

一体化国家战略体系和能力建设中的安全风险研究

杨晓昕¹, 董支晓²

(1. 中国海洋大学国际事务与公共管理学院, 山东 青岛 266100;

2. 国防大学军事管理学院, 北京 100081)

摘要: 巩固提高一体化国家战略体系和能力是中国加快国防和军事现代化建设的重要路径, 在当前中美大国战略竞争加剧且国际政治环境动荡的背景下, 一体化国家战略能力建设中的国防科技产业安全面临新的风险与挑战。中国国防科技工业在国际政治互动中形成的高度集中的市场结构、大国竞争状态下的非公主体低可靠性, 以及一体化实践中的信息扩散与泄密, 共同组成了国防科技工业一体化战略能力建设的核心风险要素。通过新兴领域科技主体培育优化国防科技工业产业组织形态, 基于风险识别、风险评估和风险处理措施管控非公主体风险, 构建系统、完善的信息化保密管理体系, 提升关于中国国防现代化建设的国际话语权, 是当前化解和治理一体化国家战略能力建设的安全风险的重要方式。

关键词: 一体化国家战略体系; 军民融合; 国防科技工业; 风险治理

中图分类号: D616

文献标识码: A

文章编号: 1005-0566(2024)02-0018-09

Research on security risks in the integrated national strategies and strategic capabilities building

YANG Xiaoxin¹, DONG Zhixiao²

(1. School of International Affairs and Public Administration, Ocean University of China, Qingdao 266100, China;

2. Military Management College, PLA National Defense University, Beijing 100091, China)

Abstract: Consolidating and enhancing the integrated national strategies and strategic capabilities is an important path for China to accelerate its national defense and military modernization. In the context of the intensifying strategic competition between China and the United States and the turbulent international political environment, the construction of an integrated national strategic capabilities brings risks and challenges to the security of the defense science and technology industry. The highly concentrated market structure formed by China's defense science and technology industry in international political interactions, the low reliability of non-state actors under the condition of major power competition, and the information diffusion and leakage in integrated practices, together constitute the core risk elements of the integrated strategic capability building of the defense science and technology industry. Optimizing the industrial organization form of the defense science and technology industry through the cultivation of emerging field technology entities, controlling non-state actor risks based on risk identification, risk assessment, and risk mitigation measures,

收稿日期: 2023-10-20 修回日期: 2023-12-28

基金项目: 中国博士后科学基金项目“‘军民融合’驱动下国防工业创新的机理、效应及路径研究”(2022M722991); 山东省自然科学基金项目“山东省国防工业产业链协同创新的机理解析、能力评估及策略设计”(ZR202211140071)。

作者简介: 杨晓昕(1993—), 女, 山东青岛人, 中国海洋大学国际事务与公共管理学院讲师, 博士, 研究方向为国防经济、军民融合、国防产业安全。

building a systematic and comprehensive information security management system, and enhancing international discourse power regarding China's defense modernization are currently important ways to resolve and govern the security risks of integrated national strategic capabilities construction.

Key words: integrated national strategies and strategic capabilities; military-civilian integration; defense science and technology industry; risk governance

当前,世界地缘政治风险加剧,地区冲突和局部战争持续不断,国际安全体系和秩序受到冲击,国家安全面临的不稳定性、不确定性更加突出。实现国防现代化是当前复杂国际背景下实现中华民族伟大复兴的坚强有力战略支撑,也是中国强军之路的发展方向。面临中美大国战略竞争的严峻挑战,封闭、孤立和依赖有限资源的国防科技工业体系将难以对抗基于国家一体化实力的国防工业基础,中国迫切需要打通军—民系统之间的隔阂,巩固提高一体化国家战略体系和能力。2015年,以统筹“富国”和“强军”为核心目标的“军民融合发展”(以下简称“军民融合”)正式上升为国家战略。军民融合通过促进军—民系统之间全领域、全要素、全方位的物质信息流动,从而形成军民兼容、相互协调和良性互动的开放系统,在提升国防创新活力的同时实现社会资源要素的最优配置,催生强大的一体化国家战略能力^[1]。

