俄罗斯国家信息安全面临的威胁及其保障措施分析

姜振军 齐 冰

【内容提要】 随着现代信息技术的广泛应用和信息网络化的飞速发展,信息安全问题变得日益迫切,成为非传统安全领域中的一个突出问题和国家安全保障的重点领域之一。美国"棱镜门"事件曝出以后,各国对本国信息安全问题更加关注。在冷静分析信息安全面临的威胁基础上,俄罗斯正在积极采取综合措施,从而最大限度确保国家信息安全。

【关 键 词】 俄罗斯 国家信息安全 国家媒体资源

【作者简介】 姜振军,1968年生,黑龙江大学协同创新中心研究员,黑龙江大学俄罗斯研究院副院长、研究员、博士、硕士生导师;齐冰,1978年生,黑龙江省政府对外联络办公室副译审。(哈尔滨 150080)

《俄联邦国家信息安全学说》指出,信息安全是俄联邦国家安全的一个组成部分,它对俄联邦国家利益产生着重要影响,因而维护国家信息安全是俄罗斯政府和有关部门特别重视,并采取相应措施确保完成的一项紧迫任务。

一 信息安全的内涵及国家信息安全的内容

当今时代,国家安全的内涵不再局限于国家传统安全范畴,而是从维护国家主权与领土完整的传统安全,扩展到经济、科技、生态、文化、社会等领域的非传统安全。无论传统安全,还是非传统安全,安全的核心是信息技术及其内容——信息。信息安全是信息时代国家安全中最突出、最核心的问题①。

(一)信息安全的内涵

狭义的信息安全是指对信息数据的机密性、完整性、可用性和可控性的保护。广义的信息安全不仅指信息数据的安全,还指信息基础设施安全、信息软件系统安全、网络安全、信息使用者与管理者安全、公共信息秩序和国家信息安全等多维、多层次、多因素、多目标的完整体系。信息安全是物理安全、数据安全、网络安全、信息基础设施安全、信息资源安全、金融安全、个人权益安全、企业生存安全、社会稳定乃至国家信息利益和安全等的总和②。

(二)国家信息安全的内容

信息安全是信息时代来临后国家安全研究方面一个越来越重要的研究对象和内容。目前,信息安全问题已成为各国信息活动和国家安全保障

① 蔡翠红:《信息网络与国际政治》,学林出版社2003年版,第163页。

② 刘跃进主编:《国家信息安全学》,中国政法大学出版社2004年版,第184~185页。

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

必须面对的一个日常性问题。国家信息安全是指维持国家政治、经济、军事、科技、文化、社会生活等系统不受到内外威胁、干扰、破坏而正常运行的状态①。

国家信息安全主要包括以下 4 个方面的内容：

1. 国家信息资源安全。国家信息资源安全是保护涉及政治、经济、军事、科技、文化、生态等领域的国家信息资源在生产、传递、贮存、管理和使用中不被他国、组织或个人所掠夺、侵占或破坏②。

2. 国家信息疆域和信息边界安全。一个国家或统治集团的信息传播力和影响力所能达到的无形空间称为“国家信息疆域”。国家主权行使的空间将不再局限于领土、领海和领空，而必须包括网络空间（Cyberspace 又称计算机空间，或称赛博空间）。“信息边界”是指一种无形的、划分国家或统治集团“信息疆域”的不规则界线。捍卫国家的“信息疆域”和“信息边界”安全，已逐步成为国家安全战略的新视点，成为网络时代维护国家主权的关键问题③。

3. 国家信息技术安全。信息技术一般是在计算机、网络、通信等技术支持下用以采集、处理、传递、显示、存贮并利用那些包括文字、图像、声音和数据在内的多种信息的一系列现代技术的统称。

从国家安全的角度来看，从狭义来说，网络战则是敌对双方在作战指挥、武器控制、战斗保障、后勤支援、军事训练、情报侦察、作战管理等方面运用网络技术所进行的一系列网络侦察、网络进攻、网络防御和网络支援行动。从广义上讲，网络战是敌对双方在政治、经济、军事、科技领域运用网络技术为争夺信息优势而进行的斗争④。

