俄罗斯人工智能军事化的新进展、动因及安全影响*

武　琼

【内容提要】　俄罗斯人工智能军事化的新进展主要体现在以下五方面：第一，从国家层面构筑军用人工智能发展战略体系；第二，建立和完善军用人工智能管理机构；第三，研发人工智能军事化项目；第四，推动人工智能军事化项目的实战化运用；第五，加强与长期盟友和合作伙伴的人工智能军事化合作。俄罗斯之所以高度重视人工智能军事化的发展，主要是基于以下五方面原因：俄罗斯素有重视军事技术的历史传统、人工智能发展带动俄罗斯军事装备进步、应对周边威胁和安全挑战的现实需要、俄乌冲突的外溢效应、世界主要军事强国着力发展以人工智能为代表的颠覆性技术。俄罗斯推动人工智能军事化造成以下三方面安全影响：第一，加深俄罗斯与美国及北约间的军备竞赛；第二，增加俄罗斯与美国及北约间意外战争的爆发风险；第三，从内外两方面冲击战争伦理，包括推动战争从迫不得已的手段逐步转变为优先尝试甚至是第一选择的手段，判断发动或参与战争的责任主体日趋模糊化，加深区域性人道主义灾难。未来，俄可能通过内外兼顾的方式推进人工智能军事化的发展与应用，但受到西方国家对俄技术封锁、芯片技术落后、人才流失等因素掣肘，俄罗斯人工智能军事化的发展仍面临严峻挑战。

【关 键 词】　人工智能军事化　军用机器人　俄乌冲突　战争伦理

【作者简介】　武琼，宁夏大学阿拉伯学院（中国阿拉伯国家研究院）讲师。

* 本文受国家社科基金重大项目（22&ZD51）的资助。

引 言

作为引领新一轮科技革命和产业变革的战略性技术，人工智能正在对生产生活方式、国家安全治理、国防和军队建设等领域产生重大而深远的影响。随着人工智能在军事领域的快速发展和广泛运用，战争形态正在加速向智能化方向演进。人工智能军事化是指人工智能技术在军事领域研发、部署和运用的过程，具体包括机器学习、深度学习、自然语言处理等人工智能技术在情报分析、指挥决策、武器平台、网络攻防等主要领域的发展和运用。人工智能军事化具有四个特点：一是智能化程度高。军用机器人能模拟人类的听觉、视觉及触觉等感知能力，自主追踪、探测并打击指挥部、弹药库及军营等重要军事目标。二是风险程度高。受到硬件故障和“算法黑箱”等因素影响，军用机器人在执行作战任务的过程中可能会偏离指挥员预先设定的作战目标，甚至不听指挥员的命令，在战场上胡乱展开行动。在这种情况下，军用机器人不会考虑攻击目标是敌人还是无辜平民，从而导致传统的伦理道德原则很难对其进行约束。三是保密性强。作为一项颠覆性技术，人工智能的算法设计、技术突破和产品研发在各国政府和大型科技企业中处于保密状态。其中，人工智能在军事领域的研发和测试保密程度较高，外界很难对其有全面且清晰的了解。四是持续发展性强。随着人工智能军事化的不断提速，主要军事强国仍将聚焦于数据分析、指挥决策、无人作战等领域，意图抢占未来战争的制高点。

人工智能以其高效的数据传输和处理能力、强大的计算能力和算法支持等优势而备受俄罗斯的青睐。随着人口数量的持续下降和老龄化进程的加快，俄罗斯兵源缺乏问题日益突出，人工智能军事化无疑能缓解这一问题。更重要的是，人工智能军事化可以极大增强俄军的战场态势感知、指挥决策、自主打击等能力，进而助力其夺取并保持战场主动权。普京强调，要更积极地使用和掌握具有人工智能元素的武器装备，包括机器人系统、自动化指挥控制系统等，这类武器不论是在今天还是在不久的将来都会极大地增强部队的潜力，并在很大程度上决定战斗结果①。

① Путин заявил о важности внедрения ИИ в российскую систему вооружений. https：//iz. ru/1102590/2020 – 12 – 21/putin – zaiavil – o – vazhnosti – vnedreniia – ii – v – rossiiskuiu – sistemu – vooruzhenii，访问时间：2023 年 6 月 10 日。

目前，国内外学界对俄罗斯人工智能军事化的研究正处于起步阶段，既有研究主要分为以下三类：一是动因类。华盾指出，俄罗斯在地缘政治和军备竞赛压力下大力推动以机器人技术为主要方向的人工智能军事化应用①。苏崇阳和王晓捷等人认为，俄军对人工智能的重视源于内部诉求和外部因素两方面②。二是具体研发和军事实践类。华盾和封帅认为，俄罗斯国防部对军用机器人系统的关注由来已久，并在军事应用方面积累了很多成功经验③。赵勋强调，俄罗斯的军用人工智能技术已在叙利亚危机中经过实战检验④。戢仕铭认为，俄罗斯十分看重人工智能在局部战争和地区冲突中发挥的作用，并通过测试应用将其优先纳入军事应用中⑤。安娜·纳迪拜泽认为，俄军方通过成立先期研究基金会（Фонд перспективных исследований）、机器人研究与测试中心（Главный научно－исследовательский испытательный центр робототехники）、军用机器人技术综合系统发展委员会（Комиссия Минобороны по развитию робототехнических комплексов военного назначения）来推动军用机器人技术的发展⑥。三是现实挑战类。绲珊珊认为，资金、资源、基础设施和人力资本是影响俄罗斯人工智能军事发展的关键因素⑦。既有研究成果具有较高的参考价值，但仍有进一步补充与完善的空间：一是时间上主要集中在俄乌冲突爆发前，其时效性有待加强；二是相关研究鲜有论述俄罗斯人工智能军事化的安全影响。鉴于此，在总结和吸收以往研究成果的基础上，本文将梳理俄罗斯人工智能军事化的新进展，分析俄罗斯人工智能军事化的动因，并探讨俄罗斯人工智能军事化造成的安全影响。

