俄罗斯信息空间建设的思路与做法

由鲜举

【内容提要】　进入21世纪，随着信息网络技术的快速发展和广泛应用，网络空间[①]已成为继陆海空天后的第五作战域和各国竞相争夺的新的战略制高点，来自网络空间的威胁已对俄罗斯国家安全构成了严峻挑战。面对这一挑战，俄罗斯通过对其国家战略性规划文件的全面修订，阐述了其主张利用信息手段应对来自信息空间的各类信息威胁的观点和立场，并表达了要建设一个强有力的电子信息产业基础，以便为信息空间建设提供技术支持与保障的决心。在加快推进信息空间专业作战力量建设的同时，积极参与和动员国际社会力量共同开展国际信息空间的治理活动，并采取措施，着力提升俄罗斯全社会的信息防护能力与水平。本文通过对俄罗斯信息空间建设情况的梳理，归纳总结了其推进信息空间建设的思路，指出了其在建设过程中仍存在的一些问题，并得出了有关网络空间建设的几点结论。

【关 键 词】　俄罗斯　信息空间　信息安全

【作者简介】　由鲜举，国家工业信息安全发展研究中心高级工程师。

21世纪，科技的快速发展，使得以互联网为代表的信息网络技术开始更加广泛地用于社会管理、工业生产、贸易交往、居民生活乃至军事领域，网络空间已成为继陆、海、空、天之后的第五作战域，并与各传统域相互交织，成为世界主要国家竞相争夺的新的战略制高点。以美国为代表的西方发达国家，开始成体系地推进网络空间建设，并在一些领域形成了新的战略优势，已严重威胁到俄罗

① 网络空间作为一个新兴的概念，各国对其的称谓和定义也各不相同，其内涵和外延也略有不同。为了准确反映各国的实际情况，在本文中，涉及美国时仍使用“赛博空间”一词，在谈及俄罗斯时仍使用“信息空间”一词。但鉴于本文只是就俄罗斯信息空间建设情况进行探讨，而非就网络空间的概念进行理论研究，在非特殊说明的情况下，读者可简单地、非严格意义地将“赛博空间”和“信息空间”都理解为我们通常所说的“网络空间”。

斯的国家安全和利益。为确保在这一新兴领域不受制于人，俄罗斯审时度势，提出要在发展传统作战力量的同时，大力推进信息空间建设，先后出台了一系列纲领性文件，统筹规划，并采取积极措施，提升其应对信息空间威胁的能力。

一 相关概念辨析

在俄罗斯，与信息空间有关的概念，常见的主要有三个，即“信息空间（информационное пространство）”、“统一信息空间（единное информационное пространство）”和“网络空间（киберпространство）”。其中，“信息空间”与“统一信息空间”是一脉相承的两个概念，而与“网络空间”则是两个完全不同的概念。

在近年俄罗斯官方文件中，曾先后有两次正式对“信息空间”进行了定义。第一次是在 2011 年国防部发布的信息空间发展战略——《俄罗斯联邦武装力量信息空间活动的构想观点》（以下简称“构想观点”）[①] 中，第二次是 2014 年发布的《俄罗斯联邦网络安全战略构想（草案）》[②] 中。上述文件对“信息空间”使用了同一定义，即“与形成、创建、转换、传递、利用、存储信息有关的活动域。该活动域中所实施的活动，可对个体和社会认知、信息基础设施及信息本身产生影响”。

所谓的“统一信息空间”，是指根据统一原则和通用规则建设和运行的信息空间。俄官方文件最早对统一信息空间进行定义的是俄总统 1995 年签署的《俄罗斯统一信息空间和相关国家信息资源建设与发展构想》[③]。在该文件中，统一信息空间的定义是，“根据统一原则和通用规则建设和运行的、用于协调公民和组织在信息领域的相互关系，以及满足其信息需求的数据、数据库、数据库管理和使用技术，以及信息通信系统和网络的总称”。通过这一定义可以看出，在俄罗斯统一信息空间是个非常宽泛的概念，既包括信息、信息系统和平台，亦包括

