智能化“混合战争”及其影响和治理[1]

周意岷 张 零

【内容提要】人工智能的应用和影响已经成为国际关系领域广受关注的热点问题。本文通过考察2021年和2023年的巴以冲突、2022年爆发的乌克兰危机，分析了人工智能在战场上的效能，进而提出人工智能发展到深度学习阶段后能够在“混合战争”中完成人力资源替代、精准识别信息和多线程操作三项职能，在武装冲突中扮演“赋能者”的角色，可提高决策者的战场分析和反应能力，改变战争发展态势。人工智能在“混合战争”中的广泛应用将导致国际政治权力格局向有利于技术强国的方向发展，并改变国家之间、国家与非国家行为体之间的权力分配，这可能会加剧各国在技术领域的竞争以及国际关系的不平衡发展。因此，国际社会需要通过构建共同治理理念、安全协调机制和技术规则协议，完善针对智能化“混合战争”的全球治理。

【关键词】人工智能 混合战争 巴以冲突 乌克兰危机 全球治理

【作者简介】周意岷，西安工业大学马克思主义学院马克思主义基本原理教研部主任、副教授；张零，西安石油大学电子工程学院助教。

【中图分类号】D815
【文献标识码】A
【文章编号】1006-6241（2024）03-0106-26

[1] 本文系教育部人文社会科学基金青年项目“贸易战背景下中国特色混合战争理论研究”（项目编号：19YJCZH275）、陕西省社会科学基金年度项目“混合战争视域下人工智能武器的风险评估及治理研究”（项目编号：2023E012）的阶段性成果。作者感谢《和平与发展》匿名评审专家及编辑部对本文提出的宝贵修改意见，文中错漏概由本人负责。

随着人工智能（AI）技术的不断完善与成熟，其在军事领域的应用和对战争形态、国际安全的影响广受关注。智能化“混合战争”(Hybrid Warfare) 是在人工智能对“混合战争”的赋能下形成的一种新的战争形式，其应用实践导致各国面临的来自物理域、信息域和认知域[1]的智能化“混合威胁”日益严重。因此，对智能化“混合战争”及其影响进行深入探讨很有必要。本文试图利用文献梳理、归纳演绎、案例分析等定性研究方法，明确人工智能技术在“混合战争”中的应用路径，梳理人工智能武器在2021年和2023年的巴以冲突、2022年爆发的乌克兰危机中的战场效能，根据实战效果分析智能化“混合战争”对国际安全带来的影响，并提出其治理和规制的路径方案。

一、智能化“混合战争”及其特点

人工智能所扮演的“赋能者”角色使“混合战争”通过提高信息识别和分析的速度、精度、效率得到持续进化，并增加了战争的复杂程度。

（一）智能化“混合战争”的基本内涵

“混合战争”是一种集合了常规战争与非常规战争的新型军事战略，其将正面战场作战、游击战、经济战、网络战、认知战（包括干扰和改变敌人的认知过程、控制敌人的知识获取、扭曲敌人的文化价值观和思维方式）等多种手段糅合在一起，具有高度灵活性和适应性，战争目标由传统战争的以颠覆对方政权为主转变为以塑造对方偏好为主。2007年，美国著名军事专家弗兰克·霍夫曼（Frank G. Hoffman）在其研究报告《21世纪的冲突：混合战争的兴起》（Conflict in the 21st Century—The Rise of Hybrid Wars）中提出并系统阐述了“混合战争”的基本内涵。霍夫曼指出：“混合战争涵盖了一系列不同形式的战争手段，包括常规武装力量、非常规战术和技术、恐怖

[1] 物理域是指物理实体（包括各类装备和人员）活动的领域；信息域是指信息产生、流通、交互的领域，可分为电磁空间和网络空间；认知域是指人的主观意识活动的领域。

袭击（如无差别使用暴力、威慑、制造社会混乱）等。”[1]同年，美国另一名军事专家玛格丽特·邦德（Margaret S. Bond）也在其关于“混合战争”的文章中指出，“混合战争意味着将庞大的军事力量投入到更加多元化的任务之中，包括维和与人道主义救援、预防冲突、执行常规军事行动、战后重建政治与经济秩序以确保和平与安全等”[2]，因而具有全向性、同步性和非对称性。2013年，俄罗斯联邦武装力量总参谋长瓦列里·格拉西莫夫(Valery Gerasimov)对“混合战争”理论做了进一步的发展完善。他在《科学在预测中的价值》一文中指出：在21世纪，战争与和平之间的界限日益模糊，不宣而战会更加普遍，战争样式也会与以往有所不同，非军事手段日益成为实现政治与战略目标的重要角色，在某些情境下甚至会比军事手段更加有效。[3]他敦促俄罗斯使用军事、科技、媒体、政治和情报策略多管齐下的“混合战争”战术，以最少的成本动摇敌人的根基。[4]

智能化“混合战争”是利用以人工智能技术为主的一系列高科技手段进行的一种“混合战争”形式。在智能化“混合战争”中，人工智能技术被广泛应用于情报收集、指挥决策、对抗操作等多个环节，大大提高了战争的效率和效果。例如，通过AI算法，可以快速分析和处理大量情报数据，为决策者提供有价值的信息；通过自动化系统，可以实现对敌方的精确打击，减少无辜伤害。由于“混合战争”具有持久性、非对称性和多维性的特征，并且覆盖物理域、信息域和认知域三个战争维度，所以需要人工智能在人力资源替代、精准识别信息和多线程操作三个方面发挥作用，通过

[1] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid War*, Potomac Institute for Policy Studies, December 2007, p.14.

[2] Margaret S. Bond, “Hybrid War: A New Paradigm for Stability Operations in Failing States,” U.S. Army War College, March 30, 2007, p.4.

[3] Valery Gerasimov, “The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations,” *Voyenno-Promyshlennyy Kurier*, February 26, 2013.

[4] 邵永灵：《混合战争：21世纪的战争新形态》，光明网，2019年10月25日，https://junshi.gmw.cn/2019-10/25/content_33264698.htm。

不断创新战争理念、战争形态和战争手段，以期在多元化、复杂化的“混合战争”中取得优势。

（二）智能化“混合战争”产生的时代土壤

首先，人工智能技术的深入应用使得战争行动更加智能化和自动化。一是基于深度神经网络的人工智能促进作战单元逐步实现自主化和智能化，使战争形态不断向自主武器主导的智能化“无人战争”演进[1]；二是人工智能技术引发了军事装备的革命性变化，致命性自主武器（LAWS）的集群式作战可能成为未来战争的主角和主要作战方式[2]；三是致命性自主武器的广泛应用表明，算法已然成为人工智能时代社会变革的关键驱动力量和新秩序的塑造者。[3]

其次，人工智能技术在涉及国家安全的诸多领域应用广泛。一是人工智能技术对网络安全、信息安全、经济与金融安全等非传统安全构成多维挑战[4]；二是目前很难阻止人工智能被恐怖组织用作发动恐袭的工具，反恐力量与恐怖组织可能面临在人工智能领域的博弈[5]；三是高度发达的人工智能技术与国际无政府状态的深度结合将会给人类整体利益带来不可预知的制度性风险。[6]

再次，除技术因素外，国际安全环境的变化加速了智能化“混合战争”的形成。随着全球化和信息化的深入发展，国际安全环境变得日益复杂，

---

[1] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War*, New York: W. W. Norton & Company, 2018, p.5.

