DOI 10.15302/J-SSCAE-2024.03.015

科技安全风险监测预警体系构建研究

刘晓峰[1]，胡高强[1*]，范兆媛[1]，隋秀峰[2]

（1. 南京邮电大学社会与人口学院，南京 210023；2. 北京理工大学国家安全与发展研究院，北京 100081）

摘要：地缘政治下的科技革命，加剧了我国科技安全风险，构建我国科技安全领域风险监测预警体系，对维护科技安全乃至国家安全具有重要意义。面对我国科技领域的博弈加剧风险、技术自主可控风险、技术应用失当风险、科技人才发展风险，解码科技安全领域风险监测预警体系运作的内在逻辑，通过技术手段赋能风险监测预警体系构建，并提出保障策略。研究认为：科技安全风险监测预警需以制度支持、跨域合作、信息共享、智力参与、产业治理、科技赋能六个方面作为逻辑前提；在系统论视角下，通过设立指标体系、明确监测预警流程、搭建分模块模型，来构建科技安全领域风险监测预警体系；为保障监测预警体系的有效实施，国家需完善相关法规与落实行业标准、拓展新技术的融入方式、完善应急响应机制与协同机制、建立监测预警指导机构、加强人才培养与队伍建设、促进科技创新与科技安全的融合发展，以确保监测预警体系高质量运行。

关键词：科技安全；科技安全风险；风险监测预警；科技创新

中图分类号：TP399　　**文献标识码：**A

Construction of a Technological Security Risk Monitoring and Early Warning System

Liu Xiaofeng[1], Hu Gaoqiang[1*], Fan Zhaoyuan[1], Sui Xiufeng[2]

(1. School of Sociology and Population Studies, Nanjing University of Posts and Telecommunications, Nanjing 210023, China; 2. Institute of National Security and Development Studies, Beijing Institute of Technology, Beijing 100081, China)

Abstract: The technological revolution under geopolitics has intensified the risks of China's scientific and technological security. Building a risk monitoring and early warning system in the field of scientific and technological security is of great significance for maintaining scientific and technological security and even national security. In the face of intensified game risks, autonomous loss of control risks, technology mismatch risks, and stable development risks in the field of science and technology in China, decoding the internal logic of the operation of the risk monitoring and early warning system in the field of science and technology security, empowering the construction of the risk monitoring and early warning system through technological means, and proposing guarantee strategies. Research suggests that the monitoring and early warning of technological security risks should be based on six logical prerequisites: institutional support, cross domain cooperation, information sharing, intellectual participation, industrial governance, and technological empowerment; From the perspective of systems theory, a risk monitoring and early warning system in the field of science and technology security is constructed by establishing an indicator system, clarifying the monitoring and early warning process, and building a modular model; To ensure

收稿日期：2023-12-10；**修回日期：**2024-05-20

通讯作者：*胡高强，南京邮电大学社会与人口学院讲师，主要研究方向为社会治理与产业发展；E-mail: 1053959729@qq.com

资助项目：中国工程院咨询项目“科技创新支撑国家安全体系和能力现代化战略研究”(2022-XBZD-28)；国家社会科学基金项目(20BZZ058)

本刊网址：www.engineering.org.cn/ch/journal/sscae

the effective implementation of the monitoring and early warning system, the country needs to improve relevant regulations and implement industry standards, expand the integration of new technologies, improve emergency response mechanisms and collaborative mechanisms, establish monitoring and early warning guidance institutions, strengthen talent cultivation and team building, and promote the integrated development of scientific and technological innovation and technological security to ensure the high-quality operation of the monitoring and early warning system.

Keywords: technology security; risks of technological security; risk monitoring and early warning; technological innovation

一、前言

2023 年 5 月 30 日，习近平总书记在主持召开二十届中央国家安全委员会第一次会议时强调，深刻认识国家安全面临的复杂严峻形势，正确把握重大国家安全问题[1]。科技安全是国家安全的重要组成部分，当前国际环境风高浪急，科技领域面临外部风险与内部风险、传统风险与新兴风险叠加的严峻态势。面对此情形，快速高效推进我国科技安全领域的风险监测预警建设势在必行。加快构建科技安全领域风险监测预警的框架体系，既有助于积极推进国家治理与社会治理、推进国家安全体系和能力现代化，也成为开创国家安全工作新局面的有机环节。

当前，科技安全领域风险监测预警研究侧重于指标或流程建构：构建科技安全领域风险的评估性指标体系，包括明确安全风险评估的指标设计原则[2]和核心维度[3]；探索具体领域的科技安全预警体系，包括海洋领域[4]和国防领域[5,6]等；科技安全领域风险治理的要素与流程，如“目标 – 需求 – 系统”的科技安全治理体系[7]、基于系统思维提出的科技安全治理机制[8]、“结构 – 流程 – 输出”安全情报体系[9]以及通过嵌入建立专家库、吸收专家研判来构建我国科技安全领域风险评估体系，实现国家科技安全领域风险的监测[10]。现有研究对科技安全领域风险监测预警指标、流程方面的思考，具有重要现实价值。

