

美国人工智能政策文本分析及启示*

明均仁 马玉婕 张曦 陈林 王莹
(武汉工程大学管理学院, 武汉 430205)

摘要: 人工智能正不断渗透到社会、生产、生活的各个方面, 已引发全球各国的高度重视。当前环境下, 在保护国家安全的同时, 推动我国人工智能高质量发展, 促进我国科技进步, 显得尤为重要。以美国自2016年起发布的人工智能政策文本为分析对象, 针对其发布主体、发布阶段、核心要点进行分析, 探寻人工智能发展给我国国家安全带来的风险挑战及对策。在思想层面, 要坚持总体国家安全观, 防范风险挑战, 筑牢安全屏障; 在政府层面, 要加强风险管控, 健全和完善人工智能相关法律法规和制度建设; 在技术层面, 要加快核心关键技术突破, 重视科技自主可控创新能力体系建设; 在行业层面, 构建由我国参与领导的全球人工智能合作网络, 完善人工智能人才培养体系。

关键词: 人工智能; 国家安全; 技术竞争; 风险管控; 战略规划

中图分类号: TP18; G359.7 **DOI:** 10.3772/j.issn.1673-2286.2022.03.008

引文格式: 明均仁, 马玉婕, 张曦, 等. 美国人工智能政策文本分析及启示[J]. 数字图书馆论坛, 2022 (3): 59-65.

1997年, IBM公司研制的“深蓝”机器人战胜国际象棋冠军加里·卡斯帕罗夫, 开启了人工智能的第三次发展浪潮。人工智能作为新一代“通用目的技术”, 创造了众多新兴业态, 并呈现多元化的发展态势^[1]。人工智能正不断渗透并改变着当前社会生产方式、思维方式以及生活习惯, 同时也给国家政治、经济等各方面带来了深远影响, 为社会的发展和进步带来颠覆性的变革, 由此引发了世界各国对人工智能的高度重视。

针对人工智能发展, 世界各国制定相关发展规划及政策文本, 开展全球人工智能竞争。新时代, 我国人工智能及其相关技术也在快速发展, 如何在保护国家安全的同时, 参考并借鉴相关政策与战略规划, 制定国家战略及执行方案, 促进科技发展尤为重要。

1 美国人工智能相关文件概述

1.1 发布主体

美国将人工智能视为维护国家安全、推动社会进步

的重要发展动力^[2]。自2016年起, 美国各部门陆续发布有关人工智能政策文件, 发布主体主要来自3个领域: ①美国政府及其及其相关部门, 如美国国会 (Congress of the United States)、美国国家标准与技术研究院 (National Institute of Standards and Technology)、美国白宫科技政策办公室 (Office of Science and Technology Policy) 等; ②非政府组织, 如美国国际战略研究中心 (Center for Strategic and International Studies)、美国国防创新委员会 (the Defense Innovation Board) 等; ③权威智库, 如新美国安全中心 (Center for a New American Security)、美国人工智能安全委员会 (National Security Commission on Artificial Intelligence)、兰德公司 (RAND Corporation) 等。不同主体在发布政策文件时, 其侧重点不同, 具体如下。

(1) 美国政府及其相关部门, 主要从国家层面对人工智能发展以及人工智能对经济、市场、安全等方面的影响进行分析, 掌控并调整人工智能发展路径。2016年, 美国总统执行办公室 (US Executive Office of the President) 发布《人工智能、自动化和经济》(Artificial

* 本研究得到湖北省高等学校哲学社会科学研究项目“突发公共事件下公众风险感知、信息搜寻行为与引导策略研究”(编号: 21D039) 资助。

Intelligence, Automation, and the Economy)^[3]报告, 调查指出人工智能的发展给美国市场和经济带来一定影响。2019年, 美国国防部(U.S. Department of Defense)发布《2018年国防部人工智能战略摘要——利用人工智能促进安全与繁荣》(*Summary of the 2018 Department of Defense Artificial Intelligence Strategy Harnessing AI to Advance Our Security and Prosperity*)^[4]报告, 明确指出为充分发挥人工智能优势, 要加强战略重点领域建设。2020年, 美国国会发布《无尽前沿法案》(*Endless Frontier Act*)^[5], 强调技术创新的重要性, 并提出要促进关键技术重点领域建设以发展人工智能。可见, 美国政府及其相关部门高度重视人工智能对国家各方面的影响, 并从战略层面指明方向, 给出建议及对策。