[2] 傅莹：《人工智能对国际关系的影响初析》，载《国际政治科学》2019年第1期，第7页。

[3] 董青岭、朱玥：《人工智能时代的算法正义与秩序构建》，载《探索与争鸣》2021年第3期，第82—86页。

[4] Michael C. Horowitz, Gregory C. Allen, Edoardo Saravalle, etc., *Artificial Intelligence and International Security*, Center for a New American Security, 2018, p.3.

[5] 傅瑜、陈定定：《人工智能在反恐活动中的应用、影响及风险》，载《国际展望》2018年第4期，第136页。

[6] 封帅：《人工智能时代的国际关系：走向变革且不平等的世界》，载《外交评论》2018年第1期，第128—156页。

传统的战略战术和攻防手段已经无法满足维护国家政治安全、国土安全和军事安全的需求，特别是网络战、认知战、无人化战争等新型战争形态的出现，使得战争更加需要人工智能技术的支持。

（三）智能化“混合战争”的特点

“混合战争”总的目的是在精神生产领域（spiritual production，人类脑力劳动创造以及表现精神性价值的各种活动）[1]、经济领域和安全领域剥夺敌人的抵抗能力。[2] 传统“混合战争”强调军事手段和非军事手段的综合运用，并以较低的成本达成战争目标。智能化“混合战争”是在“混合战争”的基础上融入前沿科技的最新成果，特别是人工智能技术，因而在战略战术上更加复杂，更加依赖高科技。

第一，智能化“混合战争”更加注重人机结合。由于人工智能可以在极短的时间内处理和完成大量任务，甚至在没有错误的情况下进行计算和预测，具备在复杂的战争环境中替代人类的潜力，所以智能化“混合战争”对于人力的依赖有所降低，无人化作战成为常态。但是，人工智能技术的发展水平和人工智能行为的不可预测性，决定了人类不能完全放弃战争主导权和决策权，而是需要人类智力和机器智能互补互动，实现有人系统与无人系统的紧密结合，建立“人脑 +AI”协作运行机制。

第二，智能化“混合战争”更加注重在大数据、算法、算力等方面的优势。传统“混合战争”主张根据情况变化有选择地使用多种手段完成既定目标，高效而节省地运用实力。智能化“混合战争”则充分利用人工智能在优化流程和提高效率方面的潜力，能够快速高效地收集、处理和分析数据，借助大数据分析优化作战规划和流程，精准掌握和预测对方行动，大幅加快决策进程，提高反应速度。因此，智能化“混合战争”要求提高对技术领域的投入，在大数据收集和处理、算法、算力等方面超越对手。

[1] 李厚羿：《马克思“精神生产”概念的当代辨析》，载《哲学研究》2023 年第 4 期，第 34 页。

[2] *Сивков К*. Приказано оболванить Гибридная война отличается исключительным многообразием методов и форм // Военно-промышленный курьер, 17.02.2016.

第三，智能化“混合战争”的潜在风险更高。人工智能武器在替代人力和降低成本的同时，也降低了战争门槛，导致极端行为增加，威胁国际安全；生成式人工智能的深度伪造能力可轻易制作和散布虚假图片和视频，从而激化社会矛盾、干扰公众认知，引发社会忧虑和信任危机，造成各国内部社会撕裂和国家之间的猜疑；人工智能军民两用和便于传播的特质导致智能化“混合战争”更加难以被察觉，增加了为抢占先机而主动发起进攻的潜在风险；无人化作战可能导致人类被排除在战场决策之外，失去对致命性自主武器系统的控制，使其在自主搜索、识别并打击目标的过程中超出指挥官预先制定的作战方案，造成主动伤害平民甚至整个人类的法理和伦理问题。

二、人工智能在智能化“混合战争”中的应用路径

人工智能的发展大致可以分为自动控制（Automation）、机器学习（Machine Learning）和深度学习（Deep Learning）三个阶段。作为最基础的人工智能技术，自动控制是根据已设定好的程序执行脚本任务的自动化系统。2000 年以后，机器学习系统逐步成熟。这种系统不需要事先编程，而是通过读取大数据识别目标行为模式，通过自我行为修正提高对未来行为模式的分类能力。2010 年之后，对深度学习系统的研究逐步兴起。深度学习系统使用多层人工神经网络识别数据模式，而不是像机器学习系统那样针对特定任务使用特定算法。[1] 智能化“混合战争”的特征要求人工智能能够执行人力资源替代、精准识别信息和多线程操作三类任务。三类人工智能系统在智能化“混合战争”中不同的应用路径（见表 1）形成了智能化“混合战争”不同的发展阶段。

[1] Jerry Kaplan, *Artificial Intelligence: What Everyone Needs to Know*, Oxford, UK: Oxford University Press, 2016, pp.27–34.

表1 人工智能在智能化“混合战争”中的应用路径

阶 段	人力替代	精准识别	多线程操作
自动控制	机械机器人	关键词提取	无
机器学习	自动驾驶载具	情报分析和技术侦察、信息精准投放	辅助决策
深度学习	致命性自主武器系统	检测系统漏洞、预测目标行为	自主决策

资料来源：作者自制。

（一）自动控制：智能化“混合战争”的雏形

自动控制系统是人工智能最基本的应用形态，虽然能够自动执行脚本任务，但是需要事先编程，且能够完成的技术动作仅限于简单的机械化动作。这一阶段的人工智能以辅助行动为主，尚不具备多线程操作的能力。

自动控制系统在搜集和分析情报方面的能力较为原始，基本停留在搜索引擎经常使用的关键词提取技术，通过设定好的算法提取目标词汇或短语，找出海量信息中的关键点，再交由人工识别和分析。虽然随着算法的进步，自动控制系统提取关键词的速度和精度不断提高，但是仍不具备主动分析和处理信息的能力。

在自动控制系统基础上开发的机器人属于比较初级的机械机器人，其本质上属于人体机能的延伸，最早主要应用于工业领域，从事流水线上繁重固化的加工装配工作。机械机器人虽然只是半人工智能，但也能够在“混合战争”中担负辅助侦察、清除危险物品、自杀性攻击、运送物资等任务。此类设备由于价格低廉，往往受到恐怖组织、极端组织等缺乏足够资源支持的非国家行为体的青睐。

（二）机器学习：智能化“混合战争”的进阶

机器学习阶段的人工智能已经具备了定制性和通用性，可以处理较为

复杂的问题，并在一定程度上拥有了学习能力，能够在大数据的支持下从事不熟悉领域的工作。因而，这一阶段的人工智能可用于提高作战系统的灵活性和针对性，从而为“混合战争”的推进提供更多支持和帮助。

在人力资源替代方面，以无人机为代表的自动化载具由遥控阶段进入半自主阶段，自动驾驶载具大量进入军事领域。借助 5G 传输、云计算和大数据技术，自动驾驶载具能够自主完成运行环境识别并计算出最佳运动轨迹，操作者则可腾出精力专心完成侦察、破坏、精确打击等重要任务。除了常规战场，自动驾驶载具在非常规战场中也能够凭借高超的机动能力潜入人类难以进入的关键区域、设施和机构，完成相应任务。