① Концептуальные взгляды на деятельность вооружённых сил Росийской Федерации в информационном пространстве. http：//ens. mil. ru/files/morf/Strategy. doc

② Концепция стратегии кибербезопасности Российской Федерации（Проект）. http：//councll. gov. ru/media/files/. 该战略构想（草案）虽然最终并未获得通过，但其提出的观点被普遍认可。

③ Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов. http：//lawru. info/dok/1995/11/23/n453820. htm

与信息创建、使用和系统运维有关的信息技术。

网络空间的概念，在俄罗斯的出现要晚于信息空间，并曾在 2011 年前后呈现与信息空间混用、趋同的趋势。但 2014 年发布的《俄罗斯联邦网络安全战略构想（草案）》对网络空间予以了一个明确的界定，指出“网络空间”是“信息空间中的一个活动域，是指基于因特网和其他电子通信网络，实现信息交流、保障其运行的技术基础设施，以及直接使用这些渠道和设施的所有人类活动的领域”。

通过上述定义可以看出，在俄罗斯，从严格意义上说“信息空间”是一个比“网络空间”更为宽泛的概念，网络空间更多的是指各种通信网络及信息基础设施，而信息空间则还要包括与之相关的一系列活动。“信息空间”要早于“网络空间”且更广泛地被官方和民众所使用。

二　推进信息空间建设的思路与做法

自 20 世纪 90 年代提出要发展信息空间以来，俄罗斯先后出台了一系列政策措施。通过对这些政策措施的梳理和分析，可以看出，俄罗斯在推进信息空间建设过程中，遵循了这样一种工作思路，即：通过顶层规划，明确信息空间建设的目标、方向、路径和保障措施，为其顺利推进提供方向性指导；主张用信息手段应对日益复杂的各类信息威胁，以确保俄罗斯联邦的国家安全和在信息空间领域的国家利益；支持电子信息产业的发展，通过强化产业基础和实现关键技术领域的突破，为信息空间的建设提供强有力的技术保障和产业支持，以摆脱受制于人的现状，实现技术领域的自主可控，进而消除安全风险；秉承战斗民族的一贯做法，主张依靠武装力量、安全、情报等部门的力量，建设专业化的信息空间作战力量；积极参与、倡导并推动有关国际准则的建立，在制衡美国的同时，突出俄罗斯的存在感，在信息空间这一新兴领域重现其大国雄风；充分认识到信息威胁已遍布国家管理、军队建设、工业生产和社会各领域，主张提升全社会的信息防护能力，但在国家财力有限的情况下，首先要保护的仍是强力部门和政府部门等关键部位。

在这一思想指导下，近年来俄罗斯的信息空间建设稳步推进。

1. 构建信息空间建设政策框架体系

为规范信息空间这一新兴领域建设，俄罗斯不仅出台了《俄罗斯统一信息空

间和相关国家信息资源建设与发展构想》《俄罗斯联邦武装力量信息空间活动的构想观点》等专门用来指导信息空间建设的战略性规划文件，并根据国内外形势的变化和信息通信技术发展应用情况，在最近的 4 年中分别对“国家安全战略”“军事学说”和“信息安全学说”进行了全面修订。新出台的这些文件，无不突出强调了信息空间建设，从不同的角度阐述了信息空间建设的迫切性、指导原则、建设重点，明确了当前及未来一段时间俄信息空间所面临的安全威胁与挑战，以及预防、遏制和解决信息空间冲突的原则等，逐步构建和完善了俄罗斯信息空间建设的政策框架体系。

