

人工智能时代的国家信息战

——以美俄信息战为例*

杨 楠

【内容提要】 信息战遵循“机制—技术—内容”的战略逻辑，即发起方官僚机构为塑造特定叙事而进行规划筹备，被塑造的信息通过特定传播技术在区域内持续扩散，并通过适配内容对受众群体发挥影响以期取得战略收益。人工智能作为一种颠覆性技术，为国家赋能信息战提供了前提条件，也被各国战略界视为提升规划机构决策质量、扩展战场规模并改变信息传播和生产的方式。竞争与博弈是美国与俄罗斯双边关系的底色，信息战则是双方互动的一种重要表现形式。美俄两国政府均高度重视信息战的重要意义，为此自冷战时期起便致力于构建长效机制、引入新兴技术，并优化宣传策略，以期削弱对方战略优势。随着人工智能技术的发展，美俄依据自身政治体制与科研生态环境特征，继续推动该技术融入信息战各个环节。在即将到来的人工智能时代，全球“信息武器化”态势将持续深化且更加难以治理。面对常态化信息战导致的“后真相时代”，中国应当从政府、社会、传播主体和国际等多个层面做好系统性战略规划，化解相关风险。本文以美俄信息战作为案例，分析人工智能对国家间信息战的影响，有助于深化对人工智能时代大国信息战的理解，确保我国在百年未有之大变局中掌握国际舆论主动、捍卫国家安全并维系社会稳定。

【关键词】 信息战 认知战 人工智能 网络安全 美俄关系

【作者简介】 杨楠，中国社会科学院美国研究所副研究员。

* 本文是国家社科基金青年项目“全球网络空间军事化态势及其治理路径研究”（23CGJ010）的阶段性研究成果，感谢中国社会科学院美国研究所富景筠研究员在本文写作过程中提供的帮助，感谢《俄罗斯东欧中亚研究》编辑部和匿名评审专家的宝贵意见，文中疏漏和不足之处由笔者负责。

信息战（Information Warfare）是指国家通过控制信息或作为信息载体的通信技术以实现相对于对手竞争优势的策略^①。作为一种独特的战争形态与手段，信息战古已有之，并长期占据各国总体安全战略规划的关键地位。通过建构信息环境、塑造国内外叙事或利用操控信息，国家预期在信息战中有针对性地影响对手，甚至改变对手决策，从而获得战略收益^②。随着近年来人工智能技术取得突破，各大国和科技强国逐步推动其服务于信息竞争和对抗，对国家间信息战的形式产生了重大影响。美国和俄罗斯之间围绕舆论叙事展开的竞争自冷战持续至今，是国家间信息战历史的重要组成部分。本文以美俄信息对抗的演进作为案例，探讨人工智能技术如何影响国家间信息战，首先分析人工智能的军事化演进如何对信息战及其背后的信息生态系统产生影响，而后探讨人工智能技术对美俄信息战战略态势的影响，最后研判人工智能时代国家信息战的风险与挑战。

一 人工智能影响国家信息战的路径

国家具有将新兴技术应用于军事领域的偏好和本能，而这些应用本身又持续改变着战争形态^③。正是传播技术发展引发的多轮“信息革命”让信息战这一“旧概念”持续泛化，在其基础上衍生出包括“认知战（Cognitive Warfare）”“政治战（Political Warfare）”“影响力行动（Influence Operation）”以及“灰色区域行动（Grey Zone Operations）”等一系列被广泛讨论的新术语^④。作为当前全

① 目前，中外学者已对信息战的概念进行了系统全面的界定，这一概念聚焦于三个核心特征：（1）一种蓄意的军事或准军事行动；（2）围绕信息和叙事展开的博弈；（3）以获取军事或战略收益为目标。本文对该概念的界定借鉴了上述内容。参见 Dale Minor, *The Information War: How the Government and the Press Manipulate, Censor, and Distort the News*, Hawthorn Books Inc, 1970；赵永华、窦书棋、赵家琦：《观念政治下的网络战：社交媒体时代信息战的观念更迭与范式转换》，载《当代传播》2023年第5期。

② William Hutchinson, Matt Warren, “Principles of Information Warfare”, *Journal of Information Warfare*, Vol. 1, No. 1, 2001.