在精准识别方面，进化到机器学习阶段的人工智能在图像识别领域已经超越人类，甚至能够在没有精确资料的情况下通过人脸识别技术标记出人群中的危险目标。人工智能通过机器学习可以找出一些事件之间存在的隐秘关联性，从而为一些特别行动提供切入点。“人工智能可以从海量数据中迅速而精确地确定各类事件之间的相互关系，预测当事人的下一步行动。”[1] 人工智能还可通过对不同人群的精准分析向其定向投送信息，根据不同人的阅读习惯和思维方式编辑信息的内容和表达方式，以构筑信息壁垒，达到影响他们偏好和认同的效果。

在多线程操作方面，机器学习虽不能完全接管作战指挥系统，但是可以依靠速度优势加快决策进程，扩大在信息化战场中的对抗优势。以空军为例，在人工智能接管空中支援、侦察和协同打击任务之后，指挥官只需根据战场形势作出最重要的决策。从理论上讲，机器学习系统可在几毫秒内对作战空间的变化做出反应[2]，而任何人工团队都无法达到这种速度。但是，基于机器学习的人工智能仍不够完善。

---

[1] Eric Schmidt, Jared Cohen, *The New Digital Age: Reshaping the Future of People, Nations and Business*, London: John Murray, 2013, pp.170−171.

[2] Sergey Levine, Peter Pastor, Alex Krizhevsky, Deirdre Quillen, “Learning Hand−Eye Coordination for Robotic Grasping with Deep Learning and Large−Scale Data Collection,” *International Journal of Robotics Research*, 2017, 37(4−5), pp.421−436.

（三）深度学习：智能化“混合战争”的成熟

深度学习是一种复杂的机器学习算法，其概念源于对人工神经网络的研究，最终目标是让人工智能像人脑一样具有分析、学习和认知能力，形成真正的“类人”智能。2006年，谷歌公司副总裁杰弗里·辛顿（Geoffrey Hinton）首先提出建立多层神经网络的有效方法。随后，美国的IBM和中国的科大讯飞、百度、中科院自动化所等机构投入到深度学习的开发之中，并取得了一系列成果。

首先，自动驾驶载具将进化为致命性自主武器系统。这种系统能够在不依赖人类指令的条件下完成目标识别、武器选择和精确打击等一系列操作。根据作战任务划分，致命性自主武器系统可分为无人机平台、无人地面载具平台、无人航行器、智能弹药等。2023年8月，美国国防部常务副部长凯瑟琳·希克斯（Kathleen Hicks）公布“复制器”计划（Replicator Initiative），首要任务是在未来18至24个月内，在陆海空多个领域部署数千个自主武器系统[1]；美国海军计划于2045年前配备150艘大型无人舰艇和潜航器，发挥“感知”和“辅助火力”作用[2]；美国空军计划通过Gremlins、OFFSET、Skyborg等项目[3]，快速推进无人机蜂群作战技术的发展。英国、俄罗斯、以色列、土耳其等国也在不断推进无人机蜂群的验证实验。

其次，进化到深度学习阶段的人工智能除了能够识别图像、语音、文字等静态信息之外，还能够借助粒子群优化算法、神经网络算法、蚁群优

[1] Joseph Clark, “Defense Officials Report Progress on Replicator Initiative,” DOD News, December 1, 2023, https://www.defense.gov/News/News-Stories/Article/Article/3604459/defense-officials-report-progress-on-replicator-initiative/.

[2] U.S. Naval Institute, “UPDATED: Navy’s Force Design 2045 Plans for 373 Ship Fleet, 150 Unmanned Vessels,” July 26, 2022, https://news.usni.org/2022/07/26/navys-force-design-2045-plans-for-373-ship-fleet-150-unmanned-Vessels.

[3] 美国国防高级研究计划局于2015年启动Gremlins项目，旨在开发可回收和重复使用的无人机；于2016年启动OFFSET项目，旨在开发无人机的进攻性蜂群战术；于2018年启动Skyborg项目，旨在开发和部署一种人工智能驱动的无人机系统，它可以与有人飞行器进行协同操作。

化算法、遗传算法等[1]，识别和破解更为复杂的信息结构。2020年，谷歌旗下的DeepMind公司开发出AlphaFold算法[2]，用于预测蛋白质结构[3]；2022年，该算法破解了几乎所有已知的蛋白质结构，构建起超过2亿种已知蛋白质结构的数据库。在可预见的未来，同类算法可用于探测网络系统的漏洞，计算出对方金融系统、贸易系统、教育系统、交通系统、工业系统等现实社会领域中的弱点，并有针对性的发起攻击；这种算法甚至能够预测每个个体的行为模式，以确定“混合战争”的合作对象、可利用群体以及清除目标，实现侦察、探测、通信与干扰自适应一体化设计技术。

再次，人工智能不再是决策环节中的辅助角色，而是凭借速度优势主导决策，在更短时间内作出更加科学合理的决策，并无缝接入行动环节。2022年12月，美国人工智能研究实验室OpenAI推出了人工智能技术驱动的自然语言处理工具ChatGPT。该程序拥有语言理解和文本生成能力，能够执行文字编辑、看图作答、数据推理、分析图表、视频编辑、图片生成、翻译、编写代码等任务；ChatGPT-4甚至能够在司法考试中取得前10%的成绩，在SAT数学考试中得到700分（总分800分），在生物奥林匹克竞赛中进入前1%的排名。人工智能凭借先进算法、庞大的数据库和语料库，获得了超越人类的学习速度和信息处理速度，具备了取代部分人类工作的可能性，从而能够构建一个深度参与“混合战争”的人工智能平台。

---

[1] 粒子群优化算法（Particle Swarm Optimization, PSO）是一种全局优化算法，基本思想是通过模拟群体行为来寻找问题的最优解；神经网络算法(Artificial Neural Network, ANN)是一种模拟人脑神经系统的工作方式，对数据进行分析和学习的算法；蚁群优化算法（Ant Colony Optimization，ACO）是一种模拟自然界蚂蚁觅食行为的优化搜索算法，主要用于解决一些复杂的组合优化问题；遗传算法(Genetic Algorithm)以生物学中的进化论为基础，通过模拟自然界中的生物进化过程来解决优化问题。

[2] AlphaFold算法使用一个深度神经网络，通过大量的训练数据（已知的蛋白质结构）来学习如何预测蛋白质的三维结构，然后在给定一个新的蛋白质氨基酸序列时，预测出其可能的三维结构。

[3] Tom Whipple, “DeepMind Finds Biology’s ‘Holy Grail’ with Answer to Protein Problem,” *The Times*, November 20, 2020.