国家安全战略为俄信息空间建设提供了政策基础。作为未来俄国家安全、国防和军队建设的指导性文件，《国家安全战略》决定着俄罗斯国家战略优先方向的选取、内外政策的走向，以及经济社会的发展，对国家的长期、稳定发展具有重要意义。2015 年新版《国家安全战略》认为，美国及其盟友正在政治、经济、军事和信息领域对俄施加压力，致使俄罗斯不得不面对八类安全威胁，即：北约抵近俄边境进行军事部署、颜色革命（包括破坏俄传统道德文化价值观的活动）、非洲和中东移民问题、乌克兰等新的冲突策源地不断涌现、恐怖主义和其他极端主义威胁、拥核国家增加和化学武器的扩散、全球信息对抗的影响不断加强，以及利用信息通信和高科技手段的新型犯罪日益增多等。其中，颜色革命、信息对抗、网络犯罪与信息空间建设息息相关，信息空间的安全问题已成为仅次于国防安全、国家安全、社会安全的俄罗斯第四大安全问题①。为此，新版《国家安全战略》主张，要采取包括加强信息保护措施在内的综合性措施应对各类安全威胁、维护国家利益。这一变化，为俄罗斯加快推进信息空间建设提供了政策依据和法律基础。

信息安全学说统筹规划了信息空间建设的目标和方向。作为信息安全领域的“战略性规划文件”，2016 年 12 月颁布的新版《俄罗斯联邦信息安全学说》进一步指出，“信息技术已成为推动国家经济快速发展和构建信息社会的重要因素，正越来越多被用于达成地缘政治、军事和战略稳定等目的”，在保障俄国家利益和战略主导权上“信息空间发挥着重要作用”，“信息安全体系已成为国家安全保障体系的重要组成部分”，为此，“必须建立安全、可靠的信息安全保障体

① Стратегия национальной безопасности Россиийской Федерации. http：//www. kremlin. ru/supplement/424

系”，以捍卫俄联邦在信息空间的国家主权[①]。新学说重新界定了信息领域国家利益的范围，进一步明确了俄罗斯所面临的信息威胁，并确定了俄信息安全保障的战略目标和主要方向，为俄信息空间相关政策的制定和信息安全体系建设指明了方向。未来，俄罗斯的信息安全领域的工作重点将是建立一套适合本国国情的信息安全评估标准和体系，并定期对其进行评估。同时要建立和完善信息网络威胁监督管理机构和公众平台，构建统一的信息安全领域人才培养体系，提升专业人员的职业技能和水平。

武装力量信息空间活动构想明确了俄军在信息空间行动的原则。作为指导俄武装力量信息空间建设的战略性文件，该构想明确了俄军信息空间建设和行动必须遵循的六项原则，即：合法性原则，即俄军在信息空间采取行动时，要自觉地遵守俄罗斯现行法律和国际法准则的相关规定；优先性原则，即要采取措施收集有关信息威胁的真实、准确信息，并采取必要的防护措施；综合性原则，为应对俄罗斯在信息空间面临的各类威胁，允许运用各种手段、动用所有力量遂行信息空间的各项任务；协同性原则，要求政府各部门和机构间要加强协作，以确保在信息空间能够协同行动；合作性原则，俄罗斯愿意基于国际法规范和准则，与所有友好国家和国际组织加强互信，共同研究合作，通过建立有效的集体行动机制，确保信息空间安全；创新性原则，提出为确保俄罗斯在信息空间领域的战略优势，要加快技术研发，推广应用先进的技术、手段和方法，并吸收高水平专业人员完成信息安全任务。

2. 主张利用信息手段对抗信息威胁

认为信息空间已成为大国博弈的新场所。俄罗斯认为，“在全球信息空间、陆、海、空、天全域施加影响”已成为“现代军事冲突的突出特征”，“信息对抗”对国际形势的影响越来越大，一些国家正在“利用信息通信技术谋求达到其地缘政治目的”，对俄罗斯实施全方位的“遏制和战略压制”；信息通信技术正越来越多地被“用于军事政治目的，以及实施违反国际法的相关活动，甚至被用来开展恐怖、犯罪与其它违法活动，已对国际和平与安全，以及全球和地区构成威胁”。信息空间这一新兴领域还被一些国家和组织当作“颜色革命”的工具，被广泛用来宣传“法西斯、极端主义、恐怖主义和分裂主义思想”。这些威

① Доктрина информационной безопасности Российской Федерации. http：//www. kremlin. ru/acts/bank/41460