就生产研发部门而言,中国国防科技工业在部分上仍延续着计划经济体制下的组织管理模式,政府在经济运行中扮演着重要角色。相比于西方发达国家,中国国防科技工业的历史演化进程具有特殊性,中国坚持的中国特色社会主义意识形态、中国特色社会主义市场经济体制、中国特色大国外交和大国政治使中国国防事业在发展过程中承受巨大压力和阻力,中国国防科技工业也因此演化形成了高度集中的产业组织结构。随着军民融合战略的推进落实,国防科技工业需要吸纳大量社会主体参与,社会主体的“理性人”行为方式以及在经营理念、组织管理和价值规范等方面与传统军工主体之间的巨大差异,导致当国家面临外部政治风险时,中国国防工业特有的产业组织结构与非公主体的自利行动策略混杂交织一处,产生与国家利益相违背的结构性风险。当前,

中美大国战略竞争局势紧张激烈,中国面临的安全环境和风险挑战比以往更加错综复杂,统筹协调国防安全与经济发展面临巨大的国际政治压力,因而在国家一体化战略能力建设的进程中,更需要切实关注军民融合实践伴随的潜在风险。

纵观现有研究,对军民融会议题的探索通常聚焦于国防工业的经济效率和技术效率,存在“去政治化”的研究惯式,缺少国家安全视角下的风险探讨。在当前科技与政治的关联度愈加提升的背景下,军民融合实践中的风险因素分析薄弱不仅会导致对现实解释力不足,更会导致对国家安全风险预判、评估及治理的缺位,可能造成武器装备生产研发工作停滞、延期,技术指标不达预期,甚至关键技术和计划泄密,进而威胁国家安全和战略利益。因此,本文基于产业视角,从产业组织结构、产业参与主体和产业知识溢出3个维度深入探究军民融合实践中的风险形成的逻辑、动因和发展路径,并提出系统性的风险治理策略。本文研究结论对维护国家国防科技安全、保障国家重大战略部署实践具有重要意义。

一、高度集中市场结构下的产业链韧性风险

市场结构是产业组织理论中的重要概念,是指一个产业内的公司数量、产品的替代性程度、市场进入退出的难易程度等关键特征。国防工业往往具有高度集中的市场结构,只有少数大型公司提供高技术的军事装备,这种市场结构与产业组织中的寡头垄断或寡头竞争模型相似,且政府通常会进行干预和规制以维护国家战略利益。中国在新中国成立后第一个50年中,最迫切的政治和军事利益就是建设一个独立自主的国防科技工业体系,减少对外国军事技术和装备的依赖,避免受到外部大国的控制和威胁。政府直接管理是短期

内建设完整国防工业产业门类、调节军工科研生产资源配置的唯一方式。自新中国成立以来,政府在国防工业运行中长期发挥着全能性职能。随着建国后抗美援朝战争、对越自卫反击战、中印边境自卫反击战和台海问题的紧张化,对武器装备的巨大需求促使政府不断强化对国防工业的宏观管理。与此同时,美国主导的多边组织“巴黎统筹委员会”(coordinating committee on export control,以下简称“巴统”)通过严格的禁运政策阻止社会主义国家获得先进技术,并专门成立针对中国的小组委员会(CHINCOM)强化对中国技术获取的审查^[2],使中国难以从西方国家获取军事武器系统。随着中苏关系的破裂,苏联停止了对中国的军事援助和技术转让,中国武器装备技术的供给渠道被彻底封锁,政府需要承担国防科技发展的全部风险和沉重经济负担,这进一步深化了中国国防事业独立自主、自力更生的发展理念。在紧张的地缘政治局势、长期的意识形态对立和严格的武器禁运限制背景下,中国组建了涵盖航空、航天、船舶、兵器、电子、核的国防科技工业体系,产业组织形态高度集中。直至今日,中国军工集团经历数次改制、拆分与重组,核心军工资产的市场集中度水平依旧维持在高位^[3]。

随着当前新一代信息技术飞速发展,民用领域的海量需求催生以信息化、智能化、数字化为代表的商业技术群快速发展,民品所处的激烈市场竞争环境保障了其产品技术性能的前沿性、时效性和灵活性,对社会力量的吸纳可以有效提升军事科技创新活力。然而在国防科技工业的高集中度市场结构下,军民一体化能力整合过程中的风险也随之显现。传统意义上的产业组织安全认为产业集中度是反映产业竞争力的一个重要指征,企业的市场集中度越高,企业的国际竞争力越强,产业越安全^[4]。但在非公主体嵌入国防科技工业基础的发展背景下,高集中度的产业意味着风险同样高度集中,当市场由少数供应商主导时,供应链对外部冲击更为敏感,外部环境不稳定或商业