---

① 华盾：《人工智能时代的俄罗斯国家安全》，载《信息安全与通信保密》2021 年第 5 期。

② 苏崇阳、王晓捷、王钰茹：《俄罗斯军事人工智能发展与应用初探》，载《国防科技》2023 年第 3 期。

③ 华盾、封帅：《弱市场模式的曲折成长：俄罗斯人工智能产业发展探微》，载《俄罗斯东欧中亚研究》2020 年第 3 期。

④ 赵勋：《美俄人工智能军事应用对比研究》，载《国防科技工业》2020 年第 1 期。

⑤ 戢仕铭：《俄罗斯人工智能发展的能力约束及参与全球价值链的困境评估》，载《国际关系研究》2020 年第 1 期。

⑥ Anna Nadibaidze，“Russian Perceptions of Military AI，Automation，and Autonomy”. https：//www.fpri. org/wp－content/uploads/2022/01/012622－russia－ai－. pdf，访问时间：2024 年 5 月 3 日。

⑦ Shanshan Xian，“An Analysis of the Military Application and Development Path of Artificial Intelligence in the United States and Russia”，*Big Data Research*，Vol. 6，No. 4，2020，pp. 125－132.

一 俄罗斯人工智能军事化的新进展

俄罗斯立足本国国情和人工智能发展情况，正加快推进人工智能技术在武器装备上应用的研发和部署进程，提升武器装备智能化程度，借此提升本国的军事优势。俄罗斯人工智能军事化的新进展主要体现在以下方面。

（一）从国家层面构筑军用人工智能发展战略体系

俄罗斯已在国家层面形成了较为完善的军用人工智能发展战略体系。2019 年 10 月获批的俄《2030 年前国家人工智能发展战略》将人工智能发展上升至国家战略层面。该战略提出了未来十年俄罗斯人工智能的重点发展目标，包括支持人工智能基础和应用科学研究、开发和推广人工智能软件、提升数据的可访问性和质量、增加硬件的可用性等。在人工智能基础和应用科学研究方面，该战略重点支持以下三个领域：一是模拟生物决策系统的算法；二是自主学习及算法；三是复杂任务的自主分解及解决方案①。2021 年 7 月出台的《俄罗斯联邦国家安全战略》强调要确保俄罗斯国防工业综合体的技术独立性和创新性，确保在新型武器系统、军事和特种作战设备等领域的开发和生产中处于领先地位②。根据俄罗斯国家技术集团执行董事奥列格·叶夫图申科（Oleg Yevtushenko）的解释，这里所指的新型武器系统、军事和特种作战设备包括指挥控制系统、军用机器人、现代化战斗机、精确制导导弹等③。2024 年 2 月获批的新版《2030 年人工智能发展国家战略》强调要加强对大型语言模型的基础和应用性研究，提升超级计算机的算力。普京表示，2030 年前俄罗斯境内所有使用人工智能技术的超级计算机总算力将从 2022 年的 0.073exaflops（每秒一百亿亿次浮点运算）至少提升到 1 exaflops。该战略还要求开展国际合作，俄罗斯要同国外合作伙伴建立人工智能

① Указ Президента Российской Федерации от 10.10.2019 г. № 490，10 октября 2019 года. http：//www.kremlin.ru/acts/bank/44731，访问时间：2023 年 6 月 17 日。

② Указ Президента Российской Федерации О Стратегии национальной безопасности Российской Федерации. http：//actual.pravo.gov.ru/content/content.html，访问时间：2024 年 4 月 24 日。

③ Литовкин Дмитрий，Бездушная армия. Зачем Минобороны меняет солдат на роботов?. https：//tass.ru/opinions/11452767；У России достаточно сырья для вооружений，заверил “Ростех”. https：//ria.ru/20240410/syre－1939193573.html，访问时间：2024 年 4 月 24 日。

研究中心，加强人工智能基础研究工作等①。

（二）建立和完善军用人工智能管理机构

2019 年版的《2030 年前国家人工智能发展战略》指出，要成立由政府领导的统筹委员会，整体推进和协调各方行动，并创建由科学界和工业界代表组成的联合会，辅助人工智能政策的制定和实施。2021 年 1 月，俄罗斯国防部成立先进武器研究和测试中心，以加大对尖端武器的研发攻关力度。2022 年 8 月，俄罗斯国防部创新发展总局局长表示，俄罗斯军方已成立人工智能技术发展办公室，致力于开发人工智能武器，加快推动人工智能技术在军用和特种装备武器领域的应用②。2022 年 9 月，俄罗斯国家人工智能发展中心（Национальный центр развития искусственного интеллекта）正式启动。该中心的重点研究项目包括人工智能技术的基础性、系统性、前瞻性研究，主要研究方向为对话式人工智能、神经网络、机器学习、语音识别、计算机视觉等。2024 年 4 月，俄国防部长表示，国防部将创建一个无人机和机器人研发和生产中心。

（三）研发人工智能军事化项目

第一，建立涵盖战略级—战役级层面的指挥控制和决策管理系统。在战略层面，俄罗斯国家防御指挥中心利用智能监控与预测系统实时监控俄罗斯和全世界发生的一举一动，以随时掌握世界范围内的军事政治形势及俄罗斯的社会政治形势变化。该中心主要包括三个指挥中心：战略核力量指挥中心、作战指挥中心、第三指挥中心。该中心负责人表示，中心配备超级计算机，不仅数据计算能力是五角大楼的 3 倍，数据存储量更是五角大楼的 19 倍。中心正在加快推广人工智能技术，以确保俄罗斯拥有对外国竞争对手的战略优势③。在战役级层面，俄罗斯正将人工智能引入作战分析和决策环节，通过对从前线情报侦察和监视系统所

---

① Указ Президента Российской Федерации от 15. 02. 2024 № 124. http：//publication. pravo. gov. ru/document/0001202402150063，访问时间：2024 年 4 月 27 日。

② В Минобороны РФ создали управление по работе с искусственным интеллектом. https：//tass. ru/armiya – i – opk/15492531，访问时间：2024 年 4 月 27 日。