在地缘政治与大国博弈日渐激烈的形势下，科技安全领域风险并不局限于科技领域，风险覆盖面进一步扩大，构建科技安全风险监测预警体系事关国家安全。本文总结了我国科技安全领域的重大风险，厘清科技安全领域风险监测预警的内在逻辑，构建我国科技安全领域风险监测预警的框架体系，提出保障监测预警框架良性运行的对策建议，以促进我国科技安全领域的长足发展。

二、当前我国科技安全领域面临的重大风险

科技安全风险在微观上影响我国现代科技发展，宏观上威胁我国国家安全和社会繁荣稳定。随着逆全球化与地缘政治加剧，科技安全风险溢出了科技领域，向经济社会等领域蔓延渗透。因而科技安全领域的重大风险在形式上，既包含了直接的国家科技竞争，如科技封锁，也包含了颠覆性科技制造的内生性技术自主可控风险，而科技人才发展风险则是内外环境交互的结果。

（一）科技博弈加剧风险

随着21世纪经济全球化的加速，地缘经济博弈特别是大国在科技领域的博弈越来越表面化，形成科技发展的霸凌主义[11]，由此带来技术的外部遏制、封锁和极限施压愈加严峻。

1. 大国科技博弈持续升级

大国博弈引发的国际科技竞争持续升级，全球科技竞争格局正在发生深刻变化。各国越来越强调科技创新的重要性，并将其作为提升国家竞争力和实现经济增长的关键驱动力，纷纷加大对科技研发的投入，积极推动技术创新和突破。特别是由于规则制定权是关键生产力，因此各国不断强化规则制定权的竞争。作为规则制定权的集中体现，科技标准的竞争涉及产业链布局、市场份额争夺和创新方向决策等方面，对科技发展产生至关重要的影响。主要国家在科技标准制定中的竞争不断加剧，如果不能在技术标准制定中占据主导地位，将有可能使未来科技发展面临高风险和高成本。

2. 高科技产业链存在断链风险

一是全球高科技产业链呈现去国际分工和内向化趋势，将阻碍国际开放合作，致使产业链韧性降低。部分跨国公司正在将原有的跨境纵向分工体系调整为企业内部纵向一体化模式，且开始实施更为体系化的供应链战略，以保障供应链的自主可控。以往分布在全球不同国家的生产环节，正逐渐向一

国或相邻国家收缩以进行集中和集聚化生产，生产的碎片化趋势正在显现；二是科技竞合并存，国际关系更加复杂。国家间在共同应对网络安全威胁、推动技术标准的制定等方面存在合作共赢机会，但信息安全攻击、技术转让和知识产权纠纷等领域的技术竞争和安全争议也越来越紧张[12]。

（二）技术自主可控风险

传统国家安全观以防御性和对抗性为主要特征，而现代安全观体现的是动态性、开放性和可控性[13]。在当前大国激烈博弈中，实现技术自主安全可控的挑战日益加大。

1.“卡脖子”局面未根本改变

我国的技术突破面临先行者底层技术生态壁垒和供应链脱钩威胁。一是关键技术依赖度较高。我国在芯片制造、人工智能、半导体技术等关键领域，对西方发达国家的依赖程度较高，导致我国在关键科技上被“卡脖子”[14]。实际上，在技术全球化时期，国家间的技术依赖反而促进了技术在互通互动中共同进步、互惠共享[15]，但国家竞争展现了我国关键科技弱独立性的现状。二是供应链韧性较弱。从大国科技博弈的极限思维来看，科技领域及其供应链方面的竞争日趋激烈，而科技生产的全球化与我国前期形成的生产依赖，共同导致我国科技生产的供应链韧性较弱，且应对能力有待提升，特别是应急恢复计划、备份方案、危机管理和紧急响应能力等。

2. 技术“小院高墙”封锁围堵加剧

一方面，西方国家通过技术封锁和限制，打击我国产业发展的掌控能力。例如，通过限制关键技术出口，对我国科技企业施加制裁，以及设置技术壁垒和标准，阻碍我国获得先进技术和核心知识产权，使我国在关键领域无法取得竞争优势，导致长期依赖进口和付费许可，丧失自主创新和掌控产业发展能力。另一方面，西方国家的技术霸权将加剧市场垄断。西方国家在全球科技市场上垄断先进技术和关键产品，并通过垄断地位操纵市场规则，限制我国企业的发展空间和市场准入，使我国在科技产业链中处于被动地位。

（三）技术应用失当风险

当前科技发展迅速，其应用速度也日趋加快，这就造成了新科技未被完全理解，特别是其与应用对象的适配上，存在较大的越界性失配与分化风险。从理想角度看，科学技术的创新与应用初衷，是为了促进人类进步，改善不良处境，然而“好心办坏事”在科技应用领域时常出现，是风险社会中“飞去来器效应”的典型体现，特别是技术隔离了大量低技术工种工人，引发就业风险、拉大社会收入差距，威胁了民生与稳定。

1. 人工智能迭代加速技术失控风险

人工智能在提升效率的同时，也加剧了技术应用的失控风险。一是颠覆性技术随时可能出现。这对于实现国家科技创新跨越式发展具有重要战略意义，可能成为扭转大国博弈战略格局的关键因素，要对其战略价值和潜在风险作出充分预判[16]。二是人工智能很可能将超越人类控制。人工智能系统的自我迭代具有超出人类预期和控制的能力，并可能引发包括伦理和法律责任的界定、决策的透明度和问责性等一系列问题。三是新兴技术的边界越发模糊，潜在影响难以预测和防范。例如，基因编辑、人机融合等技术可能引发伦理、社会和法律问题，需要谨慎评估和管理。