胁，以及日益频发的针对俄罗斯的“信息攻击和破坏信息基础设施的行为已对俄国家安全构成了严重威胁”，使俄罗斯面临着新的、复杂的、相互关联的威胁，信息安全业已“同国家、社会、生态、经济、交通、个人安全一样，成为俄国家安全的一个重要组成部分”，信息空间威胁与大规模杀伤性武器、局部战争一起，被列为“当前俄罗斯面临的主要外部军事危险之一”①。

承认俄罗斯正面临着各类信息空间领域的威胁。2016 年出台的新版《信息安全学说》，细数了俄罗斯信息空间所面临的各类威胁。这些威胁主要包括：发达国家出于各种目的，对俄基础设施（包括关键信息基础设施）施加的影响日益严重，并加大了对俄国家机关、科研机构和军工综合体的技术侦察力度；个别国家、宗教、种族和社会组织，利用专业机构（包括媒体）不断加大对俄罗斯公民的信息心理影响，对俄内政外交政策进行大量非客观的、存有偏见的报道和评论，干涉俄罗斯内政，破坏俄社会稳定；利用信息手段，对俄罗斯人（首先是年轻人）施加信息舆论影响，腐蚀多民族文化基础和精神财富，动摇国家精神基石、历史基础和爱国传统，加剧民族和社会紧张关系；信息网络技术已成为各种恐怖和极端组织宣传极端主义思想最为快捷的传播工具和途径，被广泛用来宣传种族、宗教仇恨，混淆个人和社会认知，并引诱人们实施恐怖活动，一些恐怖和极端组织正在加快研发相关技术，用以破坏对俄罗斯国家安全和居民生活都至关重要的关键信息基础设施；计算机网络犯罪日益增多，特别是在货币、金融和资本市场等领域；利用信息技术、信息系统和通信网络，侵犯个人和家庭隐私、违反个人数据保护的事件正在增多，其方式方法不断推陈出新；信息通信技术和产品严重依赖进口，形成了受制于人的局面；发达国家信息通信技术领域的优势，正在转化为经济和地缘政治优势等。

主张利用信息手段捍卫国家安全。近年来，俄罗斯一直强调，要采用包括信息手段在内的各种手段，捍卫国家和领土安全，“巩固俄罗斯联邦作为世界领导者之一”的地位。新的《信息安全学说》更是明确了俄罗斯联邦信息空间安全建设的基本原则：首先是要遵守俄罗斯宪法、其他联邦法律的限制及公认的国际法准则和标准，即合法性原则；其次是要保持公众的信息需求与限制信息传播之间的平衡，但这种平衡必须是要确保国家的安全，包括信息安全，即安全性原则；第三是要提升俄罗斯的信息威胁检测与预警能力，并保障能够投入足够的人

① Военная доктрина Российской Федерации. http：//www. kremlin. ru/events/president/news/47334

力、物力确保国家的信息安全，即保障性原则。除此之外，还明确了其提升信息保障能力的途径和方向，如：尽快完善武装力量、其他军队和机构的信息安全机制；大力发展信息对抗力量和装备；防范和打击针对俄罗斯的技术侦察和破坏等活动；利用现代化的信息手段，加强对国家秘密信息及受控信息的保护；建立信息安全威胁预警、检测及后果消除机制，大力发展威胁检测、预警和数据分析系统；加快信息基础设施建设，并加强对关键信息基础设施的保护；按照国际法准则和标准，加快研制高水平的信息传输设备；强化公民和全社会的信息防护能力；加大对信息空间活动的监管力度；禁止极端思想、暴力、种族、宗教和民族偏见的产品在信息网络平台的传播；推广使用更加安全的现代化信息设备；防范和打击网络犯罪等。

3. 加大自主可控信息通信技术研发

俄罗斯认为，缺乏具有竞争力的信息技术和产品，且关键技术和产品严重依赖进口，对于原本形势就比较严峻的俄罗斯信息空间建设来说无异于雪上加霜。为此，俄罗斯将发展“有竞争力的”的信息通信产业视为其信息空间建设的重要一环，将“提高信息技术水平列为俄罗斯保障科技和教育领域国家安全的重要方向”，并将发展国产的信息、网络和通信技术与产品列为俄罗斯联邦信息安全领域科学研究工作的主要方向①。