(2) 非政府组织, 其发布的人工智能相关文件是对政府发布政策文本的补充。2018年, 美国国际战略研究中心发布《人工智能与国家安全, 人工智能生态系统的重要性》(*Artificial Intelligence and National Security, the Importance of the AI Ecosystem*)^[6]报告, 通过分析其他国家人工智能现状, 指出人工智能在信任、安全、人员、数字能力、政策等5个层面存在的问题, 并提出相关建议。2019年, 美国国防创新委员会发布《人工智能原则: 国防部人工智能应用伦理的若干意见》(*AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense*)^[7], 指出人工智能技术的发展伴随着伦理、法律等问题的迭代与综合, 并提出人工智能道德规范使人工智能更好地服务于美国。针对人工智能发展过程中存在的问题, 结合政府发布的政策文本, 非政府组织通过系列报告向有关部门提出针对性建议。

(3) 权威智库, 其发布的人工智能相关文件与政府发布的行动建议及实施计划相呼应。2018年, 新美国安全中心发布《人工智能: 决策者需要了解什么》(*Artificial Intelligence: What Every Policymaker Needs to Know*)^[8], 认为发展人工智能技术是保卫国家安全的重要基础。2020年, 兰德公司发布《保持人工智能和机器学习的竞争优势》(*Maintaining the Competitive Advantage in Artificial Intelligence and Machine Learning*)^[9], 强调发挥人工智能竞争优势, 并提出一系列建议及对策。2021年, 美国人工智能安全委员会发布《最终报告》(*Final Report*)^[10], 全面系统地分析人工智能及其相关技术的发展对美国社会安全、国家安全

等方面的影响, 委员会从社会安全、国家安全、人民安全、基础设施及技术等5个层面, 提出相应的实施计划及建议。为完善人工智能发展, 权威智库主要针对人工智能发展过程中的不利因素、薄弱环节, 向美国政府及其相关部门提出发展建议。

1.2 发布阶段

伴随国际及社会环境变化, 美国发布的人工智能政策及文件, 其重点及作用导向具有差异, 大致分为发展起步阶段和快速发展阶段。

在发展起步阶段, 美国政府重视人工智能发展, 并将人工智能作为一项国家战略进行长期投资。2016年, 《为人工智能的未来做好准备》(*Preparing for the Future of Artificial Intelligence*)^[11]与《国家人工智能研发战略报告》(*The National Artificial Intelligence Research and Development Strategic Plan*)^[12]发布, 美国开始将人工智能作为一项国家战略进行实施, 并为美国人工智能发展指明了方向; 同年, 《人工智能、自动化和经济》报告跟进和指出, 要深入研究人工智能发展为市场和经济带来的机遇及挑战。2017年, 美国国会颁布《人工智能未来法案》(*Future of Artificial Intelligence Act of 2017*)^[13], 针对人工智能发展带来的机遇和挑战提出相应的建议, 该法案成为美国针对人工智能发展的第一个联邦法案。2018年美国连续发布了《机器崛起: 人工智能对美国政策不断增长的影响》、《人工智能与国家安全, 人工智能生态系统的重要性》、《维护美国人工智能领域领导力的行政命令》(*Executive Order on Maintaining American Leadership in Artificial Intelligence*)^[14]等系列政策文本, 进一步阐明需采取相应行动, 大力发展人工智能, 促进科技发展。可见, 在该阶段, 美国通过发布多个政策文件, 强调了人工智能发展的重要性, 并初步提出人工智能发展的主要方向。