制裁以及由此造成的供应商的生产中断或失败可能会对国防科技工业系统造成广泛的影响。国际政治极端环境下的供应链受阻及交付延迟等一系列情况将导致高技术产品技术链、创新链、供应链断裂,单个企业的风险上升为整个产业的风险,进而危及国家经济和军事安全。与此相反,多样化的生产主体可以实现供应链韧性(supply chain resilience),更好地分散和化解风险,降低风险发生的负面影响。一体化国家战略体系的建设过程中要求加强军事和民用部门之间的合作与协同,非公主体的嵌入增添了国防科技工业产业链条中的风险节点,而当前中国高度集中的国防科技工业市场结构并不存在充分的冗余和弹性空间化解这类风险,一旦由“民参军”主体引发的风险要素发展成为现实,将对这个产业链条上的生产活动造成系统性破坏。

相较之下,美国拥有一个建立在大型国防承包商和广泛中小企业之上的军民一体化的国防工业基础(defense industrial base),以洛克希德·马丁、波音、诺斯罗普·格鲁曼、雷神、通用动力等为代表的大型国防承包商在不同武器产品领域互相竞争、互为备份。虽然大型国防承包商同样存在较高的产业集中度水平,但每个产品大类至少保障两个不同的国防承包商可以提供替代性选择(见表1)。美国却仍然对这种市场结构保持高度警惕,认为其存在任务风险和国家安全风险。国防部指令 5000.62 要求严格限制国防承包商的并购交易(mergers and acquisitions, M&A),包括以收购与其产品或重叠业务为目标的水平合并以及以收购供应链上下游公司为目的的垂直合并,由反垄断机构对并购交易产生的垄断后果及反竞争影响进行审查评估,避免关键技术产品的生产过程被封锁于单一公司内部^[5]。同时,美国通过军民两用技术标准的普及与大量中小企业建立深度合作,形成广泛、分散的军工生态体系,这类企业创新活力高,专利申请数量是大型企业的 16.5 倍,构成美国高科技工作岗位的 43%。美国长期致力于培育参

与国防工业的中小企业,来打造具有多样化能力的可替代性供应商,增强国防工业基础的弹性和韧性。在2011—2021年,美国国防部对小型供应商研发服务的购买支出增长了83%,在小型供应商的产品购买支出增长了28%。至2021年,国防部的小型供应商的支出高达803亿美元,创下历史新高^[6]。此外,美国还通过“其他交易”(other transaction, OT)和“开放性商业方案”(commercial solutions opening, CSO)等不受《联邦采购条例》(FAR)约束或简化采办程序的国防采购模式,促进传统和非传统国防承包商、学术界、非营利组织和其他小型企业积极迅速地参与广泛的武器装备原型研发生产^[7]。通过国防创新单元(DIU)、国防创新市场平台(defense innovation marketplace)、国家安全创新网络(national security innovation network)、梦之港(dream port)、空军创新工作坊(AFWERX)、海军创新工作坊(NavalX)等项目扩大国防工业基础的参与主体^[8]。

表1 美国武器装备类型及核心承包商

武器类型	核心国防承包商1	核心国防承包商2	核心国防承包商3
战术导弹	洛克希德·马丁	波音	雷神科技
固定翼飞机	诺斯罗普·格鲁曼	洛克希德·马丁	波音
消耗型运载火箭	洛克希德·马丁	波音	—
卫星	诺斯罗普·格鲁曼	洛克希德·马丁	休斯
水面舰船	通用动力	亨廷顿英戈尔斯	—
战术轮式车	美国汽车综合	豪士科	通用汽车
战略导弹	洛克希德·马丁	波音	—
鱼雷	洛克希德·马丁	雷神科技	—
旋翼飞机	洛克希德·马丁	波音	贝尔

二、非公参与主体的低可靠性风险

非公企业是一体化国家战略体系建设中的重要参与者,但是作为利益驱动型主体,当非公企业社会责任行为与企业的逐利行为冲突时,其有动机以牺牲相关者利益为代价追求利润。非公企业对其社会责任采取“为我所用”的策略,相较于公有制企业,其背离了社会责任不可推卸的属性与原则,导致企业存在责任的缺失^[9]。参与国防科技工业生产科研实践的非公企业既不受国家意志下的行政命令干预,又无规模庞大稳定的国有资本支持,军民主体之间不对称的利益目标与价值