将信息通信技术列为发展重点。在俄罗斯近年发布的诸多文件中，信息通信技术都被列为重要或视为最具良好前景的高新技术，予以鼓励发展，其目的就是为俄罗斯的国家安全建设提供充足的技术基础和保障。在 2011 年确定的联邦科学、工艺和技术优先发展方向中，俄罗斯将“安全和反恐”和“信息通信技术”分别列为要第一和第三优先发展的方向。2012 年出台的《2013～2025 年电子和无线电电子工业发展国家纲要》②，则明确提出，要进一步加强电子工业基础能力建设，注重挖掘其科技创新潜力、提升国际竞争力，最终缩小与世界先进水平的差距，为俄罗斯社会经济发展和国家安全建设提供技术和产品保障。2013 年，研究制定了一个五年期的《俄罗斯信息技术发展路线图》③，明确了 2018 年前俄

① Основные направления научных исследований в области обеспечения информационной безопасностиРоссийской Федерации. http：//www. scrf. gov. ru/sevurity/information/document94/

② Государственная программа Российской Федерации "Развитие электронной и радиоэлектронной промышленности на 2013－2025 годы". http：//government. ru/programs/249/events/

③ План мероприятий ("дорожная карта")"Развитие отрасли информационных технологий". http：//government. ru/media/files/41d4b29db7c74fb

罗斯信息产业的发展目标和实施路径，指出要通过科技园区建设、加大技术研发、加强基础教育、予以税收优惠、加大国产产品的推广应用等手段，推动俄罗斯信息产业的发展，提升其能力与水平，在 2018 年实现 4 500 亿卢布的产业规模，并创造 90 亿美元的出口，使俄罗斯的“信息社会指数”排名提升至第 15 位①。2016 年出台的《信息安全学说》更是明确提出，为确保俄罗斯在信息空间建设过程中的安全，在科技和产业发展领域要重点做好以下工作：一是要大力发展信息领域的科技潜力（包括人才潜力），努力将信息技术和电子工业发展成为一个“创新型的行业”；二是要加快研制和广泛应用具有世界一流水平的国产信息防护技术、产品和服务，实现信息技术的自主可控，并建立稳定的技术体系；三是要创造有利条件，提升俄罗斯信息通信技术企业的竞争力；四是要发展国产电子元器件并提升其工艺制造水平，在保障国内市场需求的同时，打入国际市场；五是要针对具有发展潜力的信息技术和信息安全保障产品，开展科学研究和试验性开发。

加快实施进口替代。为了在信息空间不落后并受制于发达国家，俄罗斯政府主张大力发展高新技术，提升其工业竞争力和相关产品的国产化水平，主张通过加快思想转变、研发并采用现代化和创新性的技术推动整个国家经济发展。特别是乌克兰危机后，西方制裁更加坚定了俄罗斯政府推进进口替代工作的决心，以普京、梅德韦杰夫为代表的俄罗斯高层频繁发表讲话，并出台一系列政策和举措，加快推进俄罗斯的自主创新，以及产品和技术的进口替代工作。俄总统普京多次公开表示，必须要“减少对国外技术和工业品的严重依赖性”，并责令政府确定技术替代的临界点，明确优先发展的技术及领域，并要采取措施，确保这些替代技术能够在生产中迅速予以应用。在高层的极力推动下，俄政府相关部门从 2014 年就着手研究制定进口替代计划和进口替代投资项目清单，并通过加大政府投入和建立工业发展基金等多种手段，畅通融资渠道，扶持相关产业的发展，在其 2015 年初公布的 18 个进口替代优先发展领域中，信息通信技术就在其中。

4. 加紧谋划信息空间作战力量建设

俄军认为，网络时代，军事行动的中心已从传统的陆地和海洋转移到空天和

① 即 ICT 指数，该指数是由联合国负责信息通信技术事务的专业机构——国际电信联盟（ITU）研究制定和发布的、全面反映一个国家和地区信息化发展水平的指标体系，全称为“信息与通信技术发展指数”。该指标体系由 ICT 接入、ICT 使用和 ICT 技术三个一级指标和 11 个二级指标构成，其二级指标主要涉及信息化基础设施、信息技术的应用、居民的知识水平和能力、信息化发展环境与效果、信息消费情况等。