2. 数据泄露与滥用风险增大

数字化技术是新兴科技的重要基础，但其快速流动性、易于抓取性等特征，形成了数据安全风险。一是数据泄露和滥用频发。随着大数据的广泛应用，个人和组织的数据收集和存储量不断增加。数据泄露可能导致个人隐私受到侵犯，造成个人信息被滥用、身份被盗窃以及金融欺诈等问题。二是虚假信息和网络谣言将更快、更易散播。通过网络和社交媒体平台，恶意用户可以故意传播虚假信息、虚构故事、炒作谣言等，导致公众被误导和混淆。三是数字盗窃和金融欺诈更难防范。例如，通过利用技术手段窃取个人和企业的财务信息、银行账户信息等，进行电子支付欺诈、身份盗窃等活动。

3. 科技发展可能加剧社会不平等

科技的快速市场化催生了“数字鸿沟”“数字人权”等问题，加剧了因劳动技能、文化水平等差异引起的社会不平等。一方面是ChatGTP等人工智能技术的出现与普及，特别是在实体产业中的大规模应用会加大劳动密集型行业的失业风险。传统的自动化和机器人技术的普及，已经带来了某些传统行业特别是劳动力密集型行业失业率上升，而不断

浮现的新技术可能再次冲击劳动力密集型行业。另一方面是“数字人权”问题[17]。科技发展要求人们具备一定的数字技能和知识，弱势群体可能无法获得适当的教育和培训，导致数字技能差距的加剧，特别是部分群体可能无法享受到便捷的电子支付和金融服务，以及电子商务带来的便利和商业机会。

（四）科技人才发展风险

科技人才发展风险是指科技人才在不同领域的分布结构、不同的地区分布结构以及流动性方面存在发展性风险。从我国当前情况来看，科技人才在行业、年龄和技能水平等方面存在结构性短板[18]，特别是在地域分布上严重不均衡；在科技人才流失方面也面临较大风险，一方面因我国自身科研环境局限导致的人才流失，另一方面是国外通过跨国公司、高等院校的高薪工作吸引我国科技人才。科技人才特别是关键科技领域人才的流失与失衡，是未来一段时期内催生我国科技安全领域风险的重要原因。科技人才是科技进步的推动者和创新的主要源泉，通过研究和开发，推动科技领域创新发展，一旦人才流失、分布失衡，将会导致我国科技发展陷于被动地位。同时，科技安全领域也需要科技人才的大力支持，因为科技安全需要科技尤其是创新科技的赋能，如利用全新的信息技术收集科技安全领域的全息数据，以监测、预警科技安全领域的风险。

三、科技安全风险监测预警的内在逻辑

当前科技安全呈现整体性、层次性、联动性，其风险则具有复杂动态性强、影响面大、容错率低的特点。在坚持普遍联系、开放发展、全面辩证的认识论指导下，基于实证调研，本文凝练了科技安全领域风险监测预警的多维运作机理，为构建整体性监测预警的框架体系进行机制铺垫。

（一）制度支持：科技安全的前提

政府关于科技领域的监管和政策支持对科技安全风险防控具有重要作用。① 科技安全的政策法规。政府通过制定和修订相关的法律法规，在明确科技安全重要性的基础上，出台相关政策与法律，这既能鼓励企业的技术研发与技术创新，也能保障信息安全。② 科技安全的管理制度。建立健全科技安全管理制度，既要强化科技活动的系统监管，也要对企业等组织定期实施制度性评估和检查，确保科技安全工作的有效落实。③ 科技安全的文化建设。政府积极推动科技安全文化建设，通过宣传教育、培训指导等方式，增强公众对科技安全的意识和认识，促进科技安全工作的有效开展。

（二）跨域合作：科技安全的导向

科技安全风险往往具有跨国和跨领域的特点，通过跨域合作能够加强防范和应对，特别是探讨技术合作模式的差异性及其对科技安全领域风险的影响。① 科技合作对象的差异与科技安全领域风险的关系。不同类型的技术合作对象在合作目标、技术实力等方面存在差异，因而对科技安全领域风险的影响不尽相同。例如，我国科技企业在与国外企业进行技术合作的过程中，很可能涉及国家安全审查等复杂因素，安全风险较大。② 合作领域差异与科技安全领域风险的关系。科技合作的差异所造成的安全风险也各不相同。例如，与卫星通信等先进领域的深度合作，会涉及国家战略机密，安全风险可能更大。③ 科技合作形式差异与科技安全领域风险的关系。差异的技术合作导致的科技安全领域风险也存在差异。例如，与高校或科研机构的技术合作，更多聚焦于基础研究和前沿技术，需要注意科技知识的产权保护，但与其他机构的技术合作，特别是与企业的合作，在技术推广与应用方面面临的风险更大。