追求、组织性质与文化差异,以及创新资源制约、信息不对称等因素,都导致了双方在面对国际政治环境和国家安全局势变化下行动逻辑的差异化。

装备的研制是一个庞大而复杂的系统工程,包括具有复杂结构的技术体系和从设想到实践的复杂系列关系^[10]。基于多主体配合实现的协同活动由于其过程的多元性、交互性和动态性,不可避免地导致了相关实践处于高风险水平,影响了实际效果并可能导致合作失败。针对协作研发项目的风险分析发现,大量协同创新项目由于合作环节出现障碍而被放弃或推迟^[11],其中道德风险、产权风险、利益分配风险、协调风险、资金风险、技术风险等内部风险因素,以及环境风险、政策风险、市场风险、政治风险等外部风险因素都是导致项目失败的重要原因。当前现代化战争样式快速发展,传统战争正向“信息战争”“混合战争”“多域战争”“马赛克战争”等非传统形式转变,武器装备的信息化、自动化、集成化、智能化特征不断凸显,这对知识和技术先进性提出了更高要求,其研制过程相比一般装备更为复杂,具有高度不确定性^[12]。这就意味着可能存在科研方案随着工作的深入而进行必要的修正,随着时间的推移增加新技术的采用,以及技术上的反复和局部的失败等,并导致军民多主体之间的协调配合更加困难。可以判断当非公主体面临关键技术产品获取受阻、国际市场业务冲击、经营利润下降、财务风险加剧等外部冲击时,其市场化的行为逻辑将导致项目停滞、履约中止、产品质量下降等系列道德风险及泄密等风险后果。

非公企业自身经济利益与国家政治利益相冲突所引发的企业社会责任缺失存在隐蔽性和长期性、从众性和常态性、破坏性和不可逆性等特征^[13],使得一体化的国防工业体系需要面对来自非公企业的不可控、不确定的风险因素。自军民融合发展战略实施以来,中国参与武器装备研发的单位数量不断增多,非公企业开始逐步参与国

家重大项目^[14],非公有资本通过参股、控股、兼并和收购等多种形式参与一般武器装备及配套产品生产的军工企业改组改制,加大资本市场运作^[15]。然而当前,中国非公主体参与国防工业生产活动的军民融合培育期和发展期与中美大国博弈的“窗口期”恰巧重合,不利的国际政治环境为中国一体化国家战略体系建设和能力生成增添了阻力。来自美国的商业制裁、美国盟友的联合围堵,以及外部合作伙伴对政治风险的担忧都会波及中国“民参军”企业的正常经营活动。

“军民融合发展”上升为国家战略以来,美国国会、政府、智库等在内的美国战略界对中国军民融合战略密切关注,并认为中国追求科技强军的军民融合对美国全球创新领导地位及军事优势构成了“前所未有的威胁”^[16]。美国国务院发布的中国军民融合战略说明性文件“什么是军民融合”(“What is MCF” one pager)将中国军民融合污蔑为通过“民口”主体窃取转移军民两用技术的战略手段^①。美国“战略与国际研究中心”(CSIS)、“新美国安全中心”(CNAS)、“国家亚洲研究局”(NBR)、“安全与新兴技术中心”(CSET)等纷纷将火力瞄准军民融合战略,渲染其对国际安全的负面影响^[17]。美国还通过一系列手段对“支持中国军队和国防组织”的商业行为进行制裁。美国商务部工业安全局(BIS)《出口管理条例》(EAR)4号补充文件744条款实时调整实体清单(entity list)、军事最终用户清单(MEU)、中国共产党涉军企业清单(NS-CMCC)、中国军工复合体企业清单(NS-CMIC)和中国涉军企业清单(CMC/1260H)等对华制裁对象^②,名单不仅涉及以十大军工集团为代表的中国军工核心主体,更有广泛的从事半导体、计算机、人工智能、信息服务、智能装备制造的非公企业。同时,美国国务院和国土安全部对中国赴美留学生实施签证筛查,停发“涉军”高等院

校、“军民融合”相关学者和学生签证,执行限制军民融合人员入境的行政令;美国国防部加强对国防采购合同的审查,禁止国防承包商供应链内涵盖中国企业;美国财政部牵头“外商投资审查委员会”对央企赴美投资加强安全审查,禁止美国投资者持有被列入黑名单的“军民融合”股票。

