:宋绪芬)