信息领域，尤其是信息空间领域。随着信息通信技术逐渐渗透到俄罗斯社会与生活各领域，互联网和其他信息空间的组成要素已成为俄罗斯经济社会发展的重要基石，“发展信息空间作战力量和资源”，捍卫俄罗斯联邦信息空间的安全，已成为俄联邦武装力量建设的一项重要使命。

2012 年，俄罗斯主管国防工业的副总理罗戈津对外宣布，俄将组建网络司令部，相关提案在国防部会议上业已获得审核通过。2013 年，俄国防部和总参谋部相关部门就组建网络司令部一事进行了专题研究，并对外宣布，计划组建一个新的兵种，用以防范各种网络攻击和威胁，形成俄罗斯自己的“防御网络威胁的数字盾牌”。

乌克兰危机期间，俄罗斯遭受了大量来自于境外的网络攻击，对其国家安全和军事行动造成了极大的威胁，加之美日等国不断加快网络空间作战力量建设，促使俄军也采取了对应措施。

2014 年，俄军总参谋部第八局局长库兹涅佐夫说，俄军“用于保障军事设施安全、免受来自外部网络攻击的专门机构”计划于 2017 年前正式组建完毕。据称，该部队在组建初期，将以国防部总局的编制形式存在，并将招募大量程序员，通过自行开发软件系统，用以满足军队网络防护的需要。俄军网络司令部的组建，将有利于俄军的作战装备、武器、作战指挥系统向高度现代化和数字化逐渐转变，推动俄罗斯全国的信息安全系统现代化进程。但有关俄军网络司令部的具体任务和职责，还在不断完善之中。

目前，俄内务部的调查局、联邦安全委员会的信息安全中心等机构，分别承担着调查俄罗斯境内的计算机犯罪、防御信息空间领域内的各种危及俄罗斯国家安全和经济安全的外国间谍、极端主义组织和犯罪机构的行动，俄军网络司令部建成后，将与上述机构一起，在捍卫俄信息空间安全领域形成“三足鼎立”之势。2017 年 2 月，俄国防部长绍伊古公开对外宣布，俄已组建了信息作战部队，该部队将整合俄武装力量、内务部和安全部门的相关人员，并借助外部专家的力量，共同遂行作战任务。尽管目前俄官员对该部队的职责鲜有谈及，但通过零星报道可以看出，该部队不仅具备网络防御能力，还将具备电子对抗、信息对抗等能力，将同时具备电子战、网络战、信息—舆论战等多重职能。目前，俄战略导弹部队已组建了负责检测和阻止网络攻击的“火山”部队，用以提高其陆基机动系统和导弹发射部队的网络安全防护。旨在应对和提升政府部门、金融机构、行业协会和执法部门网络安全事件的“国家信息安全响应中心”的组建工作，

也正在积极推进中。

5. 积极参与信息空间国际规则制定

俄罗斯认为，面对日益严峻的信息威胁，各国存在着共同利益与合作空间，建立一个安全、稳定、繁荣的信息空间，对世界各国来说都至关重要。为此，俄罗斯主张在相互尊重各国国家主权和相互信任的基础上，就保障信息空间安全、推进信息空间发展，开展实质性的对话与合作，共同构建和平、安全、开放、合作的信息空间新秩序，推进信息空间发展，更好地造福各国人民。其国家安全战略明确指出，“俄罗斯支持集体安全条约组织共同应对信息威胁，形成全球化的信息安全体系”，并主张与独联体及其周边国家建立更为广泛的“信息通信环境”。