（三）信息共享：科技安全的载体

科技安全的信息共享涵盖了科技信息的共享机制、平台建设、防护建设等方面。通过信息共享，能够加强科技领域不同部门和行业间的合作，协调应对信息安全风险。① 科技信息的共享机制。不同地区间科技信息共享机制的搭建和形式，均存在显著差异。这主要由其背后的驱动力量决定，无论是政府引导还是市场运作，直接决定了地区性不同部门之间信息共享机制的形成过程、中间流程、最终成效，进而导致科技安全领域风险的暴露程度也不一样。一般情况下，政府主导的信息共享风险要小于市场化运作。② 科技信息的平台建设主要涉及信息收集、信息整合、漏洞管理等方面。平台建设首先需要收集信息，可通过互联网协议地址、域名、

端口和组件信息等形式多方汇集；其次再对信息进行有效系统整合，以实现分析和挖掘，而如何整合信息就需要打造成熟的科技信息运转平台；再次，进行信息安全培训，其现实意义是增强人的信息安全意识，减少由于人为原因造成的信息安全风险。最后，将漏洞修补纳入平台建设，通过及时发现、处理信息安全漏洞，减少风险威胁，提高平台信息处理的安全阈值。③ 信息成效的系统监测。通过分析技术合作与信息共享，评估科技安全领域风险监测预警的系统成效，包括科技安全领域风险现实水平的监测（如避免技术漏洞、加快技术研发、提高产品可靠性）、预警（通过共享风险信息预防风险发生）。

（四）智力参与：科技安全的基础

专业知识和创新能力的关键人才，特别是制度化教育与专门培养的人才，能够解决科技安全领域风险治理中风险识别、技术支持等痛点难点问题。① 风险识别。专门人才是科技安全领域风险识别的主体，通过观察、分析、判断等主观过程对风险进行有效评估与识别。这就要求相关人员在经验、技能、知识水平上接受过专门的训练，形成成熟的智力资源。② 技术支持。科技安全离不开新技术的掌握与使用，它是维护安全的重要手段与基础。相关专业技术人员通过开发科技安全技术，如云安全技术、入侵检测系统、人工智能等，保护科技信息传输、保存方面的安全。③ 治理创新。科技赋能科技安全的治理路径，需要相应人才制定创新性治理的战略战术，既要研究不同技术领域技术创新与科技安全领域风险发生的关联性和内在逻辑，也要强化跨学科合作在科技安全领域风险管理中的创新意义。

（五）产业治理：科技安全的重心

科技安全的监测预警，离不开科技相关产业的系统治理，科技安全领域风险对产业的影响具有全局性、传导性，一旦关键产业链受损，将直接限制与该产业相关的一系列配套产业，在经济和社会层面将制造巨大隐患。那么，利用科技能够实现强化产业链的安全管理和监控、建立安全合作机制的目标，包括用新科技识别产业链中可能存在的、由旧科技引发的风险点，以及预测这些风险点对关键产业链的整体影响。同时，通过不同监控技术和系统，如供应链追溯系统、数据监测系统、漏洞扫描工具等，能够追踪、定位、分析产业链安全管理中的风险。

（六）技术赋能：科技安全的核心

通过合理的整合和应用创新技术，能够提升风险监测的精确性、实时性和全面性，更好地应对科技安全挑战。

1. 风险识别：人工智能与机器学习

从大规模的数据中自动识别模式、发现异常，从而提供更精准的风险监测和预警。使用监督学习算法来建立模型，通过训练数据让系统学会识别不同类型的风险事件。监督学习算法可以帮助探索未知的风险模式，此外，深度学习技术如卷积神经网络（CNN）和循环神经网络（RNN）也可以用于分析复杂的多模态数据，如图像、文本和声音，以提供更全面的风险评估。

2. 风险追踪：自然语言处理（NLP）

利用NLP技术，可以分析和理解与科技安全相关的大量文本数据，如新闻、社交媒体短文、政府文件等。通过情感分析、实体识别、关系抽取等技术，可以追踪并识别潜在的风险事件，如恶意信息传播、网络攻击等。此外，NLP还可以帮助挖掘专业文献和研究，了解最新的科技安全趋势和威胁。

3. 发现关联：大数据分析

利用大数据分析技术整合和分析多源异构的数据，包括结构化数据（如统计数据、日志）和非结构化数据（如图像、视频）。通过数据挖掘和数据分析，发现隐藏在数据中的关联和模式，从而提前发现科技安全风险。此外，大数据技术还可以帮助构建实时的风险监测系统，及时响应风险事件。

4. 数据共享：区块链技术

区块链技术可以用于确保数据的透明性和不可篡改性。使用区块链建立一个安全的数据存储和共享平台，确保监测和预警数据的真实性与完整性。此外，还可以用于建立去中心化的身份验证系统，确保参与数据采集和共享的各方都是合法可信的。

5. 硬件探查：物联网和传感器技术

利用物联网和传感器技术收集和监测与科技安全相关的物理世界数据，如设备运行状态、网络流量等。这些数据可以用于实时监测设备和网络的健

康状态，及时发现异常和潜在的风险。可以将物联网数据与其他数据源结合起来，实现更全面的风险评估。

四、科技安全风险监测预警的框架体系

面对科技安全领域的重大风险，除了不断提升科技创新能力，以发展解决发展问题，也要重视并建立风险监测预警机制，抢占先机、防患未然[19]。通过采纳新兴科技，利用其先发优势赋能我国科技安全领域风险监测预警的指标系统、重大风险监测预警的模型系统，构建科技安全领域风险监测预警的框架体系，提升监测预警的科学性、精确性和全面性。