③ Frank Barnaby, Marlies ter Borg, eds., *Emerging Technologies and Military Doctrine: A Political Assessment*, Palgrave Macmillan, 1986.

④ 这些概念与信息战既有联系又存在诸多不同。广义上讲，上述概念均强调在低于物理域门槛之下诉诸行动，这些行动不仅能够规避国内法律监管，同时也处于国际法律规制并未触及的区域内；狭义上讲，信息战仅通过塑造信息内容并借助各类传播技术来实现战略目标，具有自身的复杂性和独特性。

球第四次工业革命的核心技术，人工智能的发展突破及其军事化态势同样为信息战形态的演进提供了物质基础。

（一）信息战的战略逻辑

国家间围绕信息与叙事展开的博弈与军事史一样古老。时至今日，各类信息战仍遵循“三军可夺气，将军可夺心”及“冷静地制造假象”的总体目标^①。作为一组实践先行于理论的概念，各国军方或学术界在后冷战时期对信息战的界定始终较为宽泛，为新兴技术对战争形态的塑造和改变预留了解释空间。信息战研究侧重大致分为三个阶段。冷战结束初期，学界基于美苏对抗历史意识到信息优势与战略优势之间的关联，开始提及“战略信息战”概念；美国智库兰德公司应美国国防部请求对信息战概念的内涵与外延进行系统分析后，指出这种战争模式“几乎涉及现代国家安全建构的任何一个方面”，“将成为冷战后国家间冲突的首要模式”^②。随着全球化程度的加深和 2001 年“9·11”事件的爆发，包括恐怖组织在内的各类非国家行为体逐渐成为战略性信息操控的发起者；各国开始意识到并着重强调信息战的非对称性，聚焦“信息恐怖主义”为国际安全带来的系统性风险^③。2010 年以来，网络信息技术的发展促进全球互联网用户数量以年均 9% 的增长率扩展，随之带来的网络与在线话语交流机制也极大地延展了信息战的理论内涵。信息战与网络战相关研究开始交汇，基于网络空间的信息战成为各国研究人员关注的重点。在美国学者马丁·利比奇看来，与信息战在 20 世纪 90 年代初首次作为一个概念被提出时相比，技术的进步让网络时代的信息战不再单纯作为“动能军事行动”（Kinetic Military Operations）的补充，而是一种更为宏观的战略规划^④。

信息战的基础逻辑与宣传、欺骗和颠覆等基本概念紧密相连^⑤，是国家秘密军

① Roger Boesche, “Kautilya’s Arthashastra on War and Diplomacy in Ancient India”, *The Journal of Military History*, Vol. 67, No. 1, 2003.

② Roger Molander, Andrew Riddile, Peter Wilson, *Strategic Information Warfare: A New Face of War*, RAND Publisher, 1996, p. xxi.

③ Ken Webb, “Information Terrorism in the New Security Environment”, *Journal of Information Warfare*, Vol. 6, No. 2, 2007.

④ Martin Libicki, “The Convergence of Information Warfare”, in Christopher Whyte, Trevor Thrall, Brian Mazanec eds., *Information Warfare in the Age of Cyber Conflict*, Routledge, 2021, p. 15.