俄罗斯倡导建立多边、民主、透明的互联网治理体系，并支持联合国在建立互联网国际治理机制方面发挥重要作用，主张在联合国框架内制定普遍接受的负责任行为国际准则。早在 2011 年，俄罗斯就提议联合国制定信息空间国际行为准则，以约束各国在信息空间的行为，但并未得到任何回应。直到 2015 年，当俄罗斯成功运用其先进的电子信息装备实施了对 IS 的打击，彰显了其在电子信息领域所拥有的技术优势和能力后，美国、英国、法国等 20 个国家代表组成的专家组，才向联合国提交了一份报告，同意俄罗斯的建议。同年 11 月，第 70 届联合国大会讨论通过了俄罗斯提出的关于“实现信息和远程通信领域国家安全环境”的决议，约定协议国间不得相互攻击关键信息基础设施，如核电站、银行等，不得在 IT 产品中安装“插件”，同时要联合打击网络犯罪和黑客。目前，同意该协议原则的国家已有 82 个。

6. 注重提升全社会的信息防护能力

为切实保障俄罗斯在信息空间的国家安全和利益，俄罗斯主张，要强化公民和全社会的“信息防护能力”，主张国家权力机关和地方自治机关要引导公民利用包括信息手段在内的，一系列政治、军事、组织、社会经济、法律手段保障国家安全，要通过推广使用现代化的信息设备，运用全社会的力量建立起全方位的防护体系。

鉴于在信息空间中，国家权力机关往往成为信息攻击的首要目标，为此，俄政府已启动国家信息通信网建设，用来提升政府机构应对网络攻击的能力。该网是一个专门用来为俄联邦政府和各联邦主体政府机关提供信息服务的专用网络系

统，各机构的信息系统和网络将通过一特殊的安全隔离装置——“安全隧道”接入该网，并通过数据加密进行信息传输。该网由联邦政府和各联邦主体共同出资建设，由联邦警卫总局负责运行维护。2018 年前，该网将正式投入运行，届时俄总统办公厅、联邦政府，联邦委员会、国家杜马，联邦法院、检察院、审计署等机构的信息系统及专用网络都将接入该平台，并利用其实现信息的处理、传输、发布和存储。

该网建成后，将为俄罗斯权力机关提供一个可最大限度避免网络攻击，并能实现机构间互联互通的网络平台，从而更加方便、快捷地实现国家管理和为公众服务的能力。据悉，为确保俄国家权力机关网络信息系统的安全，俄罗斯联邦保卫局正在会同有关部门，研究编制“国家权力机关信息系统和信息通信网目录”，以便对俄罗斯的政府网络系统进行全方位、无死角的网络监控和防护。同时，俄罗斯正在筹划建设一个更加安全的保密通信网，以满足相关部门对防范非法入侵的特殊要求。

三　存在的问题

纵观俄罗斯的信息空间建设，虽然起步晚于美国，但近两年发展较为迅速，特别是在顶层设计方面，形成了国家安全战略、军事战略与信息安全战略相互呼应、共同推进的战略框架体系，并开始投入力量加快推进信息空间建设，但与美国这一传统对手相比，仍存在着一定的差距。

首先是网络部队建设相对落后。尽管俄罗斯国防部长已公开表态，声称俄罗斯已组建了信息战部队，但相对于美国来说，俄罗斯的网络部队建设可以说相差甚远。早在九一一事件后，美国就将赛博安全列为国家安全的一个重要组成部分，2005 年便在其《国家军事战略》中提出，赛博空间列为第五作战域，并于 2010 年组建了赛博司令部[①]，2012 年开始启动专业化的网络任务部队建设。美国的计划是，在 2018 年前，建设 133 支、总人数在 6 200 人以上的专业网络任务部队。这 133 支网络任务部队又按职能划分为国家任务部队、作战任务部队和网络防护部队，将遍布陆、海、空军和海军陆战队。截至 2016 年底，这 133 支网络任务部队均已具备初始作战能力，并有一半以上具备完全作战能力。与美国相

① 目前，更多的人习惯称其为网络司令部。

比，俄罗斯的网络部队建设只能说仍处于起步阶段。

其次是国产技术和产品不能满足现实需求。信息空间建设离不开信息网络技术。在 1993 年美国提出信息高速公路建设、大力发展信息产业时，俄罗斯却处于国家动荡、百废待兴的时期，大量的人才外流，导致电子工业受到重创。经过 20 多年的调整和恢复，到 2011 年，俄罗斯电子信息产业的产值只有 120 亿美元，仅占据国际市场份额的不足 0.3%，国产电子产品占据国内市场份额还不到 20%①。俄罗斯的电子产品以内销为主，只有不到 25% 的产品出口②。尽管近年来，普京政府十分重视信息网络建设，但在国家经济形势整体没有根本好转、投入有限的情况下，这样的产业结构很难得到根本性的改善，远不能满足信息空间建设的巨大需求。