（一）科技安全风险监测预警指标体系

科技安全监测预警框架体系的构建与运行，建立在明确的指标系统之上，包括厘清指标覆盖的主体、对象及其特性（制度性、跨域性、共享性等），方能有的放矢。本文构建指标系统，一方面基于当前我国科技安全领域风险的客观事实；另一方面是基于系统论视角，从科技安全的要素维度，构建风险监测预警的多维指标。系统理论将科技安全视为一个整体，将其影响因素作为系统要素，以便考察其特征[20]，典型代表是“科技安全六要素”，包括科技的基础、体制、活动、环境、领域、智力资源[21]。应该说，系统要素分析是一种辩证的系统分析方法，科技安全作为一个系统，其运作和维持需要相应的要素。不过，科技安全领域的风险在当前时期存在侧重点，即一些风险更具优先级，特别是在还未建立风险监测预警体系的前提下，将各个要素纳入其中，会丧失重点，导致监测预警精度下降。那么基于当前我国科技安全领域风险的现实，结合系统理论视角，从政策制度、关键技术自主可控、技术应用失当、人才安全四个核心关键构建指标体系。

政策法律风险指标：包括重点行业或组织在科技安全相关法律法规和政策上的合规性；相关指标可以包括安全合规评估结果、安全政策和规定的制定和执行情况、对安全事件的报告和响应机制等。关键技术自主可控风险指标：包括关键技术的安全性、可靠性和保密性，以及技术基础设施的安全性；相关指标可以包括技术漏洞数量和严重程度、关键技术的自主掌握程度、技术基础设施的鲁棒性等，其中数据安全指标极为重要，如数据的保密性、完整性和可用性。技术应用失当风险指标：考查科技在适配与应用过程中，特别是在赋能科技安全过程中，是否产生了自反性，包括技术使用率与回报率、技术适配程度（生产提升率、维护成本）等。科技人才发展风险指标：包括科技人才行业领域的分布结构、地区分布结构、核心重点科技领域的科技人才数量与效能等，同时还应该囊括科技人才安全培训的效果、安全行为和报告安全事件率等。

（二）科技安全风险监测预警关键环节

科技安全领域风险监测预警的框架模型是一个综合的、系统性的方法结构，可以从整体上识别、监测和预警科技安全领域的潜在风险。模型中的各环节相互关联，形成一个循环迭代的过程，以不断改进和提升科技安全领域风险管理的能力。该模型包括以下关键环节。

1. 利用大数据整合数据源

收集与科技安全相关的数据，包括安全事件数据、漏洞数据、威胁情报、行业报告等。整合这些数据源，建立一个全面的数据集，以便进行分析和建模。

2. 信息技术赋能大数据处理与建模

信息技术是科技安全数据处理的重要手段，利用其高效性处理数据，包括数据清洗、数据归一化、特征提取等。同时，根据处理后的数据，建立相应的预警模型，包括统计模型（如时间序列分析、回归分析）、机器学习模型（如决策树、支持向量机、神经网络）、深度学习模型（如 CNN、RNN）等。根据数据的特点和目标需求，选择合适的模型进行建模和训练。

3. 验证与优化

对建立的预警模型进行验证和测试，评估其准确性和可靠性并进行优化。使用合适的评估指标（如准确率、召回率、F1 值等）对模型进行评估，判断模型的性能和有效性。根据评估结果，进行模型的优化和调整，包括特征选择、参数调整、模型结构调整等。

4. 预警发布

根据实际需求和风险偏好，确定科技安全领域风险的预警阈值。通过设置适当的阈值，当监测指

标超过或接近阈值时，触发预警机制，及时通知相关人员并采取相应的应对措施。根据预警模型的结果，发出相应的预警信号。

5. 动态更新

监测预警模型是一个动态的过程，需要不断地进行改进和更新。利用信息科技定期传回的最新数据，回顾模型的性能，识别模型的局限性和改进空间。跟踪科技安全的新动态和威胁，及时更新模型，确保模型的准确性和适应性。

（三）构建科技安全风险监测预警的分模块模型

本文重点关注了新形势下的四大风险，为有针对性地监测和预警不同类型风险，同时还需要构建基于不同风险类型的分模块模型。每个模块能够独立进行监测和预警，并通过整合不同模块的结果来提供决策建议。这样的模块化模型有助于为决策者提供更准确、及时地预警和决策支持。① 博弈加剧风险预警模块。该模块能够帮助相关组织和人员及时发现和识别潜在的国际博弈风险，有利于及时应对和处置博弈风险，提高组织的风险防范能力。② 自主可控风险预警模块。此模块主要针对的是我国科技安全自主可控风险，涉及核心科技的依赖程度、创新能力等，模块在“极限思维”指导下，设定极限阈值，当低于阈值时，科技安全将出现较大风险。③ 技术应用失当风险预警模块。新科技可能会被应用到不合时宜的领域，存在不确定性和复杂性，潜藏着不可估量的风险因素，从而带来经济损失或者社会影响。此模块主要监测科技应用、适配过程中产生的“意外后果”的可接受程度，并通过设定等级来发布预警。④ 科技人才发展风险预警模块。科技人才是科技创新发展的关键要素。此模块监测我国科技人才地域分布结构、行业分布结构、年龄结构等方面的均衡程度和紧迫性，特别是关键技术领域的人才需求状况，设定阈值并发布预警信息。