美国各项制裁措施直指中国“涉军”主体,自2017年开始的美国对华科技战可以被视为美国政府面向中国军民融合战略的精准打击^[18]。这本质上源自美国霸权主义和冷战思维的“双重标准”。一方面,美国已经形成了融合大型国防承包商、广泛中小企业、国防部高级计划研究局(DARPA)、美国国家创新网络(NSIN)、国防创新单元(DIU)和各军兵种军民协同创新培育项目的一体化国防工业基础;另一方面,美国却坚决否定中国实施军民融合战略和构建一体化国家战略能力的正当性,污名化中国统筹协调国家社会军民科技资源的进程,并通过各类制裁手段予以阻碍。然而,迄今为止,国内学界大多只关注美对华贸易战、科技战、地缘政治围堵和意识形态挑斗,对于美国误解、污名化、防范和打压中国军民融合战略的行为重视不足,这也给中国一体化国家战略体系 and 能力的建设留下了风险发生的空间。当前,“西强中弱”的国际话语传播格局并未发生根本性转变,这也使得中国在军民融合战略推行上声量小,中国实践军民融合战略的合理性、西方国家军民融合发展方式的普遍性等事实无法有效传播,中国民参军企业的正常商业活动可能需要长期面临来自美国的无端干扰和打压,进一步降低了非公主体的参与意愿和国防科技工业对商业力量的有效整合。

三、军民主体互动中的保密风险

中国是个有着悠久保密传统的国家。中国古人很早就认识到保密的重要性和必要性。《周易·系

① U. S. Department of State, <https://www.state.gov/remarks-and-releases-bureau-of-international-security-and-nonproliferation/what-is-mcf-one-pager/>, 2024-01-07。

② U. S. Department of Commerce, <https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear>, 2024-01-07。

辞上》：“君不密，则失臣；臣不密，则失身；凡事不密，则害成”；道家代表人物老子则提出“鱼不可脱于渊，国之利器不可以示人”^[19]；宋代兵书《翠微北征录》则论述得更具体，“我秘敌泄，则胜常在敌；敌秘我泄，则胜常在我”^[20]。近代历史上，中国共产党成立面临反动军阀的镇压以及国共两党的紧张斗争，这都要求中国共产党以严格恪守保密要求为己任，毛泽东同志指出“保密就是保生命，保胜利”^[21]。20世纪80年代末90年代初，邓小平同志基于对中国国情的深刻认识和世界局势的全面把握，提出了“韬光养晦”的外交战略思想。“韬光”即隐藏光芒、锐气、才华和能力，这被西方国家认为这是一种对国家政治、经济、军事真实情况秘而不宣的“战略模糊”（strategic obscurity）^[22]。公开军事信息会让敌对国家或团体更容易评估中国的实际军事能力，从而降低战略优势或增加风险。与之相反，保密可以提高军事战略的不可预测性。作为军事能力后发国家而言，这种不可预测性是军事策略的重要补充。当敌对方无法获知我方真实意图、能力或计划时，将被迫在多个可能的场景中作出决策，从而消耗其资源和注意力，且当敌对方信息缺失时，将倾向于避免冲突，从而增强我方的战略威慑力。

国防保密工作长期以来都是党和国家的一项重要工作，军工企业是履行国防保密义务的核心主体。军工企业所涉及的国家秘密可以大致分为两类：一是战略型秘密，即军工企业生产的武器系统型号、产量、交付时间、军品募集资金和投资项目信息建设信息等，其中隐含国家国防战略布局规划，可以推测国家的军事意图；二是国防技术性秘密，主要针对国防专利等先进武器系统应用技术和前沿基础知识，代表了国家在军事领域的竞争优势，泄露关键技术或设计细节可能使其他国家或竞争对手受益，从而削弱国家的战略优势。“国家利益高于一切”的核心价值观，决定了军工企业的定密事项范围广、保密工作要求严、政治素质要求高^[23]，并基于此形成了集保密意识、保密管理体

系、责任追究机制等于一体的军工保密文化。保密教育作为军工企业入职培训的“第一堂课”，已经成为军工人的职业素养和习惯。为了避免可能的风险或问题，军工企业不仅针对本单位在研项目的技术方法原理和项目状态，还包含对上级单位和上下游配套企业的广泛要求，尽可能地避免敏感信息泄露^[24]。