③ Алексей Рамм，Антон Лавров，В Центре шторма：как офицеры – операторы охраняют безопасность страны. https：//iz. ru/959129/aleksei – ramm – anton – lavrov/v – tcentre – shtorma – kak – ofitcery – operatory – okhraniaiut – bezopasnost – strany；“Russian Defense Data Center Outperforms US Facility Threefold：Official”. https：//sputnikglobe. com/20141219/1016046303. html，访问时间：2023 年 6 月 23 日。

搜集的海量数据进行快速分析和处理，帮助指挥员实现高效决策。俄罗斯常见的智能化指挥控制系统主要包括“仙女座－D”（Andromeda－D）、“火枪手－M”（Strelets－M）等。在具体实施过程中，俄军经常根据联合演习和战场实战对这些智能化指挥控制系统进行修正和完善。

第二，研制军用机器人，同时借助人工智能技术升级传统武器装备。在实体空间，俄罗斯主要采取以下两方面的措施：一是打造军用机器人。在陆地机器人方面，俄罗斯正在研发和部署“天王星－9”（Uran－9）、“平台－M”（Platform－M）、BR－2 等无人战车。在海洋机器人方面，俄罗斯主攻水面无人系统（无人艇）和水下无人系统（无人潜航器）两大类。无人艇主要包括 GRK 700 维兹尔号、CyberBoat－330、探索者（Explorer）等，无人潜航器主要有“加尔特尔”（Galtel）、“波塞冬”（Poseidon）核动力无人潜航器等。在空中机器人方面，俄罗斯正在部署和升级“柳叶刀”（Lancet）、“立方体”（KUB－BLA）等自杀式无人机。二是借助人工智能技术升级传统军事装备。通过为图－22M3M 远程轰炸机、“阿玛塔”主战坦克等传统武器装备配备人工智能技术，提升智能化探测和攻击能力。

在虚拟空间，俄罗斯主要采取以下三方面的措施：一是研发网络武器，提升智能化攻击能力。网络武器系统已在以俄罗斯为代表的网络空间优势国家出现智能化雏形①。俄乌冲突爆发后，俄罗斯正在全力开发复杂网络工具包，其中包括能实现自主化和智能化攻击的恶意软件，其产生的威力不亚于“震网”（Stuxne）攻击②。此外，有研究指出，俄罗斯黑客正使用大型语言模型 ChatGPT 来提升网络攻击能力。就当前而言，俄罗斯黑客正在利用 ChatGPT 研究与对乌特别军事行动有关的各种卫星和雷达技术③。根据 Check Point 软件技术公司的调查，俄罗斯黑客已经在探讨并尝试突破地理围栏的限制，以将 ChatGPT 用于制造恶意软件④。其

① 周磊、欧微：《透视外军网络战发展新趋势》，载《解放军报》2021 年 4 月 8 日。

② Grace B. Mueller，Benjamin Jensen，Brandon Valeriano，et al.，“Cyber Operations During the Russo－Ukrainian War”. https：//www. csis. org/analysis/cyber－operations－during－russo－ukrainian－war，访问时间：2023 年 7 月 9 日。

③ Karen Weise，“Hackers for China，Russia and Others Used OpenAI Systems，Report Says”. https：//www. nytimes. com/2024/02/14/technology/openai－microsoft－hackers. html，访问时间：2024 年 5 月 6 日。

④ Tiernan Ray，“Russian Hackers Are Trying to Break into ChatGPT，Says Check Point”. https：//www. zdnet. com/article/russian－hackers－are－trying－to－break－into－chatgpt－says－check－point/，访问时间：2024 年 5 月 6 日。

二是依托深度伪造技术对目标人物实施智能模仿。深度伪造技术是指通过深度学习算法篡改原始声音、图像和视频的智能处理技术①。据悉，俄罗斯的深度伪造技术可以使用几乎任何人作为动作模型或驱动图像来创建高分辨率的面部虚假视频②。三是利用社交机器人开展舆论斗争。社交机器人是指在社交平台中模仿正常用户自主进行操作并发布文本、图片、音频、视频等内容的自动化程序体。俄罗斯政府内部的管理部门控制着社交机器人的运作，其主要任务是通过在社交媒体平台上创建大量伪造的个人账户来传播虚假信息③。

（四）推动人工智能军事化项目的实战化运用

俄罗斯在叙利亚危机、俄乌冲突等地区冲突中注重部署和使用人工智能技术，并取得了较为显著的效果。以俄乌冲突为例，在战略级层面，由俄罗斯国家防御指挥中心负责人米津采夫领导的专业人员依托智能监控与预测系统，对战场各个环节进行动态跟踪和实时监控，随时掌握俄军和乌军在不同战线上的作战情况，以及美国和北约对乌军事援助的最新情况，从而确保俄罗斯军政领导人及时掌握战场环境、判断威胁性质，并对前线俄军实施有效指挥和控制。如在马里乌波尔战役期间，俄罗斯国家防御指挥中心及时截获了据守在亚速钢铁厂的乌克兰武装力量的无线电通信。据米津采夫介绍，被包围的民族主义团体武装分子和外国雇佣兵的无线电通话频率急剧增长，仅 2022 年 4 月 15 日一天，中心就监听到 367 次无线电消息④。

在战役层面，叙利亚危机之后，俄罗斯根据实战经验对“仙女座－D”等指挥控制系统实施升级改造，以更好地配合俄军战场行动。据俄国防部长介绍，俄军指挥控制系统的发展已取得重大进展，人工智能在对乌特别军事行动中的使用使俄

---

① 武琼：《乌克兰危机中网络空间对抗的影响及启示》，载《俄罗斯东欧中亚研究》2023 年第 3 期。

② Jim Nash，“New，Easier Way to Make Deepfakes Emerges from Russia”. https：//www.biometricupdate.com/202208/new－easier－way－to－make－deepfakes－emerges－from－russia，访问时间：2023 年 7 月 10 日。

③ Sarmīte Ēlerte，“Kremla Trolli”. https：//ir.lv/2014/7/18/kremla－trolli/，访问时间：2023 年 6 月 23 日。