根据技术采纳及其价值、指标系统、监测预警的整体模型与分模块，本文构建了我国科技安全领域风险监测预警的框架体系。它属于“中观层次”，既是指导、启发其他国家安全领域的整体思路，构成落实总体国家安全观的重要内容，也能够通过具体而微的实证研究真正实现对我国科技安全领域风险的监测和预警。

五、建立科技安全风险监测预警体系的策略

（一）推动科技安全法律法规和标准的制定与落地

加强科技安全法规和标准的研究与制定，明确科技安全领域的安全要求和责任，规范科技安全项目的审批和实施，提高科技安全风险的管控水平。一是完善科技安全相关的法律体系。二是完善科技安全相关的评估标准和技术规范，涵盖关键技术、数据安全、网络安全、系统安全等方面。标准应基于最新的科技发展和国际经验，提高科技安全风险管控的标准化和有效性。三是建立科技项目的审批和监管机制，确保项目在安全风险可控的前提下进行。审批过程应包括科技安全风险评估和审查，审批部门应具备科技安全专业背景和能力。四是推动法规的落地实施，加强对法规实施的宣传和培训，确保各相关部门、企事业单位能够理解和遵守科技安全法规。

（二）拓展新技术融入科技安全保障体系的方式

开辟新技术融入科技安全体系，形成多元国家安全保障机制的协同合作[21]，保障其落实与执行，能够提升科技安全保障体系的效果和影响力，推动科技创新与社会发展的良性互动。一是构建多方数据的可信共享机制。针对信息系统之间存在的“信息孤岛”问题，利用同态密码、区块链、差分隐私保护等技术，实现数据的多方安全共享。二是实现基于多模态的大模型数据融合分析。针对不同来源、不同类型、不同数量的信息，利用知识注入、场景对齐、领域微调等技术，实现科技安全生态数据中台。三是建立可解释人机协作机制。针对人工智能模型存在的“数据幻觉”“决策偏见”等问题，利用监督学习、强化学习、可视化、人机交互等技术进行人机协作，提升人类对人工智能的信任度和人机协作的效能。四是构建科技安全生态的数字孪生系统。针对科技安全数字孪生中的展现、分析、预演等实际需求，利用物联网、第五代移动通信和大数据智能模型，搭建科技安全生态，深度支撑科技安全保障。

（三）完善科技安全风险应急响应机制与协同机制

完善科技安全风险的响应机制与协同机制，对保障科技安全、促进经济发展、维护社会稳定、培

育人才队伍等方面都具有现实意义。一是制定科技安全风险应急响应的操作指南和流程，明确各级响应部门和责任，确保在发生安全事件或风险时能够迅速组织响应，并采取合适的措施进行处置。建立专门的应急响应团队，提前进行培训和演练，以提高应对突发事件的能力。二是建立科技安全风险监测预警的协同合作机制，促进相关部门和组织之间的信息共享和联动。建立跨部门的工作协调机制，定期召开联席会议，共同研判风险形势，制定协同行动方案，并加强合作的法律、政策和技术基础。三是建立科技安全风险事件的报告和通报机制，要求各相关部门、企事业单位及时向指定机构报告安全事件和风险情况。确保信息的透明度和及时性，及早发现、评估和回应风险，减少风险的扩散和影响。四是建立科技安全风险信息共享和联动平台，整合各部门、企事业单位的科技安全风险数据和信息资源，实现快速、准确的信息交换和共享。通过信息的汇聚和分析，提高科技安全风险监测预警的准确性和预测能力，打造“科技咨询–政府决策模式”，为决策提供科学依据[21]。

（四）建立科技安全风险监测预警指导机构

建立权威的科技安全风险监测预警指导机构，由国家相关部门、专家学者和行业代表组成。该机构应具备科技安全领域的专业知识和技术能力，负责制定科技安全风险监测预警的指导方针、政策和标准，指导和推动相关工作的开展。其主要职责包括：一是促进各相关部门、企事业单位之间的合作与协调。通过组织定期会议、研讨会和培训活动，促进信息共享、经验交流和合作项目的开展，以确保科技安全风险监测预警体系的全面落地和运行。二是提供技术支持和专业指导，包括为各部门、企事业单位提供科技安全风险监测预警的技术手段、方法和工具。同时，开展培训和知识普及活动，提高相关人员的科技安全风险监测预警能力。三是对科技安全风险监测预警体系进行监督和评估。定期开展科技安全风险的评估和预警能力的考核，及时调整和优化预警指标、方法和流程，提高预警体系的准确性和有效性。