4. 国家信息人才安全。信息人才一般包括：一类专业信息人才，即那些系统学习、研究信息科学基础理论的学生和学者；那些设计、研制、开发、推广信息技术的研究人员；那些熟练掌握并使用国家核心信息技术的专业技术人员；那些负责国家信息安全的决策、立法、保护、侦察人员以及集体电脑族群和个体电脑迷等。另一类是指相关信息人才，包括国家首脑及决策人物以及那些在新材料、新能源、生物、航天、海洋等技术领域的科学家和研究人员等⑤。

从所涉及的领域来看，国家信息安全还涉及政治、经济、军事、文化、生态和民族宗教等具体领域的信息安全问题。

二　影响俄罗斯国家信息安全状况的因素

俄罗斯国家信息安全状况表明，俄罗斯的国家信息安全程度并没有完全达到国家和社会要求的水平。

（一）国家相关政策支持不够

在俄罗斯，信息空间的形成、大众信息系统的发展、国际信息交流以及俄罗斯的信息空间与世界信息空间实现一体化等方面，俄罗斯的国家相关政策缺乏明确性。这可能将俄罗斯大众媒体排挤出国内信息市场。俄罗斯政府对本国通讯社把自己的产品推向国外市场的运作给予的支持力度尚显不足。

为此，俄罗斯总统普京下令重组国家媒体资源，加大对外宣传俄罗斯国家政策和社会生活的力度。2013 年 12 月 9 日，俄罗斯总统官方网站发布了普京签署的关于“提高国家级媒体效率措施”命令的全文。这份总统令中涉及了对全俄电视广播公司、俄通社－塔斯社、俄罗斯报以及俄罗斯新闻社这几家最主要的国家级大媒体的改组。最引人注目的是取消了俄罗斯新闻社，在此基础上改组为“今日俄罗斯”国际新闻社。俄罗斯国家对外广播机构“俄罗斯之声”也被并入到这家新闻社旗下。总统令中指出，“今日俄罗斯”的定位为对外报道俄罗斯国家政策和俄罗斯的社会生活。改组后的新闻社将由俄罗斯著名记者、全俄电视广播公司副总经理基谢廖夫领导。

（二）关于信息的自由交流与限制的相关法律不健全

在信息化时代，各国的广大民众要求扩大信

① 金小川：《信息社会的重大课题：国家信息安全》，载《国际展望》1997 年第 3 期。

② 刘跃进主编：《国家信息安全学》，第 185 页。

③ 刘跃进主编：《国家信息安全学》，第 186 页；刘文富：《网络政治——网络社会与国家治理》，商务印书馆 2002 年版，第 16 页。

④ 濮端华：《“制网权”：一个作战新概念》，载《光明日报》2007 年 2 月 7 日。

⑤ 刘跃进 主编：《国家信息安全学》，第 186～187 页。

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

息自由交流与国家在信息传播方面进行必要的限制之间存在着矛盾，而且这种矛盾正在与日俱增。

在俄罗斯，对信息领域社会关系进行法律调节的矛盾性和滞后性引起了严重的消极后果。通过宪法对大众信息自由加以限制，其目的在于维护宪法制度基础，保护公民的道德、健康、权利及合法利益，保障国防能力和国家安全。但是，由于在这方面的法律法规协调不力，给保持个人、社会和国家在信息领域的必要平衡带来了困难。对大众信息领域的关系进行法律协调不到位，有关法律法规不健全，使俄联邦境内很难形成具有竞争力的大众媒体。

在这种矛盾之中，对包含国家机密的信息进行有效保护变得越来越难。

（三）公民在信息领域享有的权利缺乏应有的保障

公民获取信息的权利缺乏保障，有些人利用信息从事诈骗活动，这在居民中引起了负面的反应，在某种情况下会导致社会局势不稳定。

俄联邦宪法规定，公民享有私生活不受干扰、个人和家庭隐私及通信保密的权利，而在实际生活中缺乏足够的法律上、组织上和技术上的保障。对俄联邦国家权力机关、各联邦主体国家权力机关和地方自治机构收集的自然人（个人）的资料保护力度不够，时有自然人个人信息被泄露，遭到不法之徒盗用的事件发生。

（四）信息人才外流，信息技术停滞

在叶利钦执政时期，俄罗斯政治、经济和社会形势动荡，导致制造信息化设备、通信和通讯工具方面的人才大量外流。与此同时，由于俄罗斯本国的信息技术落后，对外国计算机和通讯设备、软件等的生产者产生的依赖性增强，俄联邦国家权力机关、各联邦主体国家权力机关和地方自治机关在建立信息系统时不得不购买进口设备和吸引外国公司参与，这就使外国公司未经允许获取正在加工信息的可能性增加。