三、智能化“混合战争”的战场效能：以巴以冲突和乌克兰危机为例

随着人工智能更加频繁地应用在武装冲突和战争之中，最新技术成果与“混合战争”的结合深刻影响了战争的形态，赋予了“混合战争”新的发展方向和作战能量。其中，2021年和2023年的巴以冲突、2022年爆发的乌克兰危机都充分体现了智能化“混合战争”巨大的战场效能。

（一）2021年巴以冲突

以色列在2006年与黎巴嫩真主党的武装冲突中遭遇失败后，深入分析原因、总结教训，在国防建设中加大技术和资金投入，充分运用人工智能技术的最新成果，加快推进“混合战争”手段的智能化转型，并在2021年的巴以冲突中取得了良好战果。所以，以色列国防军将2021年的巴以冲突定义为“第一次人工智能战争”。

第一，通过算法战精确提取情报信息。以色列国防军在2006年与黎巴嫩真主党武装冲突中的重大失误之一，就是因情报不足难以定位真主党军事力量的部署情况。而2021年巴以冲突爆发后，以色列利用卫星、无人机和特工对冲突地区实施不间断的侦察监视，收集大量图像信息、通讯数据和网络动态，随后通过“炼金术士”（Alchemist）、“福音”（Gospel）、“智慧深度”（Depth of Wisdom）等人工智能系统处理、整合海量数据，精准绘制出冲突区域情景全图，并标注巴勒斯坦伊斯兰抵抗运动组织（哈马斯）在加沙地带各类目标的精确位置。据当时报道称，辛贝特（Shin Bet，以色列国家安全局）建立了加沙地带居民楼、办公楼、医院内民众的电话号码库，对哈马斯在该地区的情况动态了如指掌。[1]

[1] Yaakov Katz, “Israel’s Gaza War is like No Other Military Operation in History,” Jerusalem Post, May 21, 2021, https://www.jpost.com/opinion/israels-gaza-operation-is-like-no-other-military-op-in-history-opinion-668709.

第二，通过先进武器系统实施精确防御和打击。为了降低国内外的舆论压力，以色列在2021年巴以冲突中大量使用人工智能武器和人工智能赋能武器，以提高打击精准度，尽量避免平民伤亡。在空袭行动中，以色列放弃了以往的大规模轰炸策略，转而使用“敲房顶”（Roof Knocking）战术，通过精准识别和精确打击减少误伤概率。该战术首先借助人工智能算法确定潜在打击目标，然后由人工选择目标并授权发动攻击；如果涉及平民设施，则由情报机构在发动攻击前两小时对目标内所有手机发送短信或电话警告；发动攻击时，首先使用两发空包弹作为警告射击，随后使用GBU-31联合直接攻击炸弹、GBU-12激光制导炸弹等对目标建筑屋顶实施打击，确保只摧毁目标建筑而不伤及附近居民楼。[1]通过这种方式，以色列定点摧毁了哈马斯的银行大楼、领导人住宅、情报机构等多处重要设施。为了减少误伤概率，以色列还使用由刀片代替炸药、仅仅依靠动能和刀刃击杀的AGM-114R9X“忍者”导弹对哈马斯多名高级指挥官和工程师进行定点清除。[2]另外，面对大量来袭的火箭弹，以色列不再采用疏散居民的方式，而是投入“铁穹”(Iron Dome)防御系统，利用雷达和其他监测设备检测、追踪和拦截来袭的火箭弹或短程导弹。“铁穹”系统使用以色列mPrest Systems软件公司开发的战斗管理和武器控制单元（BMC），一旦检测到威胁，其人工智能软件会立即分析来袭弹药的轨迹，然后决定是否拦截，并自动识别和忽略不构成威胁的火箭弹，整个过程在几秒钟内完成。在其辅助下，作战系统能够同时定位多个目标并根据具体情况制定应对策略。[3]以色列军方自称“铁穹”系统在2021年巴以冲突中的拦截成功率高达85%以上。

---

[1] Yaakov Katz, “How the IDF Invented ‘Roof Knocking’, the Tactic that Saves Lives in Gaza,” *Jerusalem Post*, March 25, 2021, https://www.jpost.com/arab-israeli-conflict/the-story-of-idfs-innovative-tactic-to-avoid-civilian-casualties-in-gaza-663170.

[2]《以色列国防军：24小时内摧毁12名哈马斯指挥官住所》，新华网，2021年5月19日，http://www.xinhuanet.com/mil/2021-05/19/c_1211161467.htm。

[3] Seth J. Frantzman, “Rafael Anticipates Iron Beam Laser System Could Deploy in Two Years,” Defense News, October 8, 2022, https://www.defensenews.com/industry/2022/10/07/rafael-anticipates-iron-beam-laser-system-could-deploy-in-two-years.

第三，通过社交媒体发动认知战攻势。以色列在2006年与黎巴嫩真主党的冲突中虽然遭受了损失，但其在战场上并未完全处于下风，主要是黎巴嫩真主党的网络宣传给世界营造了以色列完全被动挨打的印象，令以色列在国际舆论压力下不得不做出让步。因此，以色列认真吸取了这次教训，此后开始重视网络宣传。2021年5月巴以冲突爆发后，以色列不断通过人工智能算法分析社交媒体用户的爱好和倾向，然后有针对性地推送以军作战动态，重点宣传以军为减少加沙地带平民伤亡而付出的努力，并“揭露”哈马斯高官的“贪腐”状况，以弱化加沙平民和国际舆论对哈马斯的支持，提高自身的“正义性”与“合理性”。

虽然以色列和哈马斯在这次冲突中都注重采用“混合战争”策略，但双方的技术实力尤其是在人工智能技术上的差距成为决定战争胜负的关键。以军情报部队高层表示：“人工智能首次成为打击敌人的关键组成部分和力量倍增器。”[1]

（二）2022年乌克兰危机

2022年2月，俄罗斯对乌克兰发动“特别军事行动”，新一轮乌克兰危机爆发。发动“特别军事行动”之初，俄军共部署了超过120个营级战斗群[2]，俄空天军的作战飞机数量是乌克兰空军的近15倍。俄军虽然在军事实力对比上占尽优势，但在实战中却未能取得碾压性战果，其中一个很重要的原因就是乌克兰在同俄罗斯的“混合战争”中，借助美国的信息技术特别是人工智能优势抵消了俄罗斯很大一部分军事实力优势。

第一，人工智能赋能无人机，实施精确打击。乌克兰危机爆发后，美国科技公司Clearview AI向乌克兰国防部提供了人脸识别技术，并向乌军开放AI人脸识别数据库和搜索引擎。据统计，该数据库中收录了超过100

[1] 成高帅、郭宇：《第一次人工智能战争？》，载《中国国防报》2021年7月13日，第4版。

[2] 胡钦：《从俄乌冲突“活剧”窥探战争形式变化》，载《世界知识》2022年第10期，第61页。

亿张人脸图像和20亿张照片[1]，配合北约国家提供的TB-2“旗手”、RQ-20“美洲狮”和UCAV“弹簧刀”等型号的无人机，对俄军作战装备及战斗人员实施精准打击，使其遭受重大损失。虽然俄军也动用了“海雕-10”“海雕-30”“前哨-R”“猎户座”“扎拉·基布”（KUB-BLA）等型号的无人机和地面机器人进行反击，但因在人工智能技术方面存在短板而在无人机对抗中处于下风，导致其在基辅、哈尔科夫等战略要地的进攻受挫。2023年，乌克兰200多家参与无人机生产的公司计划借助人工智能对无人机进行重大升级，新的人工智能软件可使无人机在受到俄军电子干扰时，仍能识别目标的物理特征和调整飞行姿态，以保持对移动目标的锁定并完成战场任务，从而进一步增强乌军的火力和侦察能力。[2]