（五）加强科技安全专业人才培养和队伍建设

科技人才是国家最宝贵、最重要的战略资源，科技竞争实际就是科技人才的竞争。加大对科技安全专业人才的培养和引进力度，建立完善的科技安全人才培养体系，培养具备科技安全监测与预警技能的专业人员，确保人才支持科技安全风险监测预警体系的运行。一是制定全面的科技安全专业人才培养计划，包括培训课程、实践项目和实习机会。该计划应涵盖科技安全监测、预警技术、风险评估、应急响应等方面的知识和技能培养，培养出具备综合能力的科技安全专业人才。为科技安全专业人才培养提供资金和资源支持，鼓励高校、科研机构和企事业单位开展科技安全实践项目与实习活动。与相关部门和行业组织合作，提供实践基地和案例资源。二是建立高水平科技安全教育机构。设立高等教育机构或科研机构，专门负责科技安全教育和研究。该机构应提供优质的科技安全专业教育，包括本科、硕士和博士的培养项目，建立科技安全领域的教学团队和实验室，培养一流的科技安全专业人才。三是加强科技安全专业人才引进和交流。通过引进国内外优秀的科技安全专业人才，提升国内科技安全人才队伍的水平。建立科技安全专家和学者的国际交流机制，组织学术研讨会和国际合作项目，促进科技安全领域的人才交流与合作。四是激励和保障科技安全专业人才的发展。建立激励机制，通过薪酬福利、晋升通道和荣誉表彰等方式，激发科技安全专业人才的积极性和创新能力。同时，加强对科技安全人才的培训和继续教育，确保其与快速发展的科技行业保持同步。

（六）促进科技创新与科技安全的融合发展

鼓励科技创新企业在研发过程中充分考虑科技安全风险，引导科技创新与科技安全的有机融合，促进科技安全保障能力提升。一是制定激励政策和支持措施，鼓励科技创新企业将科技安全纳入创新项目的设计和实施。例如，提供财政资金支持、税收优惠和知识产权保护等方面的政策支持，以促进科技创新与科技安全的有机融合。二是加强对科技创新企业的科技安全培训和宣传，提高从业人员对科技安全风险的认知和重视程度。组织针对科技创新企业的科技安全培训课程，引导企业加强科技安全管理，建立科技安全保障机制。三是建立科技创新与科技安全的合作机制，促进关键领域相关企业内部各部门之间的沟通与协作，实现科技创新与科

技安全的有机融合。同时，鼓励不同科技创新企业之间的合作与交流，分享科技安全经验和最佳实践，共同提高科技安全风险的识别和防范能力。四是建立科技创新成果的科技安全评估和审查机制，确保新技术、新产品在推广应用前经过科技安全的全面检验。相关部门可以组织专家对科技创新成果进行风险评估和安全审查，对具有较大安全风险的项目提出相应的改进措施和建议。五是鼓励科技创新企业建立科技安全管理体系，包括制定科技安全策略、规范安全管理流程和加强内部安全培训。这将有助于科技创新企业全面认识和管理科技安全风险，提升其科技安全保障能力。

利益冲突声明

本文作者在此声明彼此之间不存在任何利益冲突或财务冲突。

Received date: December 10, 2023; **Revised date:** May 20, 2024

Corresponding author: Hu Gaoqiang is a lecturer from School of Sociology and Population Studies, Nanjing University of Posts and Telecommunications. His major research fields include social governance and industrial development. E-mail: 1053959729@qq.com

Funding project: Chinese Academy of Engineering project “Research on the Mechanism and Improvement Path of the Execution Power of Grassroots Government Institutions” (2022-XBZD-28); National Social Science Fund Project (20BZZ058)

参考文献

[1] 中华人民共和国中央人民政府. 习近平主持召开二十届中央国家安全委员会第一次会议 [EB/OL]. (2023-05-30)[2024-04-05]. https://www.gov.cn/yaowen/liebiao/202305/content_6883803.htm.
Central People’s Government of the People’s Republic of China. Xi Jinping presided over the first meeting of the 20th Central National Security Committee [EB/OL]. (2023-05-30)[2024-04-05]. https://www.gov.cn/yaowen/liebiao/202305/content_6883803.htm.

[2] 蔡劲松, 谭爽, 武佳奇. 关键科技领域安全风险评估指标体系构建研究 [J]. 中国科技论坛, 2022 (3): 33–41.
Cai J S, Tan S, Wu J Q. Research on construction of security risk indicator system in key science and technology area [J]. Forum on Science and Technology in China, 2022 (3): 33–41.

[3] 郭秋怡, 张斌, 武宇. 面向科技安全的技术预见方法初探 [J]. 中国科技论坛, 2020 (11): 180–188.
Guo Q Y, Zhang B, Wu Y. A preliminary study on technology foresight method for science and technology security [J]. Forum on Science and Technology in China, 2020 (11): 180–188.

[4] 涂永强. 中国海洋经济安全的预警实证研究 [J]. 海洋经济, 2013, 3(1): 12–17.
Tu Y Q. An empirical study on the warning system of China’s marine economic security [J]. Marine Economy, 2013, 3(1): 12–17.

[5] 王刚, 陈伟, 曹秋红. 国防科技工业科技安全能力评价 [J]. 北京理工大学学报 (社会科学版), 2020, 22(5): 107–112.
Wang G, Chen W, Cao Q H. Evaluation of national defense industry’s science and technology security capability [J]. Journal of Beijing Institute of Technology (Social Sciences Edition), 2020, 22(5): 107–112.

[6] 李江磊. 国防安全风险评估模型构建 [J]. 国防科技, 2010, 31 (2): 41–46.
Li J L. The construction of the national deferse risk evaluation model [J]. National Defense Science & Technology, 2010, 31(2): 41–46.

