俄罗斯国家和军队信息安全建设概况

王 峰 陈 君*

苏联解体、俄罗斯地缘政治潜力削弱和当代几场武装冲突的进程与结局，使俄罗斯当局清醒地认识到信息安全不仅具有重要的地缘政治意义，而且关系到国家的战略发展和生死存亡。针对自身所面对的国内外复杂、严峻的信息安全形势，俄罗斯近年来采取了一系列综合措施，不断加强国家和军队的信息安全建设，以应对不断变化的信息安全挑战。*

一、俄罗斯国家和军队信息安全形势

近年来，俄罗斯国家和军队信息化建设发展迅速，以计算机为中心的军队 C4I系统已经得到普遍装备和应用，大大提高了作战指挥、教育训练和各种勤务保障水平。与此同时，随着全球信息化的迅猛发展，国家和军队建设对计算机网络及相关设备的依赖性日益增强，人们接触到的各种社会心理诱惑也急剧增加，俄罗斯国家和军队在信息技术安全和信息心理安全防护方面的问题日显突出。

(一)国际环境带来严重威胁。俄罗斯认为，在信息安全保密方面来自国外的威胁十分严重，主要包括：一是以美国为首的一些西方国家在全球信息监测和信息传输，以及高新信息技术的推广方面对俄采取不友好政策，阻碍了俄罗斯平等加入全球信息化体系的进程。二是发达国家的信息化建设起步较早，对信息化重要性认识深刻，高新技术侦察系统的研究和开发速度较快，信息处理自动化水平较高，技术侦察和电讯密码分析人才队伍健全，使技术侦察和情报信息分析能力较以前有了很大的提高，给俄罗斯信息安全造成了直接的威胁。三是俄罗斯仍是世界各国侦察机构侦察活动的众矢之的，虽然冷战后国际形势有一定程度的缓和，但一些西方国家针对俄罗斯使用具有多功能全球侦察能力的地面、海洋、空中、宇宙等各种系统装置的侦察活动空前活跃。四是一些国际集团、政治和经济等组织，采取舆论攻击、心理瓦解、金钱诱惑等多种手段不断对俄罗斯进行信息窃取活动。

(二)信息安全体系遭到破坏。苏联解体带来的政治和经济结构的急剧变化，使俄原本完整、庞大的信息安全体系遭到破坏，国内研究信息化设备和信息保护设施的机构经过多次变动后，相关的科研机构和生产部门遭到不同程度的破坏，机构间整体协调性降低，企业生产能力持续下滑，大批专业技术人才流失。由于信息技术和工艺落后，信息安全方面的大部分软硬件设备不能完全自主生产，再加上俄在发展信息基础设施和研制信息产品方面不断扩大国际合作，造成不加保护地广泛使用国外生产的信息技术和安全防护设备。目前，俄国家和军队重要机构在信息通讯方面主要依赖于外国的计算机和电视网络技术设备，很大一部分机密信息完全靠西方国家的信息技术收集、存储和发布，以前研制和装备的保密设备不能适应新形势和新情况，尚不能生产具有足够信息防护能力的设备，就连总统出访时携带的通讯和保密设备也已十分陈旧。

(三)信息安全的机制法规不够健全。俄罗斯建国初期军政领导人没有像美国等西方领导人那样，对国家和军队信息化、信息对抗、信息安全保障等问题给予高度重视，只是到了 20世纪 90年代中后期，在作为高技术基础的国家电子工业遭到惨重损失后，才下达制定和执行国家和军队信息安全保障构想的任务。但由于起步晚、任务紧，缺乏足够的组织和资金支持，信息安全保障构想又被放到了次要位置，导致信息安全建设的内部机制不尽完善，信息安全防护的法规和标准尚不完备，信息安全防护

* 作者单位：解放军 61565部队（翻译），牡丹江师范学院（讲师）。

方面的管理体制、人才培养、队伍建设与迅速发展的形势和现代战争的要求也不相适应。

(四)信息心理安全建设薄弱。俄罗斯在对国家原有行政管理系统进行改革的基础上,建立以民主、法治和信息公开为原则的新国家体制的过程中,激化了扩大信息自由交换和必须限制某些信息流通之间的矛盾。随着自由经济区和外企的增加,外国驻俄机构和人员不断增多,某些敌对势力利用俄罗斯媒体与文献公开报导和出版范围扩大等现实条件,向其传播、渗透西方的思想、文化和价值观,进行国家精神文化扩张,企图改变和破坏其国家的道德观念。俄学者认为,忽视国家信息心理安全保障,是俄罗斯在同西方进行地缘政治角逐的"冷战"中失败的重要原因之一。一些人员信息安全保密观念淡薄,保密知识缺乏,极易造成无意识泄密。如苏联解体以后,一批掌握国家政治、经济、科技机密的人才迫于生活压力和事业发展的需要,相继移民西方国家;一些曾在重要军事设施和秘密指挥机关服役的军官及前苏联克格勃成员,也陆续到北约国家谋生,造成大量军事、经济机密外泄。