第二，人工智能整合数据，获取信息优势。乌克兰危机爆发后，美国将其侦察卫星和侦察机获取的战场信息共享给乌军，并通过Seekr Technologies Inc、Semantic AI、Primer、Palantir Technology等科技公司整合各类情报信息，运用人工智能技术将目标和物体识别与卫星地图相结合以提升信息分析质量，从各类开源数据中寻找俄军动向，精准识别俄军人员、武器、作战系统或作战单位，分析其战略战术，预测俄军行动方针，辅助战场决策。俄罗斯虽然已经在2020年初建立一套完整的军事指挥和控制系统，但其天基、空基、地基的电子和光学侦察能力智能化改进仍处于试运行阶段。[3]因此，在实际应用场景中，俄军鲜有将人工智能投入战场使用的案例。2023年6月，据社交软件“电报”（Telegram）俄语频道报道，俄“柳叶刀—3”（Lancet-3）无人机正在使用卷积神经网络[4]（Convolutional

[1] 徐舒悦、高飞：《乌克兰危机背景下“混合战争”理论与实践评析》，载《和平与发展》2023年第4期，第84—85页。

[2] John Hudson and Kostiantyn Khudov, “The War in Ukraine is Spurring a Revolution in Drone Warfare Using AI,” *The Washington Post*, July 26, 2023, https://www.washingtonpost.com/world/2023/07/26/drones-ai-ukraine-war-innovation.

[3] 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，第105页。

[4] 卷积神经网络是一类包含卷积计算且具有深度结构的前馈神经网络，是深度学习的代表算法之一。

Neural Networks, CNN）收集、分类和分析其所收集到的图像和视频内容。[1] 可以肯定的是，俄军正寻求在信息战中使用人工智能，但其应用水平与乌克兰战场的实际需求尚存在不小的差距，导致俄军在部分地区陷入被动。

第三，人工智能助力深度伪造（Deepfake）和推荐算法，影响国际舆论。乌克兰危机爆发初期，俄罗斯通过混合—认知战（hybrid-cognitive war）在乌克兰全国各地制造舆论影响，指控乌克兰政府存在严重腐败等种种弊端，以及西方对乌克兰的援助不可靠等[2]；利用乌克兰总统泽连斯基（Volodymyr Zelensky）的脸部图像制作深度伪造视频，呼吁乌克兰士兵向俄军投降，并将视频在即时通讯系统上快速传播。[3] 然而，由于多数主流社交媒体平台受西方国家控制，俄罗斯媒体的平台账号或是被直接封禁、限流，或是被贴上“虚假新闻”的标签。在国际上拥有广泛影响的“今日俄罗斯”（Russia Today，RT）电视台和俄罗斯卫星通讯社（Sputnik）更是西方各国的重点防范对象。[4] 比如，X（即原来的Twitter）、Facebook、YouTube等国际主流社交媒体通过推荐算法对“今日俄罗斯”电视台和俄罗斯卫星通讯社等账号限流，降低它们在用户推荐页面中的出现频率，限制俄罗斯媒体的传播范围。同时，西方主流社交媒体平台放任自媒体大范围传播使用深度伪造技术制作的假图片和假视频，传播对乌克兰有利的信息，引发国际舆论同情乌克兰并对俄军强烈谴责，塑造乌军民“坚强抵抗”和俄军“弱鸡”形象，动摇俄军心民心，以营造舆论向乌克兰“一边倒”态势。

（三）2023年巴以冲突

2023年10月7日，哈马斯对以色列发动代号为“阿克萨洪水”（Al-

[1] Samuel Bendett, “Here’s How the Russian Military Is Organizing to Develop AI,” Defense One, June 20, 2018, https://www.defenseone.com/ideas/2018/07/russian-militarys-ai-development-roadmap/149900/.

[2] Yuriy Danyk, Chad M. Briggs, “Modern Cognitive Operations and Hybrid Warfare,” *Journal of Strategic Security*, 2023, 16(1), p.40.

[3] Nicolas Mazzucchi, “AI-Based Technologies in Hybrid Conflict: The Future of Influence Operations,” Hybrid CoE Paper 14, June 2022, pp.14-15.

[4] 许华：《乌克兰危机中的美俄混合战：演化、场景与镜鉴》，载《俄罗斯学刊》2022年第4期，第60页。

Aqsa Flood）的军事行动，以色列随即宣布实施报复，新一轮巴以冲突爆发。哈马斯在冲突之始曾凭借灵活多变的战略战术一度取得先机，但是以色列很快利用军事和技术优势夺取了作战主导权，展开对加沙地带的全面进攻。在这次冲突过程中，以色列充分利用人工智能技术开展的智能化“混合战争”发挥了重要作用。

第一，借助人工智能系统，定位哈马斯关键设施。以色列对哈马斯展开反击后，国防军通过无人机和卫星侦察、拦截通信、窃取闭路电视和摄像头监控数据等手段收集海量信息，将其交由“福音”人工智能系统快速自动提取情报，生成与战争局势发展相关的打击目标，包括隧道、军事大院、用作哈马斯高级成员军事指挥中心的住宅、武器仓库、通讯室以及藏有哈马斯资产的建筑等，并且仅在冲突爆发后 10 天内就使用精确制导武器和地堡炸弹（bunker buster）袭击了其中约 5000 个目标[1]，极大削弱了哈马斯的战争潜力，为地面部队进攻加沙地带提供了重要支持。

第二，使用人工智能识别技术，辅助“定点清除”行动。为报复哈马斯的“阿克萨洪水”行动给以色列造成的惨重损失，以军加大了对哈马斯领导层的袭击力度。除哈马斯留在加沙地带的军事领导人物之外，其居住在黎巴嫩、卡塔尔等地的政治领导人物也被列入“定点清除”名单。以色列利用情报机构、卫星、无人机和“飞马”（Pegasus）间谍软件等手段获取大量电子邮件、短信、照片和语音等信息，然后用人工智能系统进行快速识别，并将信息上传到武器系统，完成搜索、识别、猎杀的完整链条。2024 年 1 月，哈马斯旗下抵抗力量卡桑旅在社交媒体发布声明称，以色列在黎巴嫩首都贝鲁特南郊发动的无人机袭击事件造成哈马斯政治局副主席萨利赫·阿鲁里 (Saleh Al-Arouri) 及 2 名卡桑旅指挥官和其他 4 名哈马斯成员共 7 人死亡。在察打一体无人机、AI 人脸识别和语音识别、精确制导武器的加持下，以色列的“定点清除”行动取得大量战果，对哈马斯政治和

[1]《以色列军方：本轮冲突已袭击加沙地带约 5000 个哈马斯目标》，光明网，2023 年 10 月 18 日，https://baijiahao.baidu.com/s?id=1780046695323510306&wfr=spider&for=pc。