⑤ Catherine Theohary, “Information Warfare: Issues for Congress”. <https://sgp.fas.org/crs/natsec/R45142.pdf>, 访问日期：2024 年 4 月 20 日。

事或情报行动的重要组成部分，这也决定了信息战低成本、非致命性和持久性的特征。另一方面，信息战的作战方式随时间推移，始终处于变动之中，是特定时间段内国家政策重点、传播能力与信息环境的集中体现。大国在信息战场上的交锋对抗是主动且持续的，其中国际形势的演进或变动决定了信息战的频率，传播技术的发展与突破决定了信息战的烈度，而对信息的处理和应用则决定了信息战的质量。从这个角度看，尽管信息战始终是最廉价、最简单且限制最少的战争类型之一，但国家却需要通过复杂的政策规划和评估，并对各类战略工具进行审慎权衡，才能取得预期收益。

科技演进与国际形势变化为国家开展信息战提供了多种路径，但其基本逻辑框架始终遵循信息传导的客观规律。首先，信息战发起者为塑造特定叙事而进行规划筹备，并作出对应的战术选择。对国家而言，这一进程往往由特定官僚机构承担。尽管信息战本质上是一种军事行动，但军事部门并非其唯一发起者；作为战略情报提供者的情报机构以及负责公共外交或对外宣传的组织机构在塑造叙事方面同样承担重要责任。随着私营部门在数字时代获得更多权力，政府对信息战的垄断地位也逐渐被打破^①。

其次，被塑造的信息以特定方式在目标区域内持续扩散，以改变受众预期并影响对方决策。其中，传播技术决定了信息扩散的速度与广度。信息战发展史上机制与路径的历次重大变革均由传播科技革命带动。两次世界大战期间，交战方之间围绕宣传的博弈主要基于传统纸质媒介展开，并通过故事、谣言、报道、图片以及其他社会传播形式来塑造信息、控制意见^②。冷战期间，无线电技术的普及引发信息战的改革，美苏两大阵营在维系原有信息战能力的基础上，借助美国之音、莫斯科广播电台以及自由欧洲电台等平台，就意识形态问题系统拓展政治宣传活动，相互争夺“叙事优势”^③。冷战末期至今，国家通过计算机、互联网与卫星等科技再度强化了信息战中的传播力，间接造成当前错误信息与虚假信息泛滥的“信息污染”（Information Pollution）环境，这是信息革命带来的最大的不

① David Gompert, “Right Makes Might: Freedom and Power in the Information Age”, in Christopher Whyte, Trevor Thrall, Brian Mazanec eds., *Information Warfare in the Age of Cyber Conflict*, Routledge, 2021, p. 60.

② 〔美〕哈罗德·拉斯韦尔：《世界大战中的宣传技巧》，张洁、田青译，中国人民大学出版社2003年版，第159页。

③ Mark Winek, “Radio as a Tool of the State: Radio Moscow and the Early Cold War”, *Comparative Humanities Review*, Vol. 3, No. 9, 2009.

利影响^①，而受众对信息真实性与有效性的甄别能力也被持续削弱。

最后，被塑造的信息经扩散后对目标发挥预期影响，并获得战略收益。传递的信息与受众群体之间的适配性成为信息战能否奏效的关键；信息内容的质量越高，其可信性与说服力就越强，反之亦然。该步骤被视为所谓“信息战杀伤链”（Information Warfare Kill Chain）的最关键一环^②。在现实中，大部分信息战的发起者将主要精力与资源投入到提升内容与目标之间的适配度上。冷战时期，美国政府为实现该目标而在社会主义国家开展“青年领袖项目”（Youth Program），在识别具体目标后进行针对性的信息宣传与影响^③。20 世纪末期互联网与在线社交平台兴起后，创建虚假媒体信息的成本持续降低，低质量信息的线上扩散更凸显内容在信息战中的重要性。

作为信息战“机构—技术—内容”逻辑框架的关键一环，传播科技的历次演进均能为信息战革命提供基础。另一方面，国家机构对有关科技的认识，以及有关科技如何赋能信息内容，同样是信息战能否奏效的关键。