二、俄罗斯国家和军队信息安全建设措施

(一)确立信息安全国家发展战略,完善信息安全政策法规和理论研究。面对全球信息化迅猛发展过程中存在的信息安全风险给国家和军队利益带来的严重威胁,俄罗斯从自身实际出发,有计划、有步骤地制定和确定了与本国国情和最大利益相适应的信息安全发展战略。1995年,俄罗斯宪法把信息安全纳入国家安全管理范围,颁布了《联邦信息、信息化和信息保护法》,为提供高效益、高质量的信息保障创造条件,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。1996年,修订后的《俄联邦刑法典》明确界定了计算机信息领域的犯罪。1997年,俄罗斯出台《国家安全构想》,特别强调"信息安全是重中之重"。2000年9月12日,普京总统批准了《国家信息安全学说》,明确了联邦信息安全建设的目的、任务、原则和主要内容,为俄"构筑未来国家信息政策大厦"奠定了基础,为对抗外国向俄罗斯政治、经济、军事等领域的信息情报渗透起到指导作用。[1] 至此,俄罗斯信息安全国家战略正式确立。此后,俄罗斯相继出台了一系列信息安全方面的政策、法规:总统信息署和联邦安全委员会制定了《保障俄罗斯联邦主体信息安全政策框架》,2001年出台了《俄联邦信息和信息化领域立法发展构想》,明确了5—10年的立法内容。同年1月出台了《2002—2010年俄罗斯信息化发展目标纲要》。2002年4月21日,发布第368号政府令,规定联邦办公室自动化系统必须使用俄罗斯智能卡。2003年又启动了《2001—2007年俄罗斯关于建立和发展国家行政机关专用通信系统的联邦专项规划》。信息安全方面的相关法规措施还包括:《产品和服务台认证法》、《国家秘密法》、《参与国际信息交流法》、《信息保护设备认证法》、《有关遵守加密设备的研制、生产、实现和应用以及提供加密信息领域服务的合法性措施》等。[2]

在逐渐完善信息安全政策法规的同时,俄罗斯国家和军队针对信息安全方面展开了系统的有针对性的理论研究,并在2004年进一步明确了信息安全保障体系的优先发展方向:发展信息安全保障体系,研究信息理论和实践;改进并研制新的信息安全保障方法和手段;改进并建立新的信息保护法律标准;改进信息安全机制;建立信息安全分析模型和方法,评估信息保护等级和信息安全的完整性;发展信息质量管理系统,改进监控方法和手段。同时,加快了信息安全理论的转变,到2003年底,俄罗斯基本完成了从传统只重视密码设备和安防产品到传统与非传统安全并重的转变,形成由涅尔科安全企业集团、诺瓦股份公司和欧亚协会等巨头为龙头的信息安全产业群。

(二)建立健全信息安全管理机构,改进信息安全制度和强化防范措施。为了有效保障信息化建设过程中的信息安全,统一领导和协调信息安全保障

[1] À¼ÄÂº¿±°¿ÆÀÂ¾±º À¿¿À» [2] ¶ ÀÁ±¿ÀÃÃº ÀÃÃº »Ã¼À» ¶µ¶Â±°° ÁÂ¶µÃÃ±½Ñ¶Á ÃÀ²À» ÃÀ³À¼ÁÁ¿ÀÃÃÎ ÀÆº È° ±Í¿Í Ç ³¹½Ñµ À³ ¿±È½º, ¹±Ê°, ÁÂº ¿È° ÁÍ º ÀÃ¿À³¿Í¶ ¿±Â±½¶¿°Ñ À²¶ÃÁ¶É¶¿°Ñ °¿ÆÀÂ¾±º À¿¿À» [2] ¶ÀÁ±¿ÀÃÃº ÀÃÃº »Ã¼À» ¶µ¶Â±°°, http //www. nasledie. ru/politvnt/19 – 35/article. php? art= 22

[2] °¶Â¶É¶¿Î ¿ÀÂ¾±º³¿ÍÇ µÀ¼Â¾¶¿ÄÀ³, Â¶´½±¶¿Ä° ÂÐË°Ç µ¶ÑÄ¶²Î¿ÀÃÃÎ ³ À²½±Ã° ¹±° °ÃÍ °¿ÆÀÂ¾±°°, http //mirash. ru/dokj/55. doc