④ Козин Владимир Петрович，Kiev Plans a Massive Provocation during Easter. It Denied Russian Offer to AFU to Surrender at “Azovstal” Plant. https：//mgimo.ru/about/news/experts/kiev－plans－a－nmassive－provocation－during－easter/，访问时间：2023 年 7 月 10 日。

军瞄准高精度目标的时间减少了数十倍①。在俄乌冲突中，俄罗斯主要使用最新型“火枪－M”和“仙女座－D”等指挥控制系统。这些指挥控制系统可以对战场上收集的海量作战数据进行分析和处理，帮助指挥官确定坦克、装甲车和火炮等重型武器以及重要军事设施的位置。在收到具体坐标后，指挥官随即派出战斗机或自杀式无人机对其实施火力打击。

在虚拟空间，俄罗斯主要采取以下三方面的措施：一是利用深度伪造技术制造虚假视频。如俄乌冲突爆发之初散播由深度伪造技术制作的总统泽连斯基的虚假讲话。二是使用恶意软件对乌克兰关键基础设施实施网络攻击。如 2022 年 4 月，乌克兰表示，俄罗斯黑客组织“沙虫”（Sandworm）使用一款名为“工业破坏者 2”（Industroyer 2）的恶意软件对乌克兰的电力基础设施实施网络攻击②。该恶意软件可以直接与电力设施中的设备交互，向变电站设备自主发送攻击命令，并且能借助模块化代码组件重新部署恶意软件以针对不同的实用程序③。三是利用社交机器人散布虚假信息。如 2023 年 7 月，乌克兰警方在文尼察等地摧毁了一个拥有 100 多名操作员的大型社交机器人农场。据悉，该农场的主要任务是诋毁乌克兰军队和国家领导人，并为俄罗斯特别军事行动辩护等。

（五）加强与长期盟友和合作伙伴的人工智能军事化合作

第一，长期盟友④。俄同这些国家的军事技术合作日益深入，军贸合作稳步推进。如俄白两国领导人于 2022 年 9 月签署《2025 年前白俄罗斯和俄罗斯实施军事技术合作计划》的法令，包括开展联合研究和开发新式武器；联合实施符合

① Глава Минобороны РФ заявил о планах внедрения новых способов ведения боевых действий. https：//topwar. ru/195177－glava－minoborony－rf－zajavil－o－planah－vnedrenija－novyh－sposobov－vedenija－boevyh－dejstvij. html，访问时间：2023 年 7 月 12 日。

② AJ Vicens，“Russian Hackers Thwarted in Attempt to Take Out Electrical Grid，Ukrainians Say”. https：//cyberscoop. com/ukrainian－electrical－grid－industroyer2－russia－sandworm/，访问时间：2023 年 7 月 24 日。

③ Andy Greenberg，“Russia’s Sandworm Hackers Attempted a Third Blackout in Ukraine”. https：//www. wired. com/story/sandworm－russia－ukraine－blackout－gru/，访问时间：2023 年 7 月 26 日。

④ 俄罗斯外交部公布的正式盟友名单显示，俄官方认定的盟友只有五个国家，包括白俄罗斯、亚美尼亚、哈萨克斯坦、吉尔吉斯斯坦、塔吉克斯坦。МИД перечислил долгосрочных союзников России. https：//lenta. ru/news/2023/03/01/soyuz/，访问时间：2023 年 7 月 27 日。

第三国利益的项目；参与在白俄罗斯和俄罗斯举行的军事技术合作活动等。两国可能涉及的军事技术合作包括数字化机载武器控制系统、数字化火控系统、高精度地基和空基武器，以及对防空导弹系统的现代化升级等①。此外，2021 年以来，俄罗斯向白俄罗斯、哈萨克斯坦等国出售了苏－30SM 多用途战斗机、米－35M武装直升机、S－400 防空导弹系统等现代化武器装备。

第二，合作伙伴。俄罗斯的合作伙伴主要包括印度、中国等国。以印度为例，一方面，两国军贸合作仍在稳步进行中。据统计，从 2018 年至 2023 年，俄罗斯向印度出口武器的总价值超过 130 亿美元②。另一方面，两国联合研发和生产现代化军事装备。2023 年 2 月，俄罗斯联邦军事技术合作局副局长表示，俄罗斯准备与印度分享“阿玛塔”技术，以便两国联合开发主战坦克。作为俄罗斯在重型装甲车领域的最新研发成果，该坦克采用无人炮塔，配备了一个单一的战术联系控制系统，并通过软件和硬件交互系统将所有系统连接起来③。2023 年，俄罗斯国家技术集团宣布与印度空军联合开发第五代战斗机苏－57。该款战机配备最先进的人工智能技术，帮助飞行员作出决策，同时具备无人机协同作战能力，能摧毁空中、地面和水下的各类目标④。

二　俄罗斯人工智能军事化的动因

俄罗斯之所以高度重视人工智能军事化的发展，主要基于以下几方面原因。

（一）俄罗斯素有重视军事技术的历史传统

俄罗斯重视军事技术发展有较为久远的历史。早在 20 世纪 20 年代和 30 年代，斯大林就反复强调，红军不能沉湎于昔日的荣耀，必须不断实现自身理论和

① Александр Алесин. Приоритеты военно－технического сотрудничества Беларуси и России. https：//minskdialogue. by/research/opinions/prioritety－voenno－takhnicheskogo－sotrudnichestva－belarusi－i－rossii，访问时间：2023 年 7 月 27 日。

② Объем экспорта военной продукции России в Индию за пять лет превысил $13 млрд. https：//tass. ru/ekonomika/17032217，访问时间：2024 年 4 月 28 日。

③ Россия готова поделиться с Индией технологиями “Арматы”，заявили в ФСВТС. https：//ria. ru/20230214/armata－1851836466. html，访问时间：2024 年 4 月 28 日。

④ Эксперт：особенности Су－57 позволят интегрировать в него передовое вооружение. https：//tass. ru/ekonomika/15017449，访问时间：2024 年 4 月 28 日。