在一体化国家战略体系的发展要求下，军民力量的系统性整合要求社会技术、人才和资源实现开放、合作和共享，这给国防工业的保密工作带来了新的挑战^[25]。以知识溢出过程为例，知识溢出是指不同主体之间通过直接或间接方式进行互动交流，并在此过程中实现知识、技术和信息从一个主体传递到另一个主体的现象。知识溢出是重要的主体协同创新路径，可以为组织提供外部的思路和视角，实现新技术和新方法的快速有效传播，避免在相似研究领域的重复工作。随着军民融合实践中不同类型参与主体的数量增加，信息和知识的横向流动频繁，敏感信息泄露或盗窃的风险随之越大。在 Walker 等^[26]设定的军民产品分类等级列表中，越往下产品的通用属性越强、军民主体在产品供应链上的合作关系也愈加密切，随着一体化国家战略能力的整合性加强，非公民用主体参与国防生产的数量增多且参与环节将向产品生产链条上游移动，而其所涉及的保密信息与技术将可能随全社会资源要素的整合程度加深而向外部扩散^[27]。就“民参军”活动而言，非公有制企业可以在完成保密资格审查的前提下申请二级、三级保密资格，申请承担涉密武器装备科研生产任务^[28]。然而，由于民营企业保密意识多以保守商业秘密为主要内容，其内涵远不如军工企业丰富，日常敏感信息处理经验缺失，操作程序也不及军工企业复杂，因而可能形成相关涉密信息的非正式扩散，如具备专业化知识的个人之间信息与构想的非正式交流，各类型的商务洽谈、闲谈交友、聚会活动等，都可能成为敏感信息的扩散渠道。在这个过程中，一体化战略体系能

力建设和保密安全任务之间将产生溢出倾向和信息保密需求的冲突。一方面,一体化国家战略体系和能力的建设过程需要实现对信息不对称和信息壁垒的破除,该过程可以基于产业链的信息流动交换和知识溢出突破结构性障碍,实现对相关联高技术产业创新绩效的有益促进。另一方面,国防科技工业涉及大量涉密型号的研制生产任务,是敌对势力重点关注的对象,各类情报机构的窃密、渗透、策反活动频繁多样,泄密风险大,一体化国家战略体系和能力的建设拆除了涉密知识的非正式传播和扩散的隔离墙。因此,从安全领域审视一体化国家战略体系的建设,其所促进的知识溢出过程是一把双刃剑,在提升技术创新效率的同时也会对国家保密安全维护造成隐患。

新时期国家安全的外延有了大幅拓展,已不再局限于传统的国防和军事安全,经济、文化、信息等领域的安全保护工作愈显重要。在互联网技术飞速发展的大背景下,对信息掌握的质与量成为国家软实力和竞争力的重要标志。发达国家在搜集及窃取他国信息方面具有的优势更加明显,因此保护秘密信息之于国家安全的实现意义重大。随着国际政治格局多极化、经济全球统一不断向纵深发展,国家受到的竞争与挑战变得多元,维护信息安全、保障机要秘密不泄露是推进国家安全发展的重要前提。

四、一体化国家战略体系和能力建设的风险治理

总体来看,中国国防科技工业的一体化国家战略体系和能力建设存在结构风险、主体风险和保密风险三位一体的风险来源。其中,结构风险表现为国防科技工业高度集中的市场结构导致的产业链低韧性问题,一体化能力建设中单个企业风险易随产业链向上下游传导造成风险蔓延和扩散,进而危及国防安全。主体风险主要体现在非公主体经济理性驱动下的自利性动机与国家利益冲突。过去的长期军民分离状态导致非

公主体在市场逻辑、组织管理、文化规范等方面与国有军工集团存在巨大差异,协同难度大,且在当前美国有针对性地阻遏中国军民融合实践的背景下,主体风险发生的可能性进一步提高。保密风险是一体化能力建设过程中必须权衡的重要命题,一体化国家战略能力建设将使得国防科技工业参与主体增多、参与事项范围扩大、信息流通频繁,中国历来奉行的保密战略文化和一体化发展的必要方式之间存在冲突,并将对国家国防信息安全产生冲击。中国一体化国家战略体系和能力建设的风险问题内生于国防科技工业自身的历史发展沿革、国家战略文化,以及所面临的国际政治环境,做好风险的预先防范和管控治理对于有序推进一体化国家战略体系和能力建设至关重要。