部门的活动,俄首先在联邦安全会议构架内组建了联邦信息安全与战略规划局,之后又在联邦各主体和军队内建立了信息安全领导机构。信息安全领导机构在组织形式上既能在平时充分履行职能,又能在战争爆发时快速转入战时体制并发挥作用;在机构职能上,既能对全军信息安全工作进行战略指导和宏观管理,又能对信息安全的具体问题进行策略支持和微观控制。同时,俄罗斯强化了政府通信和情报局、总参情报侦察局、联邦安全局、对外情报总局和国家科技委员会等情报部门在网络与信息安全管理方面的职能。其中,政府通信和情报局主要由原苏联克格勃负责密码和通讯的第 8局、负责窃听的第 12局和负责信号情报的第 16局演变而来。该局人员为现役军人和文职人员,包括语言学家、数学家、密码研制和破译人员、计算机“黑客”及各类安全专家和技术人员,承担着国家和军队要害部门的通信保密、密码处理、破译以及信号情报等任务,并在俄罗斯信息安全设备(包括密码设备)的研制、生产、销售、应用、装配、调试、检验与进出口中拥有认证与许可权。2003年 3月 11日,根据普京总统令,该局被撤销,其密码与认证等大部分职能都归转到俄联邦安全局。[1]

在建立健全信息安全管理机构的同时,俄罗斯建立了多种信息安全制度:(1)强制认证制度。俄罗斯对信息安全企业和产品实行许可认证制度,建有专门的认证机构和实验室;安全等级分为 A、B、C、D、E五个等级;重要系统不使用国外产品;坚持自己标准的同时也考虑与国际标准的兼容,如 CC标准等。(2)国家干预和调控制度。俄在信息安全技术市场上实行国家干预和调控,保证优先发展特种信息保护设备和保护国家机密的手段,将信息保护设备分为四类:信息流失通道显示设备、信息保护设备、信息监控设备和移动信息保护技术,并加紧研制新一代信息保护特种设备,其中包括:信息压缩积聚设备、信息形式掩蔽设备、灾难恢复与备份设备、信息分析诊断设备和技术侦察跟踪设备等。(3)数据恢复与备份制度。注重数据的灾难恢复和备份工作,规定将信息传输中数据完整性要求放在首位,经常进行不同地点的数据备份,在全俄大力普及、推广和应用最新的应对灾难恢复的软件产品。(4)网络信息检查制度。建立个人非法使用信息的闭锁系统,允许对经由因特网传播的信息进行监督检查。(5)安全评估制度。俄信息安全部门制定了计算机系统安全评估标准(橙黄皮书)、产品安全评估软件、特殊环境下计算机系统安全评估标准使用指南(黄皮书)、安全网络计算机系统安全评估标准说明、安全数据库(虹霓系列)等一系列比较完善的系统安全评估指标。

为加强对信息安全的领导,俄还采取了许多重要举措:(1)增加对信息产业的投入和扶持,包括:增加对国家和军队信息化建设关键领域的拨款;拓宽预算外经费来源;在“谁投资谁受益”的原则基础上开展跨部门协作,并实行国家及其军队的信息安全防护经济独立核算原则;在“经济核算和自负盈亏”基础上通过超计划的科研工作、试验设计及举行招商会、展览会等方式加强技术基础,用商业行为聚集信息设备资源。(2)发展全军乃至俄罗斯统一的信息空间设施,同时为联邦国家权力机关、联邦各主体国家权力机关,特别是军事安全系统建立专用的信息传输系统,确保国家在研究和使用国防用途信息传输系统方面保持技术上的独立性。(3)研究并建立通过国家大众传媒提高国家领导和军队指挥控制系统效率,以及实施国家和军队信息政策的机制。(4)保护国家关税,从政策上支持国内信息安全技术的开发者,保护国内市场,避免对手的信息武器对国内市场的渗透。(5)倡导根据国际法签订一系列协定,以确保平等参加政治、经济、军事和生态进程的全球监视网(比如国际信息处理联合会和各地域性的信息技术学术组织每年都召开各式各样的信息安全会议,研究和交流信息安全问题等),为加强国际间合作和各国的安全作出现实的贡献。(6)规范自动化管理系统、通用和专用信息传输系统信息化及信息安全保障方面的国家标准。(7)增强公民的法律观念和维护国家信息安全的自觉性,提高其计算机和网络专业技术水平,消除计算机犯罪。(8)加强信息心理安全保障措施,降低敌方信息心