（二）人工智能技术革命及其军事化态势

人工智能技术在近年来的迅猛发展深刻改变了人类社会的生产生活方式。借助机器学习、深度学习或神经网络等算法，人工智能在图像识别、语言处理及自主决策等领域发挥的作用逐步增强。2023 年至 2024 年初，美国开放人工智能研究中心（OpenAI）先后发布语言模型 GPT-4 与文本转视频模型 Sora，标志着人工智能技术进入新一轮技术突破期。另一方面，与网络安全领域的境遇相似，国际社会对人工智能的相关技术监管与法律规制同样远落后于科技演进本身，现有多边治理框架亦不具备普遍的影响力，并衍生出一系列人工智能应用中的法律、伦理和道德问题。

人工智能的“技术—治理错位”为国家利用该技术提升军事能力、维护国家安全提供了动力。全球军事大国在近年来竞相推动人工智能技术融入军事安全

① Cai Kaiyuan, Zhang Chaoyang, “Towards a Research on Information Pollution”, *IEEE International Conference on Systems, Man and Cybernetics*, 1996, p. 3124.

② Christopher Whyte, Ugochukwu Etudo, “Cyber by a Different Logic: Using an Information Warfare Kill Chain to Understand Cyber-enabled Influence Operations”, in Christopher Whyte, Trevor Thrall, Brian Mazanec eds., *Information Warfare in the Age of Cyber Conflict*, Routledge, 2021, pp. 120-121.

③ Joël Kotek, “Youth Organizations as a Battlefield in the Cold War”, *Intelligence and National Security*, Vol. 18, No. 2, 2003.

领域，并将其视为下一轮全球国防竞争与军备竞赛的优先事项^①。作为一项颠覆性技术，人工智能的军事化态势将从四个方面改变战争形态。一是提升决策质量。人工智能暂无法在战争中替代人类进行决策，但能够通过融合战场各方面大量数据来辅助决策，弥补人类因认知不足导致的固有缺陷^②。二是提高作战速度。人工智能可以通过强大的算力加快处理各类信息，减少人类劳动的时间消耗，为决策者预留更多研判空间。三是增加伪装性。狭义人工智能及其机器学习能够通过对图像、文本和声音的研判和模仿，以不引发怀疑的具体方式与对手进行互动，驱散“战争迷雾”也因此变得更为困难。四是降低成本。相比核武器或传统动能武器的高研发制造门槛，人工智能技术具有数字时代各类新兴技术的低门槛、易获取等特征，令小国甚至非国家行为体在理论上具备参与战略竞争的资格。

数字数据作为驱动人工智能的核心要素，近年来成为国家争夺的战略资源^③。此前，科技公司等私营部门是个人数据与信息的主要获取者与保有者，它们采用专门定制的算法来预测和影响个人行为从而获利。这种被称为“监控资本主义（Surveillance Capitalism）”的数据获取与使用方法开始被引入军事领域；各国国家安全相关机构竞相争夺高质量、大规模的数据并确保其安全性，从而为人工智能军事化应用提供基础^④。其中，国家的政权类型与治理结构将决定“监控资本主义”的落实程度。

（三）人工智能如何塑造国家信息战

人工智能及其军事化进程同时对信息战的战略和战术产生重要影响；相关技术均可以增强信息战的行动速度、影响广度以及战略效度的预期，导致人工智能时代的信息战更具侵略性和破坏力。

^① John Hurley, “Enabling Successful Artificial Intelligence Implementation in the Department of Defense”, *Journal of Information Warfare*, Vol. 17, No. 2, 2018.

^② Avi Goldfarb, Jon Lindsay, “Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War”, *International Security*, Vol. 46, No. 3, 2021.

^③ Jeffery Ding, Allan Dafoe, “The Logic of Strategic Assets: From Oil to AI”, *Security Studies*, Vol. 30, No. 2, 2021.

^④ Lance Hunter, Craig Albert, Josh Rutland, Kristen Topping, Christopher Hennigan, “Artificial Intelligence and Information Warfare in Major Power States: How the US, China, and Russia are Using Artificial Intelligence in their Information Warfare and Influence Operations”, *Defense and Security Analysis*, Vol. 40, No. 1, 2024.