军事领导层造成沉重打击。

第三，广泛使用生成式人工智能，争夺舆论主导权。在本次冲突过程中，以色列和哈马斯都十分注重争夺舆论主导权，以占据道德制高点，争取国际舆论支持，而以色列更是着力将人工智能优势运用于舆论战。以色列和西方的主流媒体及支持以色列的自媒体经常使用生成式人工智能创作图片和视频，用视觉化信息指控哈马斯是“恐怖组织”、其所开展的军事行动是“恐怖主义袭击”，并为以军军事行动对加沙平民造成的伤害和人道主义灾难展开辩护。以色列还使用 Sensity AI（主要用于深度伪造检测）、Fictitious.AI（主要用于抄袭检测）等人工智能检测工具识别巴勒斯坦及其同情者所创作的数量庞大的生成式产品，据此大肆指责哈马斯开展虚假宣传，以引导舆论认知，降低哈马斯在社交平台的可信度。

四、智能化“混合战争”对国际安全的影响

智能化“混合战争”加强了武力手段的灵活性，降低了作战成本，提升了战场指挥和反应速度，势必给国际安全带来深刻影响。

（一）物理域：智能化“混合战争”抵消非对称优势

“混合战争”的发起者往往会避免与敌方正面决战，而是采用非常规、非对称手段直击敌方的政治、经济、文化和平民目标。[1] 因此，只要采用适当的战略战术，就能够在“混合战争”中以小博大。比如，2006 年黎巴嫩真主党对以色列的反击就是通过混合使用信息战、游击战等战术，“令以色列输掉了虚拟空间的战斗”[2]，打破了以色列军队在常规战场上的优势。

然而，智能化“混合战争”逐步抵消了技术弱国和非国家行为体的非对称优势。以 2021 年 5 月的巴以冲突为例，以色列首先使用“铁穹”系

[1] Frank G. Hoffman, “Hybrid Warfare and Challenges,” *Joint Forces Quarterly*, 2009(1), p.36.

[2] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid War*, Potomac Institute for Policy Studies, December 2007, pp.38–39.

统拦截了大部分来袭的火箭弹，有效减少了本国损失；之后又通过斩首行动定点清除哈马斯领导人，以减少对平民的误伤，尽量减轻所面临的国内外舆论压力。在这一过程中，人工智能的精准识别能力发挥了极大的作用。在可预见的未来，技术强国可凭借致命性自主武器的隐蔽性和预测目标行动轨迹的精确性，直接威胁对方关键人物的生命安全；也可以通过人工智能检测发现敌方在人员构成、经济结构、组织体系、军事系统、关键基础设施等方面存在的致命漏洞，从而发动直接攻击造成对方瘫痪或者以此相要挟迫使对方屈服。虽然不少弱小国家和非国家行为体也在尝试使用人工智能武器，但却缺少开发前沿技术的资源和人才支持，难以跟上大国、强国的技术发展进度。

在智能化“混合战争”背景下，因为“博伊德循环”（OODA Loop，包括观察 Observation、调整 Orientation、决策 Decision、行动 Actiont 四个步骤）将按照人工智能的速度而非人类判断思维的速度运行，依赖人类决策的指挥系统与复杂的军事等级制度将输给更高效的人机合作系统。技术强国可同时从陆、海、空、天、网、电磁等各个维度发动进攻，让落后国家防不胜防，瞬间失去组织力和战斗力。由于智能化“混合战争”打破了各国间的军事力量平衡，技术强国可以凭借人工智能领域的优势，以较低的成本和人员伤亡，迫使技术弱国和非国家行为体改变自身的利益和安全诉求，从而增强了技术强国实施先发制人打击的收益；而技术弱国因制约技术强国的非对称手段越来越少、非对称优势越来越弱，也增强了对先发制人的依赖性。这些都可能成为威胁国际安全的新的不稳定因素。

（二）信息域：智能化“混合战争”加剧科技优势争夺烈度

由于智能化“混合战争”在信息域中主要表现为算法战和算力战，这使人工智能因素在战争中所发挥的作用不断加强，科技优势争夺战成为各国维护军事优势的重要表现。因此，技术领先国家往往通过提高技术门槛和设置技术壁垒的方式，竭力在算法、芯片等关键领域遏制其他国家的技术突破，以图长期保持本国在智能化“混合战争”中的优势地位。而技术后发国家则

力图打破技术领先国家在算法和算力领域的技术封锁，维护自身安全。

一方面，技术领先国家加大人力、财力和资源投入，在人工智能领域保持科研优势。美国是人工智能技术领先国家的主要代表，为了维护自身技术霸权，一直非常重视科研投入。2019 年 6 月，特朗普政府发布《国家人工智能研究与发展战略计划》（2019 版），明确提出要通过持续的技术发展与创新保持美国在人工智能领域的领导地位[1]；2020 财年，美国人工智能研究项目快速增加到 6000 多个，涉及云计算、自主系统、5G 传输、大数据等多个领域，共投资 48.3 亿美元。[2] 拜登政府时期，美国国土安全部于 2021 年 8 月发布《人工智能 / 机器学习战略计划》，提出要增加研发投资，推动下一代人工智能和机器学习技术用于国家安全保障并构建安全的网络基础设施；2022 年 8 月，拜登签署《2022 年芯片和科学法案》（CHIPS and Science Act 2022），拨款 2800 亿美元用于芯片研发，其中 520 亿美元用于美国半导体生产、2000 亿美元用于芯片相关研究。[3] 总体来看，美国在人工智能前沿研究中占有主导地位，并通过地缘、同盟等传统方式影响欧盟、日本等盟友提出的支持人工智能研发的资助计划，以保持自身领先。作为回应，部分大国在人工智能技术研发方面采取了一系列措施，以保持自身竞争力。俄罗斯政府于 2018 年 3 月发布人工智能 10 点议程，计划建立人工智能和大数据联合会、算法和程序基金、人工智能培训和教育项目、人工智能实验室、人工智能中心等一系列机构[4]；2019 年 10 月，俄罗斯批准了人工智能“路线图”和《2030 年前人工智能发展国家战略》，旨

[1] Select Committee on Artificial Intelligence of The National Science & Technology Council, *The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update*, 2019, p.20.

[2] U.S. Office of the Under Secretary of Defense, *US Department of Defense Fiscal Year 2021 Budget Request Irreversible Implementation of the National Defense Strategy*, 2020, p.15.

[3] *CHIPS and Science Act 2022*, January 3, 2022, p.12.

[4] Samuel Bendett, “Here’s How the Russian Military Is Organizing to Develop AI,” Defense One, June 20, 2018, https://www.defenseone.com/ideas/2018/07/russian-militarys-ai-development-roadmap/149900/.