在快速发展阶段, 美国延续发展起步阶段的主要思想, 针对人工智能发展过程中出现的问题及挑战, 制定详细的发展内容, 以保持人工智能技术优势。2019年美国发布的《2019年国家人工智能研发战略规划》(*The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update*)^[15]在保留2016年发布的战略规划的基础上, 增加公私合作战略, 加速人工智能发展; 同年发布的《2016—2019年人

工智能研发进展报告》(2016-2019 Progress Report: Advancing Artificial Intelligence R&D)^[16], 进一步总结2016—2019年人工智能发展状况及进展。2020年, 美国白宫科技政策办公室发布《美国人工智能行动: 第一年度报告》(American Artificial Intelligence Initiative: Year One Annual Report)^[17], 总结过去一年人工智能政策实施情况, 并为进一步推进人工智能发展以及促进创新突破提出相关建议; 美国国会研究服务中心(Congressional Research Service)发布《美国2020年人工智能与国家安全报告》(Artificial Intelligence and National Security Updated November 10, 2020)^[18], 指出发展军事人工智能存在的潜在问题, 阐述人工智能在国防领域应用的机遇和挑战。2021年, 美国人工智能安全委员会发布《最终报告》, 该报告结合人工智能发展现状, 指出需调整人工智能发展方向, 以抵御人工智能带来的竞争和冲突。可见, 在本阶段, 美国进一步对已实施的人工智能政策进行总结, 重视人工智能发展带来的一系列问题, 强调在人工智能时代保卫国家安全的重要性, 在动态发展过程中制定与修改人工智能建设方向, 以保证人工智能可持续发展。

2 核心要点

在美国发布的人工智能政策文本中, 其内容侧重点有所不同。总体来看, 文件的核心要点主要由3个方面组成: ①人工智能发展在国家战略中占据重要地位; ②人工智能发展具有广阔前景; ③采取相应的措施以解决人工智能发展过程中出现的问题及挑战。

2.1 人工智能发展在国家战略中占据重要地位

人工智能水平与国家实力强弱的关联程度进一步加深, 技术的落后将会使得国家在国际战略博弈中处于不利地位^[19]。为赢得技术竞争、发挥人工智能优势、保障国家安全, 美国政府及其相关部门、非政府组织和权威智库等先后发布人工智能相关政策及文件, 大力发展人工智能技术, 部署人工智能系统, 并及时调整国家发展战略。为支持和推进人工智能建设, 美国国会以及美国的总统办公室、国防部等核心政府部门相续参与其中, 并发布相关政策文本, 为人工智能的发展指明方向。

美国在多个人工智能政策文本中强调, 人工智能的

发展具有战略意义, 是保卫国家安全、促进经济繁荣发展、加快科技进步的重要手段。《人工智能未来法案》强调人工智能将在未来扮演重要角色, 因此为应对这种发展趋势, 该报告中制定了进一步的发展举措; 《维护国家人工智能领域领导力的行政命令》要求加大对人工智能相关研究的资金投入, 保证人工智能的优先发展地位; 《2020年人工智能倡议法案》(National Artificial Intelligence Initiative Act of 2020)^[20]中, 为确保美国人工智能快速、健康发展, 给政府部门提出相关建议。

2.2 人工智能发展具有广阔前景

人工智能为科技、军事、国防、国家情报等领域发展带来巨大的发展前景。美国国会研究服务中心发布的《美国2019年人工智能与国家安全报告》(Artificial Intelligence and National Security Updated November 21, 2019)^[21]中指出, 相关部门正在考虑将人工智能技术运用到多个军事场景当中, 如网络空间行动、指挥和控制、半自动和自动驾驶系统等; 美国也积极促进人工智能在国家情报领域的应用, 优化情报流程。

同时, 人工智能技术的进步, 促进了人工智能与其他领域的融合与交叉, 推动了各领域的变革性进步。

《无尽前沿法案》明确提出为促进人工智能发展, 政府需要增加研究投资, 促进美国技术创新, 因此要推动发展与人工智能相关的机器学习、高性能计算、通信技术、生物技术、网络数据安全等关键技术领域发展。