人工智能技术将提升国家信息战规划机构的决策质量。一方面，国家内部信息战发起者的多样性将不可避免地引发机构间壁垒以及资源调配的不均衡，而人工智能技术的引入能够有效化解人类因“自由裁量权”而带来的官僚主义损耗^①。人工智能有助于推动战争权力迈向韦伯提出的“理想式政府秩序”，即对权力的明确分配、委托、界定与等级化^②。在此基础上，各部门的具体职能将得以明晰，进而推动各类战略工具融合贯通。另一方面，通过自然语言处理、深度挖掘和机器学习等人工智能技术，情报机构能够发现隐藏的模式和关联，在大数据“噪音”中寻找所需“信号”的能力得以提升，从而更好地为决策者规划信息战提供支持。

人工智能技术将扩展信息战的“战场规模”；其中“个性化”与“定向传播”是人工智能重构传播生态的重要起点，网络空间则成为其发挥作用的主要平台。在基于内容推荐系统、协同过滤推荐系统以及基于知识推荐系统等不同算法下，规模性的信息传播与内容分发能够在极短时间内得以完成，覆盖更广泛的受众群体与对应平台^③。与此同时，这种传播模式也不再如以往呈现单向性特征；通过捕捉用户行为习惯、搜集用户反馈数据，信息战发起者能够及时调整信息的呈现方式，甚至与受众建立持续的社交关系。这种模式可以弥合传统媒介与公众之间的“偏好差异”^④，持续扩大传播的覆盖面和影响力。

人工智能改变了信息的传播和产生方式，对信息内容的影响持续而深远。“内容真实性”是传递的信息与受众群体之间能否适配的关键。2010 年以来，生成式人工智能被多国战略性地应用于社交媒体操纵活动，以期提升内容的真实性。兰德公司在其 2023 年发布的报告中，将国家利用人工智能塑造内容以实现战略目标的历史发展分为三个阶段。早期低质量的程序机器人和虚假账户虽然可产生大量文本，但内容粗糙且缺乏与用户的互动。而随着技术突破，人工智能开

① Justin Bullock, “Artificial Intelligence, Discretion, and Bureaucracy”, *The American Review of Public Administration*, Vol. 49, No. 7, 2019.

② Rodgigo Presuel, Jose Sierra, “The Adoption of Artificial Intelligence in Bureaucratic Decision – making: A Weberian Perspective”, *Digital Government: Research and Practice*, Vol. 5, No. 1, 2024.

③ 新华社：《2019 年度“人工智能时代媒体变革与发展”研究报告》，2020 年 2 月，第 17 页。

④ 有关人工智能技术如何弱化“偏好差异”，参考 Pablo Boczkowski, Eugenia Mitchelstein, *The News Gap: When the Information Preferences of the Media and the Public Diverge*, MIT Press, 2013.

始具有抓取互联网内容并深度加工的能力，通过“深度伪造”而形成的音频、图像或视频开始出现，但仍可以通过各类技术予以侦测。当前，基于人工智能的信息操纵迈入了所谓“3.0时代”，真实内容与合成内容之间的界限被进一步模糊，模型也具有一定的自主决策能力，且在内容交付后极易引发受众共鸣^①。随着技术的成熟，生成式人工智能对国家反虚假信息的检测能力与政策部署提出了越来越高的要求，信息竞争也逐步具有“易攻难守”的特点。

二 人工智能与美俄信息战

历史上，同为地缘政治大国的美国与俄罗斯均将对外宣传作为实现战略目标的重要工具。第二次世界大战期间，两国大规模运用宣传工具，并分别建立了专门负责进行对外话语博弈的机构，政府控制公众舆论成为大规模战争的必然结果。随着美苏关系在二战末期由合作转为竞争，两国之间旷日持久的信息战也随之开启。而相比冷战时期聚焦传统媒介的话语博弈，数字时代美俄两国的信息对抗转战至网络空间。这也为人工智能介入国家间信息战提供了关键契机。