个人、社会和国家经常使用国外信息技术，广泛使用公开信息和通信系统，本国信息系统与国际信息系统实现一体化。在这种情况下，运用“信息武器”攻击俄罗斯信息基础设施的危险性在提高。

为了尽可能消除类似危险，俄罗斯正在努力加强协调，增加预算拨款，重视太空侦察和电子对抗设备的研制，提高自主创新能力。

三 俄罗斯国家信息安全面临的威胁

在网络时代，俄罗斯国家信息安全面临的威胁在不断增强。

俄罗斯国家安全构想中列举了俄罗斯国家信息安全面临的种种威胁：

（一）国家信息政策方面的威胁

首先表现在俄罗斯信息市场的垄断上，本国和国外信息机构垄断俄罗斯信息市场的某些领域；其次是国家相关政策封锁本国大众媒体在国内外的某些信息宣传活动；第三是由于缺乏专业人才、没有制订和落实国家信息政策及其机制，使俄联邦国家政策信息保障效率低下。

（二）经济领域的信息安全面临的威胁

确保俄联邦经济领域的信息安全是保障国家信息安全的一项重要内容，同时发挥着关键作用。

国家统计系统、金融信贷系统、联邦执行权力机关中负责保障社会和国家经济活动部门的信息系统及统计系统、各种所有制企业、机关和组织的财会系统等搜集、处理、储存和传递有关信息的系统最易受到觊觎者的攻击和被盗取信息资料。

在俄罗斯，国内外的经营单位在建立和保护信息的加工、储存和传递系统方面缺乏监督，这给俄罗斯经济领域的信息安全带来了现实威胁，尤其外国公司会带来类似的更大威胁，因为这些外国公司可能超越权限，未经允许获取经济机密信息和不受监督地传递和加工信息。

俄罗斯本国信息化、通信和信息保护设备研制和生产工业企业处于危机状况，只能大量使用相应的进口产品，这使俄罗斯有对外国产生技术依赖的危险。

通过垃圾邮件传播计算机病毒和窃取信息是常见的。据计算机安全公司 Sophos 称，俄罗斯已经成为一个垃圾邮件“超级大国”，成为仅次于美国的第二大制造垃圾邮件的国家。美国产生的垃圾邮件占全球垃圾邮件数量的 27%，俄罗斯产生的垃圾邮件占 8.7%，目前世界每 12 封垃圾邮件

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

就有一封来自俄罗斯①。

（三）内政领域的信息安全面临的威胁

俄联邦内政领域信息安全面临的威胁主要包括：个人和公民在信息领域应享有的宪法权利和自由被削弱；法律在对各种政治力量利用大众媒体宣传自己思想方面的调节力度不够；大肆传播有关俄联邦政治、国家权力机关、国内外发生事件的虚假信息；某些社会团体企图以暴力改变宪法制度和破坏俄联邦完整，挑动社会、种族、民族和宗教间仇视，并在大众媒体上传播相关思想。

（四）外交领域的信息安全面临的威胁

俄联邦外交政策领域信息安全最容易受到攻击的方面：负责实施俄联邦对外政策的联邦执行权力机关、驻国外的代表处和组织以及驻国际组织的代表处的信息资源；负责实施俄联邦对外政策的联邦执行权力机关驻各联邦主体代表处的信息资源；负责实施俄联邦对外政策的联邦执行权力机关所属的机关和组织、俄罗斯企业的信息资源。

俄联邦外交政策领域信息安全面临的威胁：

1. 来自内部的最大威胁主要包括：破坏负责实施俄罗斯对外政策的联邦执行权力机关及其所属机关和组织以及俄罗斯企业的信息收集、加工、储存和传递的确定程序；某些政治力量、社会团体、大众媒体和个别人员开展信息宣传活动时歪曲俄联邦对外政策活动的战略战术；居民获得的有关俄联邦对外政策活动的信息有误。