[7] 陈劲, 朱子钦, 季与点, 等. 底线式科技安全治理体系构建研究 [J]. 科学学研究, 2020, 38(8): 1345–1357.
Chen J, Zhu Z Q, Ji Y D, et al. Research on the construction of science and technology security governance system based on bottom line thinking [J]. Studies in Science of Science, 2020, 38(8): 1345–1357.

[8] 赵世军, 董晓辉, 旷毓君. 系统论视域下我国科技安全治理的机理和路径研究 [J]. 系统科学学报, 2023, 31(4): 73–78.
Zhao S J, Dong X H, Kuang Y J. Research on the mechanism and path of science and technology security governance from the perspective of system theory [J]. Chinese Journal of Systems Science, 2023, 31(4): 73–78.

[9] 张家年, 赵妍. “结构 – 流程 – 输出” 视阈下科技安全情报体系研究 [J]. 情报理论与实践, 2022, 45(9): 6–14.
Zhang J N, Zhao Y. Research on security intelligence of science and technology from the perspective of “structure-process-output” framework [J]. Information Studies: Theory & Application, 2022, 45(9): 6–14.

[10] 李辉, 曾文, 刘彦君, 等. 面向科技安全的科技情报监测与分析系统构建研究 [J]. 情报理论与实践, 2021, 44(6): 98–104.
Li H, Zeng W, Liu Y J, et al. Research on the construction of intelligence monitoring and analysis system for science and technology security [J]. Information Studies: Theory & Application, 2021, 44(6): 98–104.

[11] 赵世军, 董晓辉. 新时代我国科技安全风险的成因分析及应对策略 [J]. 科学管理研究, 2021, 39(3): 27–32.
Zhao S J, Dong X H. Causes analysis and countermeasures of science and technology security risks in China in the new era [J]. Scientific Management Research, 2021, 39(3): 27–32.

[12] Lin Z L. Theoretical study of strategic management of science and technology security [J]. Science of Science and Management of S & T, 2007: 16789552.

[13] 孟东晖, 李显君, 梅亮, 等. 核心技术解构与突破: “清华 – 绿控” AMT 技术 2000—2016 年纵向案例研究 [J]. 科研管理, 2018, 39 (6): 75–84.
Meng D H, Li X J, Mei L, et al. Core technology deconstruction and breakthrough: A longitudinal case study on “Tsinghua-Lvkon” AMT technology from 2000 to 2016 [J]. Science Research Management, 2018, 39(6): 75–84.

[14] 曾德明, 张磊生, 禹献云, 等. 高新技术企业研发国际化进入模式选择研究 [J]. 软科学, 2013, 27(10): 25–28.
Zeng D M, Zhang L S, Yu X Y, et al. Research on the selection of entry mode for high-tech firms’ R & D internationalization [J]. Soft Science, 2013, 27(10): 25–28.

[15] 黄正元. 科技意识形态化及其风险——风险视域中的科技与意识形态 [J]. 武汉理工大学学报(社会科学版), 2009, 22(6):

12–15.
Huang Z Y. Science and technology ideologization and its risk—Science and technology and ideology in view of risk [J]. Journal of Wuhan University of Technology (Social Sciences Edition), 2009, 22(6): 12–15.

[16] 宋保振. “数字弱势群体” 权利及其法治化保障 [J]. 法律科学(西北政法大学学报), 2020, 38(6): 53–64.
Song B Z. The rights of “digital vulnerable groups” and their legal protection [J]. Science of Law (Journal of Northwest University of Political Science and Law), 2020, 38(6): 53–64.

[17] 孙德梅, 吴丰, 陈伟. 我国科技安全影响因素实证分析 [J]. 科技进步与对策, 2017, 34(22): 107–114.
Sun D M, Wu F, Chen W. Empirical analysis of influencing factors of Chinese science and technology security [J]. Science & Technology Progress and Policy, 2017, 34(22): 107–114.

[18] 梁梦凡. 科技领军人才健康状况及影响因素研究 [D]. 西安: 西安工程大学(硕士学位论文), 2016.
Liang M F. The research on science and technology leading talents health status and influencing factors [D]. Xi’an: Xi’an Polytechnic University (Master’s thesis), 2016.

[19] 李林, 廖晋平, 张烜工. 科技安全预警机制的建立及完善 [J]. 科技导报, 2019, 37(19): 26–32.
Li L, Liao J P, Zhang X G. Establishment and improvement of early warning mechanism of science and technology security [J]. Science & Technology Review, 2019, 37(19): 26–32.

[20] 王路, 张守明, 张笔峰, 等. 系统理论视角下的科技安全研究进展 [J]. 科技导报, 2023, 41(6): 68–73.
Wang L, Zhang S M, Zhang B F, et al. Research progress of science and technology security from the perspective of system theory [J]. Science & Technology Review, 2023, 41(6): 68–73.

[21] 王少. 重大突发事件中的科技咨询与政府决策: 问题、利益博弈和优化路径 [J]. 东北大学学报 (社会科学版), 2021, 23(4): 51–58.
Wang S. Scientific and technological consultation and government decision-making in serious emergencies: Based on problems, interest game and optimization path [J]. Journal of Northeastern University (Social Science), 2021, 23(4): 51–58.