（一）美俄信息战的数字基础

冷战末期至21世纪初期，军用互联网的商业化和民用化进程加速，电子商务开始兴起。与之相对应的是网络安全问题日益突出；黑客行为、网络犯罪以及网络空间军事化态势成为各国关注的焦点，国际社会迈入网络冲突时代。俄罗斯独立之初，两国信息化发展程度具有较大的差异。美国国内网络基础设施推进迅猛，互联网普及率持续上升；俄罗斯则处于网络信息化的初级阶段，在苏联时期为数不多的局域网的“废墟”上重新推动全国计算机网络建设^②。随着美俄关系在20世纪90年代末期由热转冷，网络空间成为双方地缘政治博弈的延伸，两国在后冷战时期一度停止的信息对抗亦死灰复燃并逐步扩大。为获取相对于另一方的信息优势，美俄两国根据自身国情搭建了对外舆论攻势的战略传导机制（如表1所示）；其中双方在信息战的机制搭建、技术使用与受众策略等方面均遵循着不同的逻辑。

^① William Marcellino, Nathan Beauchamp – Mustafaga, Amanda Kerrigan, Lev Navarre Chao, Jackson Smith, *The Rise of Generative AI and the Coming Era of Social Media Manipulation 3.0*, Rand Corporation, 2023, p. 3.

^② 杨楠：《美俄关系中的网络安全问题》，载《太平洋学报》2022年第6期。

表 1 数字时代美俄的信息战传导机制

	美国	俄罗斯
机制	由下至上的 公私合作模式	由上至下的 国家主导模式
技术	关键基础设施	互联网信息
内容	建构主流叙事	分化目标受众

资料来源：作者自制。

冷战时期，在决策机构和国家安全机制的战略部署下，美苏两国制定并推广了系统性的信息战战略，且逻辑高度相似，即通过各类方式宣扬自身，质疑并攻击对方，同时对处于“中间地带”的国家进行说服、影响和拉拢。与冷战时期高度类似的战略逻辑相比，美俄在数字时代的信息战侧重开始出现差异。两国对网络空间的不同认知是造成这种差异的根源，即网络安全概念是否应当包含信息和心理层面，以及政府在应对网络冲突时应当扮演何种角色。1999 年克林顿政府在其发布的《新世纪国家安全战略》中首次提到“网络安全”（Cybersecurity）概念。此后，美国政府在推进相关政策进程的大部分时间里将网络空间和信息空间视为两个不同但密切相关的领域：前者被广泛建构为由电子基础设施、互联网、通信系统以及数字数据所构成的集合体，对其管理和保护属于传统军事安全机构责任范畴；后者则意指包括网络传播在内的各类信息传播渠道，是以国务院为代表的各类外交事务相关机构的重要行动领域^①。对网络与信息概念的区分界定模糊了信息战的作战权责。一方面，21 世纪初美国各军种在多份官方文件中提到的所谓“信息战”概念更多侧重于为通过计算机信息网络对基础设施展开攻防“创造和利用信息优势”^②，从而应对可能发生的“网络珍珠港”和“网络九一一”等情景。另一方面，美国政府在互联网发展的早期阶段就形成了强调网络空间开放性、自由和创新的基本治理原则，并将网络空间形成的公共区域视为一种战略资源。在美国海军战争学院研究员龚培德看来，美国政府坚持“互联网自由”原则的背后，是其坚信这种模式有助于尚在享受“单极时刻”红利的美

^① “A National Security Strategy for A New Century”. <https://clintonwhitehouse3.archives.gov/WH/EOP/NSC/Strategy/>, 访问时间：2024 年 4 月 20 日。

^② 例如 U. S. Joint Chiefs of Staff, “Joint Vision 2010”. <https://apps.dtic.mil/sti/tr/pdf/ADA402777.pdf>, 访问时间：2024 年 4 月 20 日。