2. 来自外部的最大威胁主要包括：外国政治、经济、军事和信息机构干扰俄联邦对外政策战略的制订和实施；国外散布有关俄联邦对外政策的不实信息；侵犯在国外的俄罗斯公民和法人信息领域的权利；企图未经允许获取俄联邦的信息资源，并试图破坏负责实施俄罗斯对外政策的联邦执行权力机关、俄罗斯政府及其国外组织、俄联邦驻国际组织的信息基础设施；对俄罗斯大众媒体有关俄联邦国家政策目标和基本方向及其对俄罗斯和国际生活中具有社会影响的重大事件的看法等对外宣传活动实施封锁，等等。

（五）科技领域的信息安全面临的威胁

俄罗斯科技领域易受攻击的方面主要包括：基础性的、勘察性的和应用性的科研成果，对国家科学技术和经济社会发展具有潜在重要性的前沿成果；未取得专利权的发明、工业样品和模型、试验设备；科技人才及其培养体系、复杂的科研综合体（核反应堆、粒子加速器、等离子发生器等）体系。

俄罗斯科技领域信息安全面临的威胁：

1. 面临的主要内部威胁：国家对科技活动的拨款尚不足，科技领域的地位有所下降，先进的思想和发明严重外流；电子行业企业不能借助最新微电子成果和先进的信息技术生产出具有竞争力的科技含量高的产品，从而保证俄罗斯应有的科技水平，不受制于外国。电子行业企业生产能力的不足使俄罗斯在发展信息基础设施时不得不广泛使用进口软件；在保护俄罗斯科学家科技成果的专利方面存在着严重的问题；信息保护措施，尤其是股份制企业、科研机构和组织的信息保护措施的落实比较复杂。

2. 面临的主要外部威胁：世界某些发达国家竭力非法获取俄罗斯的科技资源，将俄罗斯科学家的科研成果为己所用；为俄罗斯市场上的外国科技产品创造优惠条件，与此同时，发达国家却想尽办法限制俄罗斯科技潜力的发挥（如购买先进企业的股票、对进出口设限等）；西方国家推行进一步破坏从苏联继承下来的独联体国家统一科技空间，使其与西方国家建立科技联系；外国国有的和商业性企业、机构和组织不断从事工业间谍活动。

（六）精神生活领域的信息安全面临的威胁

俄联邦国家权力机关、各联邦主体权力机关通过的某些法律法规侵犯了个人和公民精神生活领域和信息活动方面的宪法权利和自由；在俄联邦，国家垄断信息的形成、获取和传播；某些人，尤其是犯罪组织侵犯公民在个人和家庭隐私、通信保密、电话交谈和其他联络方面享有的宪法权利；非法使用对个人、团体和社会认识产生影响的特种装置；将俄罗斯通讯社、大众媒体从本国信息市场排挤出去，强化俄罗斯社会生活中精神、经济和政治领域对国外信息机构的依赖；宣传与俄罗斯

① 《美国居首，中国第三，俄成第二大垃圾邮件“大国”》，载《生活报》2008 年 2 月 14 日。

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

社会价值相矛盾的大众文化;降低俄罗斯的精神、道德和创造潜力,使利用最新技术的劳动力资源(包括信息领域的)的培训工作变得复杂起来;存在利用信息进行欺骗,如制造假信息、藏匿信息和歪曲信息现象,等等。

(七)信息和通讯领域的信息安全面临的威胁

该领域易受攻击的方面:包含国家机密和秘密信息的情报信息资源;信息化工具和系统、软件、自动化管理系统、进行限制类信息接收、加工、储存和传递的通讯和数据传输系统、信息物理场;限制类信息加工地点以及放置在限制类信息加工地点的技术装备和系统;举行秘密谈判的地点及有关禁止获取信息的谈判。

这一领域的信息安全面临的威胁:外国特种机构、犯罪团伙和组织从事的活动,某些个人未经允许获取信息和对信息和通信系统功能进行监控的非法活动;因本国工业技术水平的落后,在建立和发展信息和通信系统时被迫使用进口软件;破坏信息的收集、加工和传递的程序;使用未经品质证明的信息化和通讯工具及系统以及信息保护和其效率监督系统;允许没有国家许可证从事信息和通讯活动的组织和公司开展建立、发展和保护信息和通信系统的业务;对俄罗斯信息产业发展,包括信息化、电信和通讯工具产业的发展,确保信息产业产品的国内市场需求及打入国际市场以及确保国家信息资源的积累、储存和有效利用构成的种种威胁。