武器装备的现代化。冷战期间，苏联除全力制造和部署洲际弹道导弹、核潜艇、战略轰炸机外，还注重研发无人机、自动化指挥控制系统等军用装备。1956 年，苏联在第 156 号实验设计局（OKB－156）成立“K 部门”，主要负责设计各型无人侦察和攻击机。随后苏联设计出了图－121 无人攻击机、图－123 和图－143 无人侦察机等。20 世纪 80 年代是苏联无人机发展的鼎盛时期，约 30 个军事单位配备了数千架无人机①。1974 年，苏联研发了一套名为“周界”（Perimeter）的自动化指挥控制系统。该系统主要功能是在苏联领导层和军事指挥机关被摧毁的情况下，计算机利用其自身储存的数据，自主完成战略核反击任务。苏联于 1984 年 11 月对“周界”系统进行了一次重大测试，成功击中堪察加半岛的重要目标。1985 年，该系统正式列装②。

2008 年的俄格战争虽然以俄罗斯的胜利而结束，但这场战争却让俄军认识到，传统的苏式军队和苏制武器装备已不适应现代战争的需要，加快武装力量现代化建设进程迫在眉睫。此后，俄罗斯大力推行以优化指挥系统、更新武器装备及完善军事训练体制为核心的“新面貌”改革③。随着人工智能技术在军事领域的快速发展和广泛运用，总统普京表示，当前发展人工智能的重要性不亚于苏联在 20 世纪 40 年代中期或 50 年代时期的核武器与导弹计划④。

（二）人工智能技术发展带动俄罗斯军事装备进步

人工智能赋能军事装备的技术机理包括机器感知、机器学习和机器行动三个阶段⑤：机器感知的目的是通过人工智能获取从战场上收集的图像、视频等海量数据；机器学习是指通过对相关作战数据进行深度学习，实现推理、智能计算等功能；机器行动是指军用机器人可以执行各种军事任务，以实现既定作战目标。

---

① Смирнов С. 45 й полк ВДВ – спецназ будущего. Офицеры. № 2. 2004，С. 28 – 31.

② David E. Hoffman，*Dead Hand*：*Reagan*，*Gorbachev and the Untold Story of the Cold War Arms Race*，London：Icon Books Ltd，2011，pp. 150 – 154.

③ 杨育才：《“新面貌”改革以来俄军的建设与发展》，载《俄罗斯东欧中亚研究》2017 年第 5 期。

④ Алексей Никольский，Путин сравнил значимость развития ИИ с атомными проектами в советское время. https：//ria. ru/20230719/ii－1885111515. html，访问时间：2023 年 8 月 23 日。

⑤ 肖晞、王一民：《人工智能赋能国家安全：理念、机理与路径》，载《探索》2023 年第 6 期。

在指挥控制系统方面，俄罗斯国家防御指挥中心的核心是一个特殊的软硬件综合设备。通过使用特殊算法，不仅能保持数据的完整性，还能从上至下整合各级军事组织，以确保指挥控制系统在战时能快速进入作战状态①。

在空中机器人方面，俄乌冲突爆发后，俄军在战场上频繁使用“柳叶刀”和“立方体”等自杀式无人机对乌军目标实施密集式打击。以“立方体”为例，该无人机配备人工智能视觉识别技术，能按类别和类型，智能化实时检测和识别1 000多个静态和动态物体，甚至能从90°的垂直视角中识别隐藏在茂密植被中的物体②。2024年2月，俄罗斯Hardberry－Rusfactor公司宣布，该公司已为在俄罗斯武装部队服役的所有类型无人机创建了一个名为NAKA的通用神经网络，安装在接收无人机摄像头视频的设备上以后，可以高精度识别包括豹式坦克、布莱德利步兵战车等在内的敌方目标和装备③。需要说明的是，随着俄罗斯无人机技术的迅速发展，反无人机技术也日益受到关注和重视。俄罗斯卡巴斯基实验室已研发出反无人机系统，通过构建人工神经网络，分析处理重要设施周边各类传感器收到的数据，同时运用特殊算法，迅速发现和识别无人机，自主进行分类，判断敌友，有针对性地作出反应④。此外，在陆地机器人方面，俄乌冲突爆发后，俄罗斯开始测试“马克”反坦克地面无人战车。该无人战车配备反坦克导弹、无人机、电子压制装置等作战模块，同时搭载了基于人工智能算法支持的多光谱视觉观测与数据处理系统，具有较强的智能化作战能力。测试结果证明，该车不仅能够自主识别并连续射击坦克及装甲车等作战目标，还能根据目标威胁程度优先打击高危目标⑤。

---

① Олег Владыкин，Центр круговой обороны страны. https：//nvo. ng. ru/realty/2014－12－05/1_oborona. html，访问时间：2024年4月24日。

② Zala Aero представила новую технологию на основе искусственного интеллекта. https：//kalashnikov. club/a/zala－aero－predstavila－novuyu－tekhnologiyu－na－osnove－iskusstvennogo－intellekta，访问时间：2023年7月12日。

③ Oleg Burunov，“Russia Unveils Drone Neural Network to Detect NATO Equipment in Special Op Zone”. https：//sputnikglobe. com/20240212/russia－unveils－drone－neural－network－to－detect－nato－equipment－in－special－op－zone－1116737245. html，访问时间：2024年4月21日。

④ 《最新实战AI武器系统》，https：//www. takungpao. com/news/232111/2023/1207/920427. html，访问时间：2024年4月21日。

⑤ 曹亚铂、刘凡凡：《俄新式无人战车亮相》，载《解放军报》2023年3月7日。

（三）应对周边威胁和安全挑战的现实需要

俄罗斯面临的安全威胁主要来自欧盟、北约、后苏联空间、俄罗斯毗邻地区、恐怖主义等①。与传统武器装备相比，人工智能军事化可以更好地帮助俄罗斯应对安全威胁。在实体空间，俄罗斯可以借助指挥决策系统监视敌方国家或军事组织。在和平时期，借助深度学习算法对从敌对国家收集的日常消费、教育经历、社交网络等海量个人数据中挖掘出关键信息，以随时掌握敌对国家的社会经济发展状况，进而帮助本国制定有针对性的打击计划②。面对美国及北约定期举行联合军演和加强东翼兵力部署等一系列军事举动，俄罗斯国家防御指挥中心的操作员实施高效监控和追踪，用该中心的话说："我们监视一切——从美国发射的弹道导弹到哈巴罗夫斯克的俄军士兵是否准时吃早餐。"③