《最终报告》提出, 实施国家微电子技术战略, 增加政府对微电子技术研究的投资, 发展美国微电子制造; 重视新技术基础研究, 并加大相关投资, 促进科技进步与发展。

2.3 制定措施化解风险与应对挑战

多个人工智能政策文本指出, 伴随技术发展, 美国人工智能主要面临人才培养、伦理道德、技术安全等多方面的挑战。在人才培养问题上, 人工智能面临相关人才缺乏、人才流失等问题; 在伦理道德方面, 人工智能技术的发展增强了对人的取代能力, 对法律、道德等方面形成巨大的影响及冲击^[2]; 在技术安全方面, 人工智能技术的发展给国家安全带来巨大的影响, 如何减少技术发展过程中存在的安全隐患, 增强民众对于人工智能技术的信任, 成为相关部门亟需解决的问题。因

此,美国通过制定相关措施以化解风险与应对挑战。

(1) 人才培养方面。相关人才缺乏是美国在人工智能发展过程中面临的重要问题之一。美国自2016年起,在《维护美国人工智能领域领导力的行政命令》、《国家安全创新途径法案》(National Security Innovation Pathway Act)^[22]、《最终报告》等多个人工智能相关文件中,针对人才缺乏问题提出相关举措,主要分为两个方面。①政府部门针对市场与社会情况制定相关政策,发展人工智能相关研究,创造就业机会。②人工智能相关人才培养方面,强化人工智能在职人员培训,增强在职人员人机协调能力;加大人工智能教育投资,如大学级别的科学、技术、工程、数学(STEM)项目,并设立本科及研究生奖学金;扩大高技能人才获得签证和绿卡方式,推行全面移民战略,拓宽数字人才输送通道,以保留和招募更多人工智能技术人才。

(2) 伦理道德方面。科学技术的发展伴随伦理的发展,科学技术发挥作用越大,越需要伦理的支持或规制^[23]。人工智能技术的发展给社会生产和生活方式带来颠覆性影响,并引发社会众多领域深刻变革,同时,人工智能技术的复杂性和不确定性也逐步引发主体责任不清、算法歧视、隐私侵犯等伦理风险^[24],反而不利于人工智能技术的发展。因此,美国在《国家人工智能研发战略报告》、《2018年国防部人工智能战略摘要——利用人工智能促进安全与繁荣》、《初步报告》(Initial Report)^[25]、《人工智能原则:国防部人工智能应用伦理的若干意见》、《中期报告》(Interim Report)^[26]等多个政策文本中,重视人工智能伦理道德问题,并将其作为重要工作项目进行开展。美国国防部发布的《2018年国防部人工智能战略摘要——利用人工智能促进安全与繁荣》报告中强调,需要建立人工智能伦理原则;在人工智能技术使用过程中,要避免对人员造成伤害,并对人工智能系统进行测试和监管。总体来看,针对伦理道德问题,美国采取的主要举措包括:①重视并解决由人工智能引起的道德、法律等方面问题;②将人工智能伦理道德作为特别项目开展工作;③提出人工智能道德规范,帮助人工智能更好地服务美国。

(3) 技术安全方面。美国人工智能安全委员会在《最终报告》中指出,人工智能的应用使得美国社会存在巨大的安全隐患,人工智能竞争引发的科技威胁正在转变为国家安全的威胁。在技术层面,人工智能的技术滥用及技术安全问题影响了美国的国家安全^[19]。因此,如何安全地使用人工智能技术,增强美国民众对于