在加快推进俄罗斯人工智能发展与应用，谋求在人工智能领域的世界领先地位，以确保国家安全、提升经济实力和人民福祉。该战略提出，到2030年，将俄罗斯境内所有采用人工智能技术的超级计算机总算力从2022年的0.073 exaflops（每秒浮点运算百亿亿次）至少提升到1 exaflops，将人工智能技术对国内生产总值的贡献从2022年的2000万亿卢布（约合21.89亿美元）至少提升到11.2万亿卢布（约合1226亿美元）。2023年11月，普京表示，将批准新版俄罗斯人工智能发展战略，该文件将作出一系列重大修改，以扩大生成式人工智能和大型语言模型领域的基础和应用研究，将现有算力至少提高一个数量级，并大力培养人工智能领域的科研人才。[1]

另一方面，技术领先国家设置技术壁垒，将技术问题政治化，以限制其他国家的技术开发路径。2019年10月，美国特朗普政府以8家中国科技公司存在人权问题为由，将其列入实体名单，并对相关中国官员实施签证限制。美国国会还考虑通过立法，阻止美国公司投资那些“不符合人权法规”的从事人工智能开发的中国科技公司，比如中国的商汤科技等[2]，并将人权问题与人工智能绑定，借口打压中国的人工智能技术发展。2020年10月，美国人工智能国家安全委员会（NSCAI）发布年中报告，提出美国应与印度建立战略技术联盟、与欧盟建立新兴技术战略对话，采用联盟方式来促进多边合作，以引领国际人工智能环境建设，并通过美国国务院启动“民主国家数字联盟”的建立进程。[3]美国《2022年芯片和科学法案》规定：接受美国资助的半导体公司，至少在10年内不得同时在中国或其他受关注的国家投资新的28纳米制程以下芯片工厂[4]，意在通过建立技术同盟将其他

[1]《普京：将批准新版俄罗斯人工智能发展战略》，中国新闻网，2023年11月25日，https://www.chinanews.com.cn/gj/2023/11-25/10117699.shtml。

[2] Jon Russell, “China’s Sense Time, the World’s Highest-Valued AI Startup, Closes $620M Follow-on Round,” TechCrunch.com, May 30, 2018, https://techcrunch.com/2018/05/30/even-more-money-for-senstime-ai-china.

[3] National Security Commission on Artificial Intelligence, *2020 Interim Report and Third Quarter Recommendations*, Otctober 2020, pp.33-45.

[4] *CHIPS and Science Act 2022*, January 3, 2022, p.18.

国家排挤出人工智能研发国际合作，特别是阻挠中国6纳米及以下先进制程芯片工艺的发展。

（三）认知域：智能化“混合战争”提升认知战强度

认知战具有隐蔽性好和渗透性强的优势，被施加方很难发现自身意识受到了外部影响，因而不会增加防范与反抗意识。加之人的思想认识和社会舆论对战争进程的影响不断加强，认知战在现代战争中的应用越来越广泛。西方著名军事理论家克劳塞维茨（Carl Von Clausewitz）在《战争论》中曾隐晦地指出，精神要素在战争中具有重要力量，所以战争目标之一就是令对方意志屈服。[1]《孙子兵法》中同样强调“不战而屈人之兵，善之善者也”。2001年，美国国防部在《网络中心战》（Net Centric Warfare）报告中首次引入“认知域”概念，明确强调“认知域决定着很多战斗和战争的胜负”。2020年3月，北约盟军转型司令部发布《作战2040：北约在未来将如何竞争》报告，全面论述了认知战的概念、目标、手段和特征。认知战与“混合战争”既相互联系又各有侧重，实际上前者可视作后者的一个重要领域。“混合战争”因为追求低成本、高效率地达成既定目标，所以较为注重对民众认知偏好的塑造，以破坏对方政府的可信度和合法性，这与认知战分化、瓦解对方意志的战略目标相一致。

认知战中，传统媒体和互联网1.0媒体多以大规模、无差别宣传为主，缺乏认知偏好塑造的精确性，无法做到根据不同对象制定有针对性地宣传策略。人工智能技术进化到深度学习阶段之后，这一问题迎刃而解。首先，在大数据和先进算法的辅助下，可根据用户数据和浏览习惯开展个性化分析。人工智能可以精确定位每个行为个体的喜好、政治倾向、学识、社会关系等基本情况，并预测其未来发展走向，从而有针对性地制定影响行为个体认知的适当策略。某种意义上，人人皆为算法对象，不停地被各种算法所挑选和排斥。算法已不能被简单地视为针对特定任务的解题工具，而

[1] [德] 克劳塞维茨：《战争论》（第一卷），中国人民解放军军事科学院译，北京：商务印书馆1982年版，第188页。

是可被视为一种社会选择工具。[1] 其次，可通过推送定制化信息制造“信息茧房”和“回音室效应”。人工智能可根据每个用户的数据生成用户画像，并以用户画像为基础，通过 X、Facebook、Telegram、TikTok 等社交平台按照用户喜欢的叙事方式推送信息，影响用户感知，营造舆论氛围和热点话题，打造有利的舆论环境，令用户成为信息孤岛，以便塑造其认知偏好。再次，可针对特定用户构建特定认知并反作用于现实政治。人工智能在精准塑造特定用户群体对相关政治、经济或安全议题的认知后，即可引导其行为影响现实世界。比如，2016 年和 2020 年美国大选，都出现了社交媒体通过引导话题流量影响选民倾向的情况；2022 年，西方媒体与俄罗斯媒体围绕乌克兰危机中的“布查惨案”“蛇岛 13 勇士”“扎波罗热核电站遇袭”等话题展开认知战攻防，影响国际社会认知，为自己的军事行动营造舆论支持。此外，ChatGPT 的日渐成熟意味着人工智能还可以利用社交媒体的交互属性，以不同风格的虚拟人物形象与用户直接互动，在潜移默化中改变其认知偏好，这样既能有效吸引用户注意，又可避免单向度宣传引发的逆反心理。2024 年，OpenAI 发布的人工智能文生视频大模型 Sora 的图像视频生成能力达到了以假乱真的程度，造成视频证据真实性和有效性的验证难题，加剧虚假信息的传播。“随着算法和人工智能等技术的普遍应用，社交媒体平台等传播媒介已构建起一种新的传播结构和政治生态图景，由此带来特定认知对现实政治的显著影响。”[2]

智能化“混合战争”的高度信息化特性，极大提升了认知战的效率和准确度。通过大数据和人工智能等技术，可以更好地理解敌方的行动模式、战略意图和认知偏好，从而更精确地开展深度伪造和信息推送。在个人层面，塑造了所谓“去政治化、去地域化、去差异化”的数字身份认同，为引导和塑造认知、瓦解对手社会凝聚力提供了更多的可能；在国家层面，通过

[1] 董青岭、朱玥：《人工智能时代的算法正义与秩序构建》，载《探索与争鸣》2021 年第 3 期，第 83 页。

[2] 蔡翠红：《社交媒体“算法认知战”与公共外交的新特点》，载《人民论坛》2022 年第 13 期，第 22 页。

一整套智力、心理和情感操纵技术侵入复杂的社会认知过程，严重破坏协商政治的社会共识，从而使民众感到困惑和迷失，侵蚀社会信任，影响国家和社会的正常发展进程[1]；在国际体系层面，加剧了主权国家与科技公司之间的规则博弈，以及主权国家之间的意识形态对峙，阻碍全球化进程。

五、智能化“混合战争”的治理路径

智能化“混合战争”对战争形态和国际安全的影响遍及物理域、信息域和认知域，且人工智能技术本身又可军民两用，因而智能化“混合战争”的全球治理必然涉及多学科、多领域、多主体和多议题。这些特征决定了单一治理主体和传统治理方式难以有效应对智能化“混合战争”带来的挑战，而是需要国际社会各方合力，创新治理模式。具体而言，可通过落实三大全球倡议，将涉及智能化“混合战争”的国家和非国家行为体整合起来，根据不同的利益诉求设立若干子机制，扩大各方的利益交汇点，从而保证将智能化“混合战争”纳入全球治理体系，在人类命运共同体框架下推动人工智能技术的良性发展。

（一）构建以全人类共同价值为核心的治理理念

“全球问题的解决，需要建立一种共同参与的治理方式，它应当是一种网络式的……各行为体在网络互动过程中，以妥协、信任、合作为基础，以平行互动来确认共同的目标、方式和途径，实施对公共事务的管理。”[2]因此，通过确立新的价值共识来创新和重建国际机制的理念是变革全球治理体系、维护国际秩序稳定的基础和起点。智能化“混合战争”兼具人工智能的精准高效和“混合战争”的隐蔽模糊，因此强化了世界各国对安全

[1] Maxime Lebrun, “Anticipating Cognitive Intrusions: Framing the Phenomenon,” *Hybrid CoE Strategic Analysis 33*, July 2023, p.6.