在虚拟空间，俄罗斯主要使用人工智能技术提升网络空间攻击能力。俄罗斯黑客组织的网络攻击技术正在从机器学习中获益，包括鱼叉式网络钓鱼、漏洞发现、向目标网络传输恶意代码和逃避网络防御④。利用从恶意软件样本中检索到的数据进行机器学习，可以建立恶意软件模型⑤。随着数据的不断更新，开发者继续完善和升级现有的恶意软件，以实现复杂和隐蔽的网络攻击。美国人工智能国家安全委员会直言，目前披露的俄罗斯对人工智能驱动的网络攻击使用只是冰山一角⑥。俄乌冲突爆发后，以人工智能技术为后盾，俄罗斯正全力研发集自主化和智能化于一体的网络武器，力争形成"侦察—武器化—投送、利用和安装—

① 姜振军：《俄罗斯军事安全面临的威胁及其防范措施》，载《俄罗斯中亚东欧研究》2009 年第 1 期。

② 武琼、蒲婧新：《中美在海底光缆领域的战略竞争及影响》，载《和平与发展》2022 年第 4 期。

③ Алексей Рамм，Антон Лавров，В Центре шторма：как офицеры－операторы охраняют безопасность страны. https：//iz. ru/959129/aleksei－ramm－anton－lavrov/v－tcentre－shtorma－kak－ofitcery－operatory－okhraniaiut－bezopasnost－strany，访问时间：2023 年 9 月 12 日。

④ Ben Buchanan，John Bansemer，Dakota Cary，et al.，"Automating Cyber Attack，Center for Security and Emerging Technology". https：//cset. georgetown. edu/wp－content/uploads/CSET－Automating－Cyber－Attacks. pdf，访问时间：2023 年 9 月 20 日。

⑤ 《机器学习创建恶意软件，网络威胁亟待解决》，https：//www. thepaper. cn/newsDetail_forward_14357159，访问时间：2023 年 9 月 22 日。

⑥ "Final Report National Security Commission on Artificial Intelligence". https：//www. nscai. gov/wp－content/uploads/2021/03/Full－Report－Digital－1. pdf，访问时间：2023 年 9 月 22 日。

指挥控制—针对目标行动”① 的智能化作战能力。

（四）俄乌冲突的外溢效应

俄罗斯军方高层最初预计对乌特别军事行动能迅速实现既定目标，因此起初并未广泛使用人工智能技术。但随着冲突的持续进行，俄军伤亡人数不断增加。因此，俄罗斯军方高层越来越寄希望于通过研发和使用军用机器人来减少战斗过程中的士兵伤亡。无人机、无人战车等军用机器人非常适合在复杂多变的战场环境中不知疲倦和不厌其烦地执行枯燥、危险和时间漫长的任务。俄罗斯不断加大对无人机、无人战车等军用机器人的研发和部署力度，以代替人力执行危险的军事任务。2022 年 12 月，普京总统指示政府建立无人机系统的设计、测试、生产中心。2024 年 2 月，俄副总理兼工贸部长表示，俄罗斯将在未来 3 年投资1 000 亿卢布用于研发和生产无人机；俄国防部长表示，俄军每天在特别军事行动中使用数百架无人机，无人机日产量则已达到数千架。根据时任俄罗斯第一副总理别洛乌索夫的预测，俄罗斯计划到 2026 年底每年生产 1.8 万架无人机，到 2030 年，每年生产 3.2 万架②。

（五）世界主要军事强国发展以人工智能为代表的颠覆性技术

克里米亚入俄后，俄美关系日益恶化。基于此，美国在尖端军事技术领域的任何异动都会引起俄罗斯的高度警惕。特朗普第一任期内，美国军方加快推动人工智能军事化的发展，其重点发展领域包括情报、监视和侦察（ISR），后勤，网络空间作战，信息操纵和深度伪造，指挥和控制，半自主和自主运载工具，致命自主武器系统③。拜登政府继续展开战略化布局和系统性推进。据统计，美军正在研发至少 800 个与人工智能相关的军事项目④。据悉，仅美国国防部高级研究计划局就至少开展了 60 多个人工智能军事化项目，涉及复杂网络攻击实时分

---

① Jason Healey，“The Impact of Artificial Intelligence on Cyber Offence and Defence”. https：//www.aspistrategist. org. au/the - impact - of - artificial - intelligence - on - cyber - offence - and - defence/，访问时间：2023 年 10 月 22 日。

② Белоусов заявил，что Россия к концу 2026 года выйдет на объем выпуска 18 тыс. БПЛА в год. https：//tass. ru/ekonomika/17633385，访问时间：2024 年 7 月 26 日。

③ 武琼：《韩国人工智能战略的实施路径及发展前景研究》，载《情报杂志》2021 年第 4 期。

④ Frank Bajak，“Pentagon’s AI Initiatives Accelerate Hard Decisions on Lethal Autonomous Weapons”. https：//apnews. com/article/us - military - ai - projects - 0773b4937801e7a0573f44b57a9a5942，访问时间：2024 年 4 月 16 日。

析、欺诈性图像检测、全域战争动态杀伤链构建、人类语言技术、多模态自动目标识别等①。此外，美国不仅积极推进人工智能军事化项目的研发工作，还极为注重推进相关项目付诸实践运用。俄乌冲突爆发后，美国向乌军提供“荨麻”（Kropyva）、“元星座”（MetaConstellation）等情报侦察和作战指挥系统，以及“凤凰幽灵”（Phoenix Ghost）、“弹簧刀－300”（Switchblade－300）和“弹簧刀－600”等自杀式无人机。由此可见，以美国为代表的世界军事强国正在加快推进人工智能军事化项目的发展和实践运用，并将其视为增强综合国力和保障国家安全的重大战略举措。如果俄罗斯不抓住这一重大历史机遇，不仅会对国防实力造成负面影响，还会在人工智能等颠覆性技术领域受制于人。