国最大程度传播其自由主义价值观^①。基于这种逻辑，2009 年成立的美国网络司令部（United States Cyber Command）最初并未将信息内容对抗作为自身的主要职能，信息战仍由美国国务院和中央情报局等机构负责。后者倾向于通过公开或秘密外交等方式对俄施压，同时策动媒体与数字企业等私营部门承包商策应其对俄宣传。

俄罗斯政府在推广互联网初期所建构的“信息空间”概念无论在内涵还是外延方面均与美国存在较大差异。1997 年，尚与美国处于“蜜月期”的俄罗斯在其推出的首份《俄联邦国家安全构想》中就提到信息在该国国家安全领域中的关键地位，着重强调“在信息的自由交换和对其传播的限制之间建立必要的平衡”，以及利用信息技术来增强俄罗斯民族价值观以及社会精神发展的基本逻辑^②。自此，俄罗斯开始使用、推广有别于“网络空间”的“信息安全”（информационная безопасность）理念。在 2000 年推出的《信息安全学说》中，俄罗斯首次将“信息安全”写入到官方正式文件中，并将其界定为能够对个体和公共意识产生影响的领域。文件指出，俄罗斯面临来自一系列国家的信息战威胁，为此需要“防止非法信息造成的心理影响侵害大众意识”^③。可以看出，俄罗斯政府从一开始就将信息安全视为由网络空间形成的“人工信息安全”与人类精神层面的“自然信息安全”的集合^④。从意识形态上看，俄罗斯战略界认为来自西方的自由主义在持续冲击和挑战俄罗斯主权，并坚信中亚和东欧频发的“颜色革命”、波罗的海国家的反俄浪潮以及国内发生的抗议活动等均源自美国主导的信息战冲

① David Gompert, “Right Makes Might: Freedom and Power in the Information Age”, in Christopher Whyte, Trevor Thrall, Brian Mazanec eds., *Information Warfare in the Age of Cyber Conflict*, Routledge, 2021, p. 45.

② “Russian National Security Blueprint”. <https://nuke.fas.org/guide/russia/doctrine/blueprint.html>, 访问时间：2024 年 4 月 20 日。

③ “Information Security Doctrine of the Russian Federation”. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf, 访问时间：2024 年 4 月 20 日。

④ Conor Cunningham, “A Russian Federation Information Warfare Primer”. https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/#_ftnref1, 访问时间：2024 年 4 月 20 日。

击；俄罗斯也因此处于一场永久的冲突中^①。基于这种广泛共识，俄罗斯延续由上至下的战略部署，形成了由联邦政府和国防部主导，以联邦安全局和总参谋部情报总局为主要推动部门的等级制信息战组织链条。

互联网是网络冲突时代的“底层科技”；数据及其形成的信息经过聚合与处理后经由网络传递，形成了新的信息环境。信息战作战场域转移至网络空间，成为 21 世纪以来网络战的关键组成部分。相比冷战时期，网络冲突时代的信息战技术具有自身的独特性。美俄两国对于网络空间的认知差异导致其将战略重心置于不同的科技发展路径。一方面，以美国战略司令部和国家安全局为代表的军方从“战略威慑”逻辑出发，致力于开发能够瘫痪对方电力系统、金融系统和其他关键基础设施的网络武器。2012 年被曝光的“奥林匹克行动”及造成伊朗核设施大规模损毁的“震网病毒”（Stuxnet）正是这种战略下的产物，这些武器部署复杂、耗资巨大，引发了全球各国的担忧与负面反应，但所获得的威慑效果却相对有限^②。另一方面，美国国务院和中央情报局等机构在策动“颜色革命”期间，同样从技术本身出发为目标地区提供促进信息流动的 TOR 技术或社交软件，并在此基础上对信息内容进行加工重塑^③。