人工智能技术的信任,克服人工智能的负面影响,成为确保美国国家安全的关键问题。美国在《人工智能:决策者需要了解什么》、《美国如何领导人工智能:联邦参与制定技术标准及相关工具的计划》(U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools)^[27]、《美国2020年人工智能与国家安全报告》、《人工智能应用监管指南》(Guidance for Regulation of Artificial Intelligence Applications)^[28]等多个政策文本中指出,要加强建设人工智能监管,建立测试与监督机制,保障人工智能技术在应用过程中的安全。《美国如何领导人工智能:联邦参与制定技术标准及相关工具的计划》确定了数据和知识、性能测试与报告方法、安全、风险管理等9个人工智能标准重点领域,促进人工智能的有效可靠发展。针对技术安全问题,美国相关政策文本提出的主要举措包括:①推进人工智能相关技术性能测试与报告方法、风险管理等重点领域建设;②通过监管和非监管方法减少研发及应用人工智能技术的障碍;③建立针对人工智能开发的监督机制。

3 对我国国家安全的风险挑战及建议

3.1 我国人工智能发展概况

我国重视人工智能发展,制订并发布了多个战略规划纲要、指南等文件,在加快人工智能体系化发展的过程中起到了重要作用。2016年,国务院发布《“十三五”国家战略性新兴产业发展规划》^[29],提出促进人工智能发展,加快人工智能支撑体系建设,推动人工智能在各领域的应用。2017年,国务院发布《新一代人工智能发展规划》^[30],制定了“三步走”战略及战略目标,以促进我国人工智能快速发展^[31]。2018年,中国电子技术标准化研究院发布《人工智能标准化白皮书(2018版)》^[32],强调加强人工智能领域研究、投入及建设,进一步推动人工智能及其产业发展。2020年,国家标准化委员会、中央网信办等发布《国家新一代人工智能标准体系建设指南》^[33],为促进人工智能领域可持续发展进行标准体系建设。

3.2 对我国国家安全的风险挑战

在新的国际环境下,人工智能成为科技革命和产

业变革的核心动力,其发展是我国抓住新一轮科技革命机遇、促进科技快速发展、提升社会生产力的重要资源和动力。我国国家安全领域的政治安全、经济安全、数据信息安全、社会安全等可能会受到多方位、多维度的风险挑战,如在数据信息安全领域,当前世界各国对数据的依赖性增强,人工智能等技术的发展衍生出具有持续性和隐蔽性的数据安全风险^[34],必须防范人工智能技术对我国信息安全防御系统进行攻击破坏、对我国网络信息基础设施进行渗透、非法搜集用户群体数据信息等行为操作,应对“算法战”“意识战”等新型数字化战略博弈^[35],巩固我国网络和数据信息安全体系,以保护我国数据信息安全^[36]。因此,需重视人工智能技术应用所带来的安全隐患及风险,促进人工智能高质量发展,筑牢安全屏障,确保我国国家安全。

3.3 应对美国人工智能战略的思考和举措

(1) 思想层面:2014年,中央国家安全委员会第一次会议首次全面论述了“总体国家安全观”^[37];2015年,第十二届全国人大常委会第十四次会议明确了总体国家安全观的内涵;2017年,中国共产党第十九次全国代表大会将坚持总体国家安全观作为新时代中国特色社会主义基本方略之一;2018年,习近平总书记在十九届中央国家安全委员会第一次会议中强调全面贯彻落实总体国家安全观,开创新时代国家安全工作新局面^[38]。总体国家安全观在随着时代发展的过程中进一步完善,并将海外利益安全、太空安全、极地安全、深海安全及生物安全纳入总体国家安全体系。总体国家安全观阐述了在新时代,我国为什么要坚持和发展国家安全事业,坚持和发展什么样的国家安全事业,以及如何坚持和发展国家安全事业。伴随各国人工智能发展的相关文件出台,我国人工智能发展环境将面临新形势与新挑战,这要求我们要坚持总体国家安全观,把握新一轮科技革命的主动权,牢固树立系统思维和底线思维,防范风险挑战。

(2) 政府层面:在总体国家安全观的指导下,加强风险管控,加快推动我国人工智能安全监管及立法过程,健全多元、立体、全方位的应对机制。一是密切跟踪、了解其他国家利用人工智能促进国家安全的技术发展水平和相关举措,掌握其在人工智能技术路线、支持举措、监管规则等方面的新动态,加强评估和预判,并出台应对举措;二是构建体系化的人工智能法律