(八)国防领域的信息安全面临的威胁

国防领域易受攻击的方面:俄罗斯武装力量中央军事管理机关和各军兵种军事管理机关、武装力量所属单位以及国防部科研机构的信息基础设施;国防综合体企业和完成国防订货或从事国防问题研究的科研机构的信息资源;军队和武器自动化软件技术及其工具,配备信息化装置的武器和军事装备;其他军队和相关机构的信息资源、通讯系统和信息基础设施。

国防领域的信息安全面临的威胁:

1. 内部威胁:破坏俄罗斯国防部总部和机构、国防综合体的信息收集、加工、储存和传递业既定的程序;特种用途的信息和通信系统的工作人员有预谋的行为和出误;特种用途的信息和通信系统的功能存在安全漏洞;损害俄联邦武装力量的声誉和备战的信息宣传活动;国防综合体企业知识产权保护不够导致最有价值的国家信息资源外流;军人及其家庭成员的社会保障问题未解决。

2. 外部威胁:外国的所有侦察活动;可能的对手施加的信息技术(包括无线电对抗、对计算机网络的渗透)影响;外国特种机构通过施加信息心理影响从事破坏活动;外国政治、经济和军事部门从事损害俄罗斯国防领域利益的活动。

(九)护法和司法领域的信息安全面临的威胁

1. 内部威胁:破坏用于调查犯罪行为的信息收集、加工、储存和传递既定的程序;有关信息交流的法律法规调节力度不够;缺乏统一的业务侦察、咨询、犯罪性质和特点等方面信息的收集、加工和储存的方法;信息和通信系统技术设备停止运行和程序出现问题;直接负责数据库管理的工作人员采取蓄意行动或出现差错。

2. 外部威胁:外国特种机构、国际犯罪团伙和组织进行涉及俄联邦内务机关及其所属部门分布地点、承担的任务、活动计划、工作方法和技术配备等情报的收集侦察活动;外国国家机构和私人商务机构试图未经允许获取护法机关和司法机关的信息资源。

四 俄罗斯保障国家信息安全采取的措施

保障国家信息安全指的是从国家的角度出发,对本国信息安全采取的一系列保护措施的统称。

俄罗斯信息安全是指俄联邦在信息领域国家利益的保护状态。信息领域是信息领域主体、信息、信息基础设施、信息的收集、形成、加工、传播和利用系统以及调节社会关系系统的总和①。俄联邦信息领域的国家利益在于维护公民获取和利用信息方面的权利和自由、发展现代无线通讯技

① Концепция нормативного правого обеспечения информационной безопасности Российской Федерации. http://jurfak. spb. ru/conference/18102000/konztepztia. htm

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

术、保护国家信息资源不被非法窃取①。俄联邦的信息安全状况可以反映出其在信息领域国家利益的保护情况，个人、社会和国家在信息领域利益的平衡状况②。

保障信息领域的国家利益，是俄联邦保障国家信息安全的核心及首要任务。为此，采取了一系列保障措施：

（一）落实国家保障信息安全的政策

制订和运用调节信息领域关系的法律法规，以保障国家信息安全构想的实施；制订和落实提高国家领导大众媒体活动和落实国家信息政策的效率；提高公民的法律文化和计算机水平，发展俄联邦统一信息空间基础设施，为社会和国家履行重要职能过程中使用的网络研发提供安全可靠的信息技术，为联邦权力机关和各联邦主体权力机关建立专用信息通讯系统，保障国家在开发和使用国防信息通讯系统的技术独立性；协调信息化和保障信息安全管理拥有通用的和专用的信息通讯系统；建立确保国家信息安全的人才培训体系等等③。

（二）完善组织和技术方式

建立和完善俄联邦信息安全保障体系；加强俄联邦执行权力机关和联邦各主体执行权力机关运用法律的力度；制订、运用和完善信息保护手段及其有效性的监督方法，研发保护性通信系统，提高专用保护程序的可靠性；建立防止非法获取加工信息及破坏、销毁和变更信息的行为；有能力发现并查出危害信息通信系统正常运行的技术装置和程序，防止信息被截获，监督信息保护专门要求的执行情况；提高信息保护手段的质量，为国家信息保护活动办理许可证，使信息保护方式和手段标准化；按照信息安全要求，完善通信设备和信息加工程序自动保护系统；培训国家信息安全保护领域的人才；建立在国家和社会生活及活动中的信息安全指数和特点的联邦级监测系统。