[1] “国外信息安全建设情况综述”, http://www.itsec.gov.cn/zxzz/lwt/513.htm

理战效果。俄联邦安全会议(首先是信息安全与战略规划局)、联邦国防会议、武装力量总参谋部一起制定“武装力量心理安全保障的总体规划”,确保部队经常性地接受信息教育,使其养成抵御消极信息作用所必需的精神心理和战斗素养:长期跟踪和评估全体军人的精神心理状况,预测可能发生的敌方信息心理作用,并及时作出告警;研究国外大众传媒针对俄军队和居民信息流的规律和方向性;加强对新闻媒体和信息机构的控制,预防并切断各种传闻和恐慌情绪,直至在必要时对士气沮丧的军人实施隔离;提高并保持对国家和军队机密的警惕性;搜集有关敌方信息对抗的信息,为信息安全防护提供信息支持。

(三)发展信息安全防护技术方法,自主研发信息安全保密系统和设备。俄罗斯在发展信息安全技术上强调自主创新、坚持自成体系,强调数学模型与论证,发挥控制理论作用,注重芯片和操作系统的研发,把“为联邦国家权力机关、联邦各主体国家权力机关、军事安全系统建立专用的信息传输系统及其信息防护设备,特别是将确保国家在研究和使用国防用途的信息系统及其防护设备方面保持技术上的独立性作为国家军事政治和战略潜力的组成部分,列入长期发展计划和重要科研课题”。圣彼得堡技术大学研制成自主安全内核的高安全等级操作系统,不受病毒和黑客侵犯,在与国外产品兼容上只局限于外层的功能调用。在财政金融系统,俄积极推广使用现代化的有保护的信息技术和网络技术,采用俄自己研制的电子数字签名及其他保护设备。据称,俄罗斯研制的智能卡(RIK)保密性可靠、操作简便、抗攻击性强,能满足信息系统对安全的诸多要求。[1]

为完善信息防护设备研制的组织和工艺,俄罗斯采取了一系列综合措施:对现有设备进行重新清理,减少设备的种类和型号;为信息设备研究人员提供最先进的计算机设备和共用软件,提供随时利用全球信息资源的条件;采取“管理程序重新设计”法提高信息系统的研制工艺;建立相应的抑制手段,包括发现和使用信息武器的技术及其独特的早期预防系统;完善和发展新的技术手段,防止机密信息网络被非法侵入,防止重要信息的流失,防止它们被破坏、删除、歪曲和拦截;研究和发展反控制信息技术。

俄军也正在加紧研究一系列信息安全防护技术:一是信息加密、信息鉴别以及防干扰、防辐射、防侦察、防摧毁、防网络入侵、防计算机病毒等“早期预防技术”;二是网络侦察技术、信息检测技术、风险管理技术、测试评估技术和计算机信息电磁泄漏(TEMPEST)技术;三是形成“杀手锏”的战略性技术,如操作系统、密码专用芯片和安全处理器等。为解决军队的信息安全防护问题,俄正在打破军地界限、部门界限,破除各种小而全、不管任何设备都关门自产的做法,开展全军乃至全国信息安全防护设备的科研和生产大协作。

(四)构建信息安全人才培养体系,加强信息技术和心理安全防护力量。建立一支心理素质过硬、专业技术精湛、创新能力很强的信息安全人才队伍,并制定出一套合理先进的干部培训制度,是保障国家信息安全的智力支撑。目前,俄罗斯国家和军队信息防护特种分队已基本建成,主要包括网络监测中心、信息安全评估中心、应急处理中心、信息安全研究中心等。同时,将全俄90所开设有信息安全专业的大学、22个信息安全地区教学中心、12个部委信息安全管理机构和科研机构组成一个信息安全人才培养体系,设置6个国家教学标准和7个基本专业(密码学、计算机安全、信息保护制度与技术、信息对象的综合保护、自动化系统的信息安全综合保障、通信系统的信息安全和反侦察信息技术)。

俄军方也将信息安全防护干部的培训列入部分高、中级军事院校的培训体系。目前已对学员展开信息加密、防干扰、防辐射、防侦察、防摧毁、防网络入侵、防计算机病毒以及信息鉴别、入侵检测、反心理战等科目的训练,如全军无线电电子学院的培训计划要求信息安全专业的学员在毕业时必须成为“信息卫士”,通晓所有信息安全防护方面的知识和技能。同时,还采用在加强近似实战条件下运用反信息封锁和信息类比法训练。近年来,俄军在各种演习演练中,特别是通信演习中,防干扰、防辐射、防侦察、防网络入侵、反心理战等已成为经常性科目。◎

[1] “俄罗斯信息安全建设综述”,《国家信息安全评测论证》2007年第1期,http://www.itsec.gov.cn/zxzz/lwt/1853.htm