监管框架,完善人工智能相关法律法规和制度建设^[39],健全数据治理体系;三是积极探索新途径、新方式,采用“监管沙箱”等方式^[40],不断提高监管的效率和灵活性,构建由政府主导,企业、研究机构、公众等多方参与的人工智能安全监管体系。

(3) 技术层面:当前,我国在人工智能相关领域研究数量激增,相关专利申请数量位居世界第一^[41],但在世界人工智能快速发展环境下,我国仍要做好前瞻布局,强化自主可控的人工智能硬软件关键核心技术研发。一是加快新一代人工智能技术研发,详细梳理“卡脖子”问题,加大支持力度,以数据、算法、模型和应用为重点,从智能芯片、基础算法等方面着手,加快核心技术突破;二是重视国家安全领域的科技自主可控创新能力体系建设^[42],实现部分关键技术的国产替代,减少技术依赖并确保技术优势,避免人工智能发展受制于人。

(4) 行业层面:落实“总体国家安全观”,构建由我国参与领导的全球人工智能合作网络,完善相关科技人才培养体系^[43]。一是加强国际合作与交流,鼓励和支持有条件、有实力的企业与高校积极参与人工智能国际标准的制定,共同搭建人工智能合作平台;二是加强相关科技人才招聘,增加人才储备,构建人工智能高水平人才库,培养技术、工程与管理的复合型人才;三是充分发挥行业组织优势,围绕人工智能研发管理、技术保障、产品应用等方面,建立完善人工智能安全标准体系,加快形成人工智能测评和监测能力,运用评估测试、跟踪监测等多种手段,持续推动人工智能安全可控策略在产业界落地。

参考文献

- [1] 李晓理,张博,王康,等.人工智能的发展及应用[J].北京工业大学学报,2020,46(6):583-590.
- [2] 李恒阳.美国人工智能战略探析[J].美国研究,2020,34(4):7,94-114.
- [3] Executive Office of the President. Artificial Intelligence, Automation, and the Economy [EB/OL]. [2021-10-20]. <https://obamawhitehouse.archives.gov/blog/2016/12/20/artificial-intelligence-automation-and-economy>.
- [4] Department of Defense. Summary of The 2018 Department of Defense Artificial Intelligence Strategy Harnessing AI to Advance Our Security and Prosperity [EB/OL]. [2021-11-12].