(一) 优化新兴军事技术领域产业组织结构

在产业组织结构方面,中国高度集中的国防科技工业体系保障了它的存在和发展都源自国家意志,资源、技术和人才可以根据国家的长期战略目标进行统筹配置,通过集中力量的方式推进大型项目或关键技术的研发。应在保持军工核心资产所有权属性基本不变的情况下基于中国商业领域技术优势,聚焦未来新军事变革,有针对性地发展“互补性”的“民技军用”实践领域,重点识别人工智能、无人系统、大数据分析和决策支持、智能传感与感知技术等与传统武器系统具有“互补性”的产业领域的军用潜力。积极谋求在“赛场转换”的过程中打破传统军工集团长期发展积累的技术垄断,超前培育新兴军事技术领域的有效竞争格局,实现对传统国有军工集团高技术能力的有益补充。同时,还应坚持放宽市场准入、完善竞争规则的正确改革方向,通过军民两用技术和标准的制定破除行业壁垒,沿着加强反垄断执法合作的思路,积极推动国务院反垄断执法机构与军方建立联合审查机制,有效预防和制止军工企业垄断行为,为一体化国家战略体系的整合培育提供制度保障。

(二) 制定完善的一体化国家战略体系风险管理方案

在当前国际环境不稳定、不确定性增强的时代背景下,中国在巩固提升一体化国家战略体系和能力的实践过程中需要通过风险识别、风险估计和风险评价等方式对实践过程中所涉及的风险实行有效的控制。通过采取主动行动规避风险事件,妥善地处理“民参军”主体可能造成的风险后果,以最小的成本保证安全、可靠地推动实践目标的达成。包括形成一套关于“民参军”非公主体风险评估的完整全面的风险管理策略,在明确风险环节、界定风险等级、跟踪风险变化、拟定风险方案等方面形成规范性文件,建立使用风险管理信息系统,共享风险管理信息的政策、程序和事项,并使用大数据手段分析处理信息并做出相关风险预判。基于中美大国竞争所引发的科技制裁现实背景,需要格外关注民参军主体在国际市场的活动及其可靠性,定期评估采购、销售、合作市场的双边政治风险,考虑与不同地域和国家进行多元化合作,避免对某一国家或地区过度依赖。除了进行风险分析和风险管理外,还应探索建立分阶段的军民协同发展目标,在装备研制阶段提倡“民参军”主体采用经过验证的可靠技术,通过军民两用标准的普及尽量选用成熟的市场化产品,采用渐进方式,积极稳妥地开展装备研制工作,避免出现重大失误。

(三) 建设现代信息技术支撑的科学保密管理体系

随着一体化国家战略体系从战略构想层面逐步向动作实践层面迈进,将必然推动技术、人才、信息等资源在经济领域与国防领域的充分共享,面临以开放融合、协同共享为基本前提的一体化发展需求和国内外复杂的政治环境,需要有效平衡国防领域保密安全和一体化能力建设过程中广泛外部主体参与的关系。首先应提升军工单位的保密工作的精细化管理水平,深化科学定密工作,尽快完成从“程序规范”到“精准识别”的转变,采

取“保核心、保重点、保要害”的原则,反对过度定密、过度保护。允许军工企业应与下游产商间建立完善的沟通协作机制,促进军工企业与社会主体之间就非保密技术信息开展的公开交流与讨论,保障一体化国家战略体系和能力建设中对信息整合的基本要求。同时,针对一体化国家战略体系下将有更多内部人员接触组织敏感数据并对国家安全构成威胁的情况,需要通过改进的信息技术手段平衡知识信息交流需求和保密安全管理的关系,完善涉密数据存储、涉密数据操作、涉密数据追踪的过程管理,以高技术手段保护国家秘密。

(四) 提高中国一体化国家战略体系建设的国际话语权

巩固提升一体化国家战略体系和能力是中国在深刻把握全球发展趋势的基础上,以维护自身利益、突破霸权遏制、平等参与国际事务为目标所凝练出的统领国家发展的重要思路,有助于构造和谐、安全的社会发展环境和稳定的国际秩序。中国需要进一步强化关于一体化国家战略体系建设的内涵、方式、历史沿革、中西方对比等理论观点的输出,宣传中国国防事业发展和军事武器装备建设的基本原则,同步推进军队、学界、工商业界、智库、媒体等共同参与发声,揭露美国在发展军民融合问题上的双重标准和霸权逻辑。通过加强与其他国家的多边外交努力,寻求国际支持和合作,在国际舞台上提升话语影响力,争取大部分知华友华的国际舆论支持。需要特别注意到,长期以来,美国针对中国涉军相关企业、高校、科研院所和研究人员的打压和制裁行为有增无减。在预期中美战略竞争基调将长期持续的大环境下,“回避型”策略不利于中国国防和经济现代化的放弃发展,中国应构建系统的一体化国家战略理论和实践体系,合理平衡其内在风险与收益,应对外部威胁,特别是对与美国相关的国防科技工业安全风险做到预前评估,提前部署,降低美国行动对中国一体化国家战略体系建