（三）建立信息资源防止网络攻击系统

随着信息技术的不断发展，网络安全日益受到世界各国政府的重视。俄罗斯总统普京签署命令（2013 年 1 月 15 日生效），授权俄联邦安全部门建立“俄联邦信息资源防止网络攻击系统”，即防黑客系统。新的国家信息资源防护系统的主要作用是对俄联邦信息安全领域的动态进行监测并分析，在受到网络极端攻击情况下对国家信息设施的防护程度进行监控以及协调信息资源的拥有者、通信运营商及信息防护领域经授权许可的其他主体之间的关系④。

（四）确保经费投入

制订俄联邦信息安全保障规划和确定拨款程序；完善与落实信息保护的法律和组织、技术方法相关的拨款工作机制；建立涉及自然人和法人信息风险的保险体系。

（五）加大信息人才的培养力度

俄罗斯信息安全方面人才的培养从 1992 年起在全国范围内取得了较快的发展，当时拟定了“高等学校间确保信息安全的方法和技术手段科学技术规划”。

俄罗斯采用是否符合职业适应性测试来选拔人才的方法，该方法成功地用于为军校、安全局和外交部各高等学校选拔考生。因从事信息安全问题的专家应具备较高的道德伦理品质，对即将从事与信息保护有关的专业工作的考生进行初步测试的经验受到极大的关注。俄罗斯简化了候选人初选程序，提供对考生入选能力进行远程判断的条件，对具体专业培训工作进行准备。对每一个应征者要对 4 个要素进行远程测试：对个人动机的评估、对个人对违法行为心理稳定性的评估、对候选人“创造潜力”方面的求知欲进行评估和对候选人为实现既定目标的积极性进行评估⑤。

高级专业人才的短缺要求不断提高教育质量。俄罗斯信息安全教育高校教学法联合会副主席 Е. Б. 别洛夫指出，“提高国家对信息保护专家

---

① Концепция нормативного правого обеспечения информационной безопасности Российской Федерации. http://jurfak.spb.ru/conference/18102000/konztepztia.htm

② Доктрина информационной безопасности Российской Федерации. http://www.dol.ru/users/rastinfo/Doctrina/doctrina.htm

③ *Доктрина информационной безопасности Российской Федерации.*

④ 《俄罗斯加强国家信息安全的新举措》，http://www.most.gov.cn/gnwkjdt/201302/t20130226_99779.htm

⑤ Геннадий Маклаков. Научно – методологические аспекты подготовки специалистов в области информационной безопасности. http://www.crime – research.ru/articles/maklakov0105/9

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

的培养质量是一项现实而迫切的任务”①。

(六)加强信息安全保障体系的建设

俄联邦国家权力机关、联邦各主体权力机关以及相关的企业、机构和组织信息安全保护意识不断增强,重视信息安全保护工作,从多角度、多层面,采取综合措施来加强信息安全保障体系的建设。

一是提高信息安全保障体系的技术水平。二是完善有关信息安全保障体系的法律法规。三是加强信息安全保障体系的管理。国家信息安全保障体系、国家机密保障体系、国家机密保护和信息保护手段领域实行获取信息许可制,以保障俄联邦信息安全。

(七)加强主要领域的信息安全保障

信息安全对俄联邦国家利益产生着重要影响,但是各个社会生活领域因其特点、脆弱性不同,面临的信息威胁和保障措施亦是不尽相同的。《俄联邦国家信息安全学说》针对不同领域提出了保障内政领域、外交领域、经济领域、科技领域、信息和通信领域、国防领域和护法与司法领域信息安全的具体措施②。

(八)努力掌控信息权和制网权

在网络信息时代,非传统安全中的网络安全倍受关注,并且日益成为国家安全的重要组成部分。在当今时代,权力(power)发生了转移。相对于硬权力而言,软权力的重要性进一步上升,信息力成为非线性综合国力③中的核心,国际政治霸权也从海权论、陆权论、空权论,发展到现在的信息权论。因而,争夺制信息权(即在一定时空范围内控制战场信息的主导权)、制网权(即是对网络的控制权,对一个主权国家而言,包括对国内网络的控制权、国内网络与国际网络通信能力的控制权以及对涉及本国政治经济利益的国际网络纠纷的司法管辖权。谁拥有制网权,谁也就获得了相对安全的权利。)成为目前各国国家战略中的重点之一④。