- <https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF>.
- [5] Congress.gov.S.3832-Endless Frontier Act [EB/OL]. [2021-11-21]. <https://www.congress.gov/bill/116th-congress/senate-bill/3832/text>.
- [6] 人工智能与国家安全: AI生态系统的重要性 [EB/OL]. [2022-01-01]. <http://mkc.ckcest.cn/article-detail.html?channelId=120231&pkId=135743>.
- [7] Defense Innovation Board. AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense [EB/OL]. [2021-11-30]. https://media.defense.gov/2019/Oct/31/2002204459/-1/-1/0/DIB_AI_PRINCIPLES_SUPPORTING_DOCUMENT.PDF.
- [8] SCHARRE P, HOROEITZ M. Artificial Intelligence: What Every Policymaker Needs to Know [EB/OL]. [2021-11-19]. <https://www.cnas.org/publications/reports/artificial-intelligence-what-every-policymaker-needs-to-know>.
- [9] RAND Corporation. Maintaining the Competitive Advantage in Artificial Intelligence and Machine Learning [EB/OL]. [2021-11-18]. https://www.rand.org/pubs/research_reports/RRA200-1.html.
- [10] National Security Commission on Artificial Intelligence. Final Report [EB/OL]. [2021-11-4]. <https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf>.
- [11] Executive Office of the President. Preparing for the Future of Artificial Intelligence [EB/OL]. [2021-06-27]. <https://files.eric.ed.gov/fulltext/ED587229.pdf>.
- [12] The National Artificial Intelligence Research and Development Strategic Plan [EB/OL]. [2022-01-01]. <https://www.docin.com/p-1756549282.html>.
- [13] Congress.gov.H.R.4625-Future of Artificial Intelligence Act of 2017 [EB/OL]. [2021-11-18]. <https://www.congress.gov/bill/115th-congress/house-bill/4625/text>.
- [14] The White House. Executive Order on Maintaining American Leadership in Artificial Intelligence [EB/OL]. [2021-12-11]. <https://trumpwhitehouse.archives.gov/presidential>.
- [15] 2019年美国国家人工智能战略报告 [EB/OL]. [2022-01-01]. <https://blog.csdn.net/cf2SudS8x8F0v/article/details/100024564>.
- [16] National Science & Technology Council. 2016-2019 Progress Report: Advancing Artificial Intelligence R&D [EB/OL]. [2021-11-21]. <https://www.nitrd.gov/pubs/AI-Research-and-Development-Progress-Report-2016-2019.pdf>.
- [17] The White House. American Artificial Intelligence Initiative: Year One Annual Report [EB/OL]. [2021-11-16]. <https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/02/American-AI-Initiative-One-Year-Annual-Report.pdf>.
- [18] Congressional Research Service. Artificial Intelligence and National Security Updated November 10, 2020 [EB/OL]. [2021-11-10]. <https://crsreports.congress.gov/product/pdf/R/R45178>.
- [19] 秦浩. 美国政府人工智能战略目标、举措及经验分析 [J]. 中国电子科学研究院学报, 2021, 16 (12): 1243-1250.
- [20] Congress.gov.H.R.6216-National Artificial Intelligence Initiative Act of 2020 [EB/OL]. [2021-11-12]. <https://www.congress.gov/116/bills/hr6216/BILLS-116hr6216ih.pdf>.
- [21] Congressional Research Service. Artificial Intelligence and National Security Updated November 21, 2019 [EB/OL]. [2021-11-20]. <https://crsreports.congress.gov/product/pdf/R/R45178/7>.
- [22] Congress.gov.H.R.7256-National Security Innovation Pathway Act [EB/OL]. [2021-11-18]. <https://www.congress.gov/bill/116th-congress/house-bill/7256/text>.
- [23] 方滨兴, 时金桥, 王忠儒, 等. 人工智能赋能网络攻击的安全威胁及应对策略 [J]. 中国工程科学, 2021, 23 (3): 60-66.
- [24] 李梅敬. 理论层次视域下人工智能发展风险的伦理应对 [J]. 探索与争鸣, 2021 (8): 167-176, 180.
- [25] National Security Commission on Artificial Intelligence. Initial Report [EB/OL]. [2021-11-30]. https://www.nscai.gov/wp-content/uploads/2021/01/NSCAI_Initial-Report-to-Congress_July-2019.pdf.
- [26] National Security Commission on Artificial Intelligence. Interim Report [EB/OL]. [2021-11-30]. https://www.nscai.gov/wp-content/uploads/2021/01/NSCAI-Interim-Report-for-Congress_201911.pdf.
- [27] National Institute of Standards and Technology. U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools [EB/OL]. [2021-12-10]. https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.
- [28] The White House. Guidance for Regulation of Artificial Intelligence Applications [EB/OL]. [2021-12-07]. <https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf>.
- [29] 国务院关于印发“十三五”国家战略性新兴产业发展规划的通知 [EB/OL]. [2021-12-08]. <http://www.gov.cn/zhengce/>