设的负面影响。

参考文献:

- [1] 廉振宇, 顾桐菲, 薛奇, 等. 一体化国家战略体系和能力研究: 概念、框架与构建途径[J]. 科学学研究, 2023, 41(4): 615-622.
- [2] BRÄUNER O. Western arms exports to China[J]. SIPRI policy paper, 2015: 43.
- [3] 梅阳. 军民融合的政治经济学分析[D]. 北京: 国防科技大学, 2019.
- [4] 何维达, 何昌. 当前中国三大产业安全的初步估算[J]. 中国工业经济, 2002(2): 25-31.
- [5] ROBERT O W. Department of defense directive 5000. 62: review of mergers, acquisitions, joint ventures, investments, and strategic alliances of major defense suppliers on national security and public interest[R]. United States Department of Defense, 2017.
- [6] Office of the Under Secretary of Defense. State of competition within the defense industrial base[R]. United States Department of Defense, 2022.
- [7] JOHN M T. Defense commercial solutions opening[R]. United States Department of Defense, 2022.
- [8] United States Department of Defense. National defense science & technology strategy[R]. United States Department of Defense, 2023.
- [9] 张圣兵. 企业承担社会责任的性质和原因[J]. 经济学家, 2013(3): 49-52.
- [10] 麦强, 陈学钊, 郭亚男, 等. 复杂性视角下武器装备研制项目混合治理模式研究[J]. 公共管理学报, 2019, 16(4): 132-141.
- [11] HYLL W, PIPPEL G. Types of cooperation partners as determinants of innovation failures[J]. Technology analysis & strategic management, 2016, 28(4): 462-476.
- [12] 张西林, 谭跃进, 杨志伟. 多重不确定因素影响下的高端装备研制任务流程优化[J]. 系统工程理论与实践, 2019, 39(3): 725-734.
- [13] 姜丽群. 国外企业社会责任缺失研究述评[J]. 外国经济与管理, 2014, 36(2): 13-23.
- [14] 湛泳, 赵纯凯. 军民融合推动产业结构优化升级的路径与机制: 基于产业外部性视角[J]. 北京理工大学学报(社会科学版), 2017, 19(1): 116-123.
- [15] 何瑛, 杨琳. 改革开放以来国有企业混合所有制改革: 历程、成效与展望[J]. 管理世界, 2021, 37(7): 44-60.
- [16] BITZINGER R A. China's shift from civil-military integration to military-civil fusion[J]. Asia policy, 2021, 28(1): 5-24.
- [17] LASKAI L. Civil-military fusion and the PLA's pursuit of dominance in emerging technologies[J]. China brief, 2018, 18(6): 12-6.
- [18] 刘建华. 美国战略界对中国“军民融合”发展战略的认知与行为反应[J]. 复旦学报(社会科学版), 2022, 64(4): 192-204.
- [19] 刘泽华. 先秦政治思想史[M]. 北京: 人民出版社, 2008: 344.
- [20] 华岳. 翠微北征录·将帅小数·反泄[M]. 北京: 解放军出版社, 1992: 663.
- [21] 严雪林. 革命战争年代中国共产党保密思想述略[J]. 档案与建设, 2009(9): 8-10.
- [22] CAMERON R, RYAN S. Competing with China today[J]. Journal of indo-pacific affairs, 2021, 4(2): 52-66.
- [23] 邱红, 刘志鹏, 文梁. 军工企业保密风险管理的创新实践[J]. 保密工作, 2020(2): 52-53.
- [24] 刘尧. 完善军工企业保密管理体系的若干思考[J]. 国防科技工业, 2019(8): 64-66.
- [25] 刘晴阳, 蔡铭杨, 李娟. 关于“民参军”企业保密工作的分析与思考[J]. 中国军转民, 2022(9): 58-59.
- [26] WALKER W, GRAHAM M, HARBOR B. From components to integrated systems: technological diversity and interactions between the military and civilian sectors[M]// The relations between defence and civil technologies. Dordrecht: Springer, 1988: 17-37.
- [27] LAVALLEE T M. Civil-military integration: the politics of outsourcing national security[J]. Bulletin of science, technology & society, 2010, 30(3): 185-194.
- [28] 刘尧. 完善军工企业保密管理体系的若干思考[J]. 国防科技工业, 2019(8): 64-66.

(本文责编: 辛 城)