[2] 刘清才、张农寿：《非政府组织在全球治理中的角色分析》，载《国际问题研究》2006 第 1 期，第 51 页。

威胁的体验和认知。为了满足自身对安全和权力的追逐，部分大国可能会选择盲目加大对智能化“混合战争”的投入，持续提升技术水平，从而引发新一轮军备竞赛。国际社会应充分利用当前的机遇期，以全球安全倡议、全球发展倡议和全球文明倡议为基础，构建以全人类共同价值[1]为核心的治理理念，并围绕该理念打造一系列应对智能化“混合战争”的国际组织和国际规范。以全人类共同价值为核心的治理理念能够令相关机制具备广泛性、包容性和发展性，在划出战略竞争底线、鼓励国际社会行为体达成军事克制的同时，推动人工智能研究的国际合作和开放共享，通过重大创新和关键核心技术突破为人类文明进步作出积极贡献。2023 年 10 月，习近平主席提出《全球人工智能治理倡议》，主张以人为本、智能向善，在人工智能治理中加强信息交流和技术合作，共同做好风险防范，形成具有广泛共识的人工智能治理框架和标准规范，不断提升人工智能技术的安全性、可靠性、可控性、公平性，这既是上述治理理念的具体体现，更为人工智能发展和国际治理指明了方向。

（二）构建以大国协调为核心的安全协作机制

由于智能化“混合战争”具备抵消非对称优势的潜力，意味着拥有技术优势的行为体更可能在未来的权力分配中占据上风，所以技术先发国家与活跃的科技跨国公司将成为人工智能时代的权力代言人。[2]考虑到技术大国的国际影响力更大、能够调动的资源更多，应以世界主要技术大国为主体，整合其他主权国家以及科技跨国公司、非政府组织等非国家行为体，构建以大国协调为核心的安全协作机制。其中首要的是大国间的对话协商机制，主要功能是增强大国互信，防止将可协商解决的分歧和矛盾误判为“混合战争”爆发的前兆；协调大国技术研发政策，防止出现人工智能军备竞赛；

[1] 全人类共同价值：2015 年 9 月 28 日，习近平主席出席第七十届联合国大会讲话时指出：“和平、发展、公平、正义、民主、自由，是全人类的共同价值，也是联合国的崇高目标。”

[2] Susan Strange, “International Economics and International Relation: A Case of Mutual Neglect,” *International Affairs*, Vol.46, No.2, 1970, p.304.

规范战争行为，防止无限制使用“混合战争”手段。其次是建立大国与中小国家间的技术合作机制，主要用于协助中小国家合理利用人工智能技术的发展成果，以技术进步应对全球性问题，避免中小国家遭遇智能化“混合战争”带来的技术霸凌，实现普遍安全和共同繁荣。再次是建立针对科技跨国公司和非政府组织的规范机制，防止它们无底线的人工智能技术开发以及民用人工智能技术和数据被滥用于“混合战争”，鼓励它们参与国际技术交流与合作，通过技术开放共享破解共同发展难题。

（三）构建以限制性原则为核心的技术规则协议

智能化“混合战争”难以治理的根本原因在于其模糊性。一方面，人工智能技术的军民两用性质导致人工智能武器的边界难以确定。比如，2022年爆发的乌克兰危机中，美国硅谷大数据公司 Palantir Technology 向乌克兰提供的人工智能地图软件 MetaConstellation 系统原本用于自动驾驶系统的开发，中国的理想、蔚来等汽车企业都在使用，而乌军却使用该系统识别战场载具的类型和数量、预测载具行驶轨迹、分析对方补给状况和持续作战能力。另一方面，“混合战争”是否已经发动、在何时何地及以何种方式发动也存在较大争议和模糊性。因此，国际社会有必要通过深度协商，构建限制人工智能技术和智能化“混合战争”无序发展的一系列相关规则，协力推进人工智能治理，避免人工智能等新兴科技在“混合战争”中被滥用。这些相关规则主要包括：明确人工智能武器（致命性自主武器）的定义，防止出现完全自主的致命性武器和战场决策系统，确保人类对人工智能的控制；明确“混合战争”的内涵外延，尽最大可能避免“不宣而战”“隐蔽战争”“非常规战争”（Irregular Warfare）[1] 等“美式霸凌”成为常态，防

[1] 美国国防部将非常规战争（Irregular Warfare）定义为国家和非国家行为体之间为了合法性和对相关人群的影响力而进行的暴力斗争，作战形式包括军事信息保障行动、网络空间行动、网络防御、反金融威胁、军民联合行动、安全合作等。参见“Summary of Irregular Warfare Annex to the National Defense Strategy,” DoD News, October 2, 2020, https://www.defense.gov/News/News-Stories/Article/Article/2369648/irregular-warfare-annex-to-national-defense-strategy-made-public/。

止破坏国家间的政治互信和恶化国际安全形势；强化互联网管理，防止深度伪造的图片、视频等信息在网络中肆意蔓延，并限制 ChatGPT 等生成式人工智能聊天机器人系统成为渗透工具。

出于自身情况、战略定位和发展策略的差异，技术大国、中小国家和非国家行为体针对智能化“混合战争”的态度必然有所不同，所以采用何种方式构建治理机制必然是各方基于国际协商和道德规范博弈的结果。但归根结底，避免人工智能军事化动摇人类对自身命运的掌控是人类社会的共同愿望，应成为未来构建相关国际机制的基石。

结 语

2021 年、2023 年巴以冲突和 2022 年乌克兰危机的进程和特点，可以确定人工智能武器的发展路径并非完全由人工智能技术的特点决定，而是还要受到军事思想和军事理论的影响。所以，人工智能需要在混合战争中承担人力资源替代、精准识别信息和多线程操作三种职能，以赋能者的角色成为决策系统的组成部分。上述变化会导致权力分配进一步向技术强国倾斜，技术强国也会通过设置技术壁垒强化权力优势，并以认知战的方式影响其他国家和非国家行为体。目前，智能化“混合战争”仍处于快速发展和演变之中，国际社会尚未在相关的法律、安全、伦理道德等方面形成共识，尤其是针对智能化“混合战争”潜在威胁的研究还有待深入，形成完善的全球治理机制还需要国际社会长时间的共同努力。

【收稿日期：2024–01–28】
【修回日期：2024–05–27】
（责任编辑：李万胜）