第三是网络防护差经常遭到攻击。俄罗斯的黑客在世界上享有“声誉”，最近的“黑客门”更是让人觉得俄罗斯的黑客似乎无所不能，从一个侧面证明了俄罗斯具备了一定的网络攻击能力。但与其相对较为强大的网络攻击能力而言，其网络防护能力却较弱。据联邦安全委员会的数据显示，2016 年，俄罗斯遭受了约 5 000 万次网络攻击，这一数字比 2015 年增长了 2 倍多，而且其中有 60% 来自于国外。究其原因，实施网络攻击主要是利用敌人的网络漏洞，而实施网络防护则需要强有力的经济保障，需要建设相应的防护系统，所以在整个国家经济不是很景气的情况下，其网络防护能力整体偏弱也就不难理解了。

第四是尚未建立军民一体化网络协调机制。信息空间的博弈，可打破时间和地域、军与民的界限，是最适合实现军民一体化联合的领域。美国在全力推进网络部队建设的同时，还通过“网络军团”项目在全国招募具有一定专业能力的网络人才，并通过在大学设立“卓越学术中心”、提供奖学金等方式，吸引计算机网络专业的学生进行人才储备。与此同时，美国还通过举办各种演习演练活动，增强军地各方在遇到网络突发事件时的协同能力，以提升整个国家应对网络安全事件的能力，其中“网络安全防御”“网络旗帜”“网络卫士”等演习活动都已成为品牌，美军的作战人员、军校学员、国民警卫队、国防供货商、政府官员、民间机构、学术研究机构乃至平民都可参与其中，在网络空间这一没有硝烟的战场上，真正做到了“全民皆兵”。而俄罗斯在这方面的工作明显还不够，其

① Государственная программа Российской Федерации "Развитие электронной и радиоэлектронной промышленности на 2013 – 2025 годы" .

② 其销往海外的大部分都是专用电子产品，而且大多是随着整机（如飞机、舰船等）一同外销的。

实施信息空间行动的主体仍以武装力量、安全部队和情报等部门的专业力量为主，政府及公众的参与度明显不足。

四　几点思考

通过对俄罗斯信息空间建设情况的梳理，以及存在问题的分析，笔者认为：

网络空间建设必须加强顶层规划，需要制定统一的国家发展战略。作为美国一直的假想敌，无论是在传统军事领域还是在网络空间这一新兴作战域，我国与俄罗斯面临着同样的威胁，面临的安全形势同样十分严峻。在综合国力还不够强的情况下，唯有举全国之力，通过统筹规划，充分发挥政治优势和组织优势，制定切实可行的发展战略，才可能在短期内缩短与发达国家的差距，以确保网络空间领域的国家安全和利益。

网络空间博弈说到底是技术和人才的竞争，必须加快核心技术的自主研发和人才培养。核心、关键技术和产品依赖进口，高端人才紧缺，是制约我国网络空间能力建设的短板。要想在这场没有硝烟的战争中争得主动，要加大对国产先进信息通信技术和产品的研发，要用创新的思维和方法，动员和招募军队和地方的高端人才共同探讨网络空间建设和装备的发展策略，以免受制于人。

网络空间建设关系到社会生产生活的方方面面，必须树立和提升全民的网络安全意识和防护能力。网络时代，软杀伤的威力不亚于硬摧毁。随着信息通信技术在社会各领域的广泛应用，网络空间的战场已拓展至社会生产乃至居民生活的方方面面。在网络战争中，没有军和民之分，任何系统都可能成为被攻击的目标。为此，要加快提升全民的网络安全意识和信息防护能力，以免出现木桶效应。

（责任编辑　李中海）