俄罗斯正在努力通过技术、组织、法律和经济等多种方式掌控信息权和制网权,最大限度地维护自身的信息安全。

(九)开展国际信息安全合作

俄罗斯信息安全保障领域的国际合作是其政治、经济、军事、文化等融入国际社会开展协作的不可分割的组成部分。这种合作能够提高包括俄罗斯在内的国际社会所有成员信息安全的程度。

俄罗斯积极参与所有信息领域国际组织的活动,其信息领域开展国际合作的主要方向:禁止研制、传播和使用“信息武器”;保障国际信息交流安全,包括对通过通信和通讯渠道传递信息的保护,防止美国窃听别国领导人手机等类似行为的发生;参与协调国际护法机关的有关活动,防止计算机犯罪;打击未经允许获取国际银行网络和国际贸易信息保障系统信息的行为;此外,俄罗斯特别重视与独联体国家的协作⑤。

信息安全被视为国家安全战略的重要组成部分和基础。俄罗斯认为,信息安全对各领域的国家利益产生着重要影响。俄罗斯信息安全领域存在各种隐患,同时面临着各种威胁,因而对俄罗斯有关部门来说,竭力采取有效措施以保障国家信息安全是一项极为紧迫的重要任务。

〔本文系黑龙江大学 2010 年高层次人才(创新团队)支持计划“俄罗斯经济与社会问题研究”(项目号:Hdtd2010 - 33)的阶段性成果。〕

(责任编辑 常 玢)

① Геннадий Маклаков, Научно - методологические аспекты подготовки специалистов в области информационной безопасности.

② Доктрина информационной безопасности Российской Федерации.

③ 非线性综合国力是指综合国力各要素之间存在着相互作用、相互制约的复杂关系。综合国力要素之间不是简单的因果关系、线性依赖关系,而是既存在着正反馈的倍增效应,也存在着限制增长的饱和效应。

④ 邢希娜:《网络安全:国家安全面临的新挑战》. http://www. cnki. net

⑤ Доктрина информационной безопасности Российской Федерации.

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

SUMMARY

Fan Chun For nearly 10 years, the Russian party landscape change revealed the new characteristics of Russia's political party system, namely one – party government – party system under control of the President. The government – party refers to these parties which integrates with the administrative institutions, using administrative resources to take seats in the parliament. Government – party system is the government – party in or close to the regime, the others were marginalized. This system resulted from the change of social economic structure, the regulation of the electoral system, and the influence of strong presidential system. The system can be seen as a response to Russian specific democratization. It is the party system of quasi – modernity with a certain competitiveness, stability and sustainability.

Jiang Zhenjun and Qi Bing With the extensive application of modern information technology and the rapid development of information network, information security has become increasingly urgent, become an outstanding problem in the field of non – traditional security and one of the key areas of national security. After exposure of "prism door", more and more countries paid attention to their own information security. Now Russia is taking comprehensive measures to ensure national information security up to the hilt.

Xu Guimin According to the Russian criminal law, reform – through labor is a punishment method with the following futures: judging by the court, not depriving of his (her) liberty and turning over his (her) part of the labor income to the state. Reform through labor is not deprived of personal freedom, but the labor rights and economic rights are restricted. Reform through labor is an independent principal punishments, not a supplementary punishments. Reform through labor just involves with person with ability to work. The people who defies a reform through labor, or makes malicious violations shall be punished severely. Russian legislation on reform through labor is more perfect, in addition to the constitutional guidance, with the basic law is concerned, it both has regulations on labor of Russian penal code and regulation on reform through labor of Russian criminal law implementation. There is a series of administrative rules, regulations and orders, also.

Yin Hong In 2010 ~ 2011 Russia made faster recovery growth than the average of world economic growth after the financial crisis. Putin's articles which published before the election in 2012 and subsequent many commands show the determination of Russian political and economic reform in the new period as well as the realization of comprehensive development planning. However, Russia's economy has begun to decline obviously since the second half of 2012. Economic downturn intensifies in 2013, annual GDP growth was only at 1.3%. To judge the economic situation, develop effective policies and boost the economy are an immediate task for Putin's government. At present, there is hot debate around the direction of macroeconomic policy and its tools inside Russia. The reason for that is how is positioning government itself.

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net