三　俄罗斯人工智能军事化的安全影响

人工智能军事化是一把双刃剑，在提升侦察监视、指挥决策、火力打击等作战能力的同时，也带来了一系列不可忽视的安全影响。其中主要包括加深俄罗斯与美国及北约间的军备竞赛、增加俄罗斯与美国及北约间意外冲突的爆发风险、从内外两方面冲击战争伦理。

（一）加深俄罗斯与美国及北约间的军备竞赛

假若 A 国基于战略防御目的而发展军备，其对手 B 国担心 A 国的行为具有进攻性，因而也增强军备，这时就会产生安全困境。而 B 国持续增加军备的行为反过来又会刺激 A 国的反应，从而最终导致军备竞赛②。冷战时期，美苏投入大量资源，深陷由安全困境引起的核军备竞赛。

世界主要军事强国从国家安全层面出发，正在围绕人工智能军事化加快战略布局，以抢占未来战争战略制高点。由于国际社会处于无政府状态，为避免被竞争对手所追赶或超越，各方都在不断加大对人工智能军事化项目研发攻关的投入力度。长此以往，各方发展人工智能军事化项目的举动会增加对方的不安全感，刺激对手作出军事反应，从而逐渐使其陷入军备竞赛的恶性循环之中。

---

① “AI Next Campaign”. https：//www. darpa. mil/work－with－us/ai－next－campaign，访问时间：2024 年 4 月 16 日。

② John Herz，*Political Realism and Political Idealism*，Chicago：University & Chicago Press，1951，pp. 14－239.

近年来，美国及北约加快部署各类人工智能军事化项目，力争在人工智能军事化领域取得突破性进展。2018 年 10 月，美国、英国等 13 个北约成员国签署一项关于研发海上无人系统的技术合作协议，以提高海域态势感知能力，应对潜艇威胁。此外，鉴于北约成员国法国、西班牙和英国已启动了无人机“蜂群”项目，且成效显著，美国计划在此基础上利用本国的硬件和软件能力来整合北约盟国军队，联合部署低成本的无人机“蜂群”①。

面对美国及北约实施的无人机“蜂群”项目，俄罗斯正在发展能控制攻击无人机“蜂群”的空中指挥所，此举有助于指挥无人机“蜂群”对数百公里甚至数千公里之外的目标实施打击②。面对美国及北约实施的海上无人系统计划，俄罗斯则加快研发以“波塞冬”为代表的核动力无人潜航器。该款无人潜航器既可以装载常规弹药，也能携带核弹头，作战距离可达一万公里，最大下潜深度达一千米，能摧毁各种类型的作战目标。

俄罗斯与美国及北约竞相推动人工智能军事化，将持续加深双方在该领域的不信任感和不安全感，使双方陷入无法自拔的军备竞赛之中。

（二）增加俄罗斯与美国及北约间意外冲突的爆发风险

随着人工智能军事化的快速发展和广泛运用，军用机器人或将逐渐取代前线士兵和指挥官，成为对外军事行动的实际决策者和主要执行者。值得警惕的是，这一变化使俄罗斯与美国及北约间的战略稳定性受到严重挑战，意外冲突爆发的风险正在快速增长。意外冲突是指产生于疏忽、恐慌、误解，而不是冷静地预先谋划的军事冲突。在意外冲突中，通常存在着一些错误或疏忽，包括对敌方反应或对敌人意图的误读，在对方不知情的前提下发生随机事件或错误警报等③。虽然人工智能军事化的发展可以提升情报分析、指挥决策、武器平台、网络空间等领域的作战能力，但也进

① Tyler Jackson，“Thinking Big with Small Drones：An Allied Approach to Swarming”. https：//warontherocks. com/2023/03/thinking – big – with – small – drones – an – allied – approach – to – swarming/，访问时间：2023 年 10 月 15 日。

② Антон Лавров，Алексей Рамм，Вожак роя：Минобороны России заказало воздушный штаб для ударных дронов. https：//iz. ru/1283713/anton – lavrov – aleksei – ramm/vozhak – roia – minoborony – rossii – zakazalo – vozdushnyi – shtab – dlia – udarnykh – dronov，访问时间：2023 年 10 月 15 日。

③ Thomas C. Schelling，*Arms and Influence*：*With a New Preface and Afterword*，London：Yale University Press，2008，pp. 90 – 238.

一步增加了双方因误解误判或不必要的擦枪走火而意外升级的风险。

俄乌冲突爆发后，在俄罗斯和北约关系日趋紧张的氛围下，围绕双方红线的不确定性正在快速增加，稍有意外或误判，如一方进行了错误打击或不恰当的挑衅，引发另一方超出预期的报复行动，都可能导致局势迅速升级①。俄罗斯武装部队总参谋长格拉西莫夫认为，俄罗斯与美国及北约间的紧张局势一旦从量变走向质变，意外冲突爆发的可能性将会大大提升②。英国国防参谋长尼克·卡特（Nick Carter）表示，美国及北约和俄罗斯间爆发意外冲突的风险比冷战结束以来的任何时候都大，因为冷战期间用来平息双方对峙的外交渠道已不复存在③。

在人工智能军事化不断提速的背景下，俄罗斯与美国及北约可能发生的冲突领域与冷战期间有所不同，无人机、高超音速武器和互联网构成了新的挑战④。2023 年 6 月，在“空中卫士”联合军演举行期间，包括察打一体无人机在内的约 250 架各类战机参演。俄外交部表示，由于北约在靠近俄罗斯陆地边界、领空和领海的地区展开模拟击退俄罗斯“攻击”的演习，发生意外事件和局势恶化的风险正在成倍增加。在俄罗斯与北约紧张局势不断升级的情况下，这类演习无意中升级为意外冲突的危险极高⑤。