- content/2016-12/19/content_5150090.htm.
- [30] 国务院关于印发新一代人工智能发展规划的通知 [EB/OL]. [2021-12-08]. http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.
- [31] 张涛, 马海群. 中国人工智能政策主题热点及演进分析 [J]. 现代情报, 2021, 41 (11): 150-160.
- [32] 中国电子技术标准化研究院. 人工智能标准化白皮书 (2018 版) [EB/OL]. [2022-01-24]. <http://www.cesi.cn/images/editor/20180124/20180124135528742.pdf>.
- [33] 国家新一代人工智能标准体系建设指南 [EB/OL]. [2022-01-07]. <http://www.gov.cn/zhengce/zhengceku/2020-08/09/5533454/files/bf4f158874434ad096636ba297e3fab3.pdf>.
- [34] 阙天舒, 王子玥. 数字经济时代的全球数据安全治理与中国策略 [J]. 国际安全研究, 2022, 40 (1): 130-154, 158.
- [35] 阙天舒, 张纪腾. 人工智能时代背景下的国家安全治理: 应用范式、风险识别与路径选择 [J]. 国际安全研究, 2020, 38 (1): 4-38, 157.
- [36] 相丽玲, 李彦如. “总体国家安全观”下的我国个人信息保护制度体系探析 [J]. 情报理论与实践, 2020, 43 (7): 18-23.
- [37] 李志斐. 总体国家安全观与全球安全治理的中国方向 [J]. 中共中央党校 (国家行政学院) 学报, 2022, 26 (01): 124-133.
- [38] 习近平: 全面贯彻落实总体国家安全观 开创新时代国家安全工作新局面 [N]. 人民日报, 2018-04-17 (1).
- [39] 杨启飞. 大数据时代国内信息安全研究: 现状、趋势与反思 [J]. 情报科学, 2021, 39 (2): 178-184.
- [40] 李真, 袁伟. 美国金融科技最新立法监管动态及对我国的启示 [J]. 金融理论与实践, 2020 (4): 69-76.
- [41] 曾闻, 王曰芬, 周琮宇. 产业领域专利申请状态分布与演化研究——以人工智能领域为例 [J]. 情报科学, 2020, 38 (12): 4-11.
- [42] 张家年, 马费成. 总体国家安全观视角下新时代国家安全及应对策略 [J]. 情报杂志, 2019, 38 (10): 12-20, 152.
- [43] 谭晓, 李辉, 胡锡晟. 总体国家安全观视阈下的情报学热点主题研究 [J]. 情报理论与实践, 2021, 44 (1): 49, 57-62.

作者简介

明均仁, 男, 1981年生, 博士, 教授, 研究方向: 数字信息服务和文本挖掘。

马玉婕, 女, 1998年生, 硕士研究生, 研究方向: 数字信息服务。

张曦, 女, 1980年生, 博士, 副教授, 研究方向: 信息管理。

陈林, 男, 1988年生, 博士, 讲师, 研究方向: 信息系统。

王莹, 女, 1971年生, 硕士, 副教授, 通信作者, 研究方向: 信息服务与战略管理, E-mail: 3650178@qq.com。

Analysis and Enlightenment of American Artificial Intelligence Policy Text

MING JunRen MA YuJie ZHANG Xi CHEN Lin WANG Kun
(School of Management, Wuhan Institute of Technology, Wuhan 430205, P. R. China)

Abstracts: Artificial intelligence is constantly penetrating into all aspects of society, production and life, and has attracted great attention all over the world. In the current environment, while protecting national security, it is particularly important to promote the high-quality development of artificial intelligence in China and promote China's scientific and technological progress. Taking the AI related documents issued by American since 2016 as the object, this paper analyzes its release subject, release stage, and core points, and explores the risks, challenges and countermeasures brought by the development of AI to China's national security. At the ideological level, we should adhere to a holistic view of national security, prevent risks and challenges, and build a strong security barrier. At the government level, it is essential to strengthen risk management and improve artificial intelligence-related laws, regulations and system construction. At the technical level, it is necessary to speed up breakthroughs in core and key technologies, and attach importance to the construction of scientific and technological independent and controllable innovation capability system. At the industry level, build a global artificial intelligence cooperation network led by China's participation and improve the artificial intelligence talent training system.

Keywords: Artificial Intelligence; National Security; Technological Competition; Risk Control; Strategic Planning

(收稿日期: 2022-02-24)