受到硬件故障和算法的不可解释性等因素影响，军用机器人不仅会作出错误认知和判断，而且还会引起难以解释的指挥决策偏见。尤其是当为这些军用机器人搭载进攻性武器时，它们可以在没有人为干预的情况下自主识别、选择和攻击

---

① Max Fisher，“As Russia Digs In，What’s the Risk of Nuclear War？‘It’s Not Zero.’”. https：//www. nytimes. com/2022/03/16/world/europe/ukraine – russia – nuclear – war. html，访问时间：2023 年 10 月 22 日。

② Герасимов предупредил о подготовке войск НАТО к масштабному конфликту. https：//russian. rt. com/world/news/699335 – gerasimov – nato – podgotovka – konflikt，访问时间：2024 年 7 月 26 日。

③ Глава генштаба Чехии не исключил вероятность войны НАТО с Россией. https：//tass. ru/mezhdunarodnaya – panorama/1787018，访问时间：2024 年 7 月 26 日。

④ Brendan Cole，“NATO Forges Secret Plans Against Russia— ‘We Are Ready To Fight Tonight’”. https：//www. newsweek. com/russia – ukraine – nato – alliance – war – 1801199，访问时间：2023 年 11 月 3 日。

⑤ “NATO Drills Near Russian Borders Raise Escalation Risk，Moscow Warns”. https：//sputnikglobe. com/20230921/risk – of – escalation – multiplies – due – to – nato – drills – near – russian – borders – – – moscow – 1113548659. html，访问时间：2023 年 11 月 3 日。

目标，这可能会超出指挥官预先制定的作战方案，从而使其作战行为和影响变得难以控制，这会大大提升国家间的军事冲突风险①。以算法的不可解释性为例，由于计算机代码的高度复杂性和不透明性及其工作原理和运行机制的隐蔽性，就连设计者也很难解释算法隐藏层的运行规律和因果逻辑关系，从而导致输出结果可能会偏离设计者最初的预定目标。

（三）从内外两方面冲击战争伦理

人工智能技术迅猛发展并被广泛应用于军事领域，也带来了一系列战争伦理风险。尤其是无人机等军用机器人在地区冲突和局部战争中被大量投入使用，一些公认的战争伦理正在受到前所未有的挑战。

第一，推动战争从迫不得已的手段逐步转变为优先尝试甚至是第一选择的手段。冷战期间，握有大量核武器的美苏之所以没有爆发核战争，与两国领导人的审慎判断和理性决策不无关系。一旦爆发大规模军事冲突，两国付出的政治和经济成本对双方领导人而言将异常高昂，因而产生战略威慑作用。

随着人工智能军事化的快速发展和广泛运用，通过向大型计算机模拟系统输入参战各方的兵力、装备、弹药等作战要素，能在近似实战环境和作战行动中全方位地对敌我双方的目标选择和兵力规模进行深度分析和精确预测，从而协助作战人员在瞬息万变的战场上作出正确决策。未来，随着战争形态加速向智能化方向演进，军事强国很可能会事前借助大型计算机兵棋推演系统模拟两军行动。一旦兵推结果显示“本国军队在战场上将所向披靡，敌国军队不堪一击”，战争很有可能会从一种无奈之举逐渐演变为解决问题的优先选择。

第二，判断发动或参与战争的责任主体日趋模糊化。在传统战争条件下，发动对外战争的政府是承担战争责任的主体。随着人工智能军事化的快速发展，以无人机、无人战车为代表的军用机器人在战场上大显身手。以无人机为例，主权国家或非国家行为体可以借助无人机实施“匿名式攻击”，以努力隐藏身份，确保无法追踪其来源。由此产生的令外界诟病的伦理问题便是难以确立战争责任。无处不在的军用机器人将会导致更加难以判断谁才是战争真正的发起者。

第三，加深区域性人道主义灾难。以无人机为例，就当前的技术水平而言，即使为无人机配备了进行精确识别的高分辨率数码相机、高清白光摄像机等设

① 武琼：《以色列人工智能军事化的新进展及其影响》，载《阿拉伯世界研究》2023 年第 3 期。

备，也很难保证其在打击作战目标时不产生任何附带损害，即平民的生命损失①。由于城市人口密度高、人员流动频繁，不管军用机器人技术如何成熟，在尽可能不误伤平民的前提下，对隐匿在城市大面积建筑物或主要道路中的伏兵、炮兵或狙击手进行精准打击是非常困难的。届时，大量运用军用机器人打击敌人很有可能会导致更多的平民伤亡。

结　论

为推动人工智能军事化的快速发展，俄罗斯正在投入大量资源，强化顶层设计，加快推动相关技术研发应用工作，已在无人战车和指挥决策系统等方面取得显著进展，同时积极将其运用于军事实践中，作战成效显著。如在指挥决策系统方面，俄罗斯不仅建立起涵盖战略级—战役级层面的指挥控制和决策管理系统，更是将其付诸实战。需要指出的是，与美国相比，俄罗斯的人工智能军事化发展存在一定的差距，如俄罗斯军用无人机技术明显落后世界先进水平。俄乌冲突爆发之初，乌克兰军队就大规模使用无人机进行前沿侦察和火炮校正等工作，之后更是派出自杀式无人机执行火力打击和效果评估任务。反观俄罗斯，无人机技术的落后使得俄罗斯在面对乌克兰这样的战场对手时很难形成非对称制胜优势。为解决该问题，俄罗斯不仅在国内建立无人机系统的设计和生产中心，还从伊朗大量采购自杀式无人机，两国甚至已在鞑靼斯坦的新工厂建立了一条无人机生产线。在受到西方国家严厉制裁的情况下，俄罗斯选择从伊朗采购自杀式无人机不失为一种现实选择。总而言之，俄罗斯在人工智能军事化领域取得了显著成果，但受到西方国家对俄技术封锁、芯片制造技术落后、高技术人才流失等因素掣肘，俄罗斯人工智能军事化的发展仍面临严峻挑战。

（责任编辑　聂侯诚）

① 武琼：《美国人工智能反恐：路径、动因与挑战》，载《新疆社会科学》2022 年第 3 期。