俄罗斯对“网络空间”更为系统化的认识为该国在网络冲突时代积极利用各类新兴技术弥补自身劣势提供了动力。网络冲突时代的战略工具无需高昂的开发经费，且因网络空间的扩散性而极易获取。这种特点为俄罗斯提供了一种不对称优势，弥补了与美国在传播领域的技术鸿沟，令其迅速具备了与美国类似的影响力和进攻性。联合国调查报告显示，2008 年俄格战争期间，俄方同时针对美国与西方发动了大规模信息战。通过在主要互联网新闻门户网站上指控格鲁吉亚种族清洗暴行、批判西方国家散布偏见和虚假信息，俄罗斯成功将格鲁吉亚塑造为侵略者，并

① Media Ajir, Bethany Vaillant, “Russian Information Warfare: Implications for Deterrence Theory”, *Strategic Studies Quarterly*, Vol. 12, No. 3, 2018.

② Jon Lidsay, “Stuxnet and the Limits of Cyber Warfare”, *Security Studies*, Vol. 22, No. 3, 2013.

③ 中国国家计算机病毒应急处理中心、360 数字安全公司：《“黑客帝国”调查报告——美国中央情报局（CIA）》，<https://360.net/about/news/article6455f555aea2dd002ac30aa8>，访问时间：2024 年 4 月 20 日。

吸引包括《卫报》在内一系列西方主流媒体进行反美亲俄的报道^①。

美俄两国对网络空间认知的差异同样影响了双方信息战的内容塑造。对美国而言，冷战的结束意味着自身所代表的意识形态与价值观的胜利。在一些学者看来，这种思想上的“主体稳定性”（Subjectivity Stability）为美国带来了某种程度上的“道义霸权”。这种优势不仅令美国重新强调军事行动中的非物质文化因素，同时也为与“主流舆论”观念不同的主体施加压力^②。例如，美国将自身在“9·11”事件后的反恐战争描述为打击不道德和非法恐怖分子的合法行动以“诱使”其他国家支持反恐战争；选择与美国背道而驰的国家则会承受来自国际社会的各类压力。这种现实令美国能够以较小成本推广自身价值观念，而不必考虑这些观念与受众之间的适配度。反观俄罗斯，由于仍沿用与冷战时期类似的信息战命令链条，加之高度重视文化要素的战略意义，该国在进入网络冲突时代后便着力于信息战中叙事及内容等方面的塑造。在冷战时期，由于美国新闻机构在向公众提供信息方面占据主导地位，苏联很难直接对美国民众发动大规模信息运动。而互联网社交媒体的兴起打破了这些机构的新闻垄断权，让俄罗斯能够直面美国社会受众。2013 年中期，俄罗斯成立名为“互联网研究机构（тролли）”的公司，其主要职能即“加工信息内容”并代表俄罗斯从事宣传和影响力行动，被西方世界称为俄罗斯的“喷子农场”（Troll Farm）^③。然而，由于技术限制，这一时期由人力或低质量程序机器人进行的在线文本输出具有明显的虚假性，也让俄罗斯难以取得相对于美国的明显信息优势。

（二）人工智能与美俄信息战

网络空间的延展让社交网络与电子商务成为人类生活的一部分，该过程催生的大量数据同时也加速了人工智能的创新研究。2010 年后，随着大数据、云计

^① United Nations Human Rights Committee, “Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant”. https://www.echr.coe.int/documents/d/echr/HUDOC_38263_08_Annexes_ENG, 访问时间：2024 年 4 月 20 日。

^② 例如 Isabelle Grunberg, “Exploring the ‘Myth’ of Hegemonic Stability”, *International Organization*, Vol. 44, No. 4, 1990; Ty Solomon, *The Politics of Subjectivity in American Foreign Policy Discourses*, University of Michigan Press, 2015。

^③ Renee DiResta et al., “The Tactics & Tropes of the Internet Research Agency”. <https://int.nyt.com/data/documenthelper/533-read-report-internet-research-agency/7871ea6d5b7bedafbf19/optimized/full.pdf>, 访问时间：2024 年 4 月 20 日。

算、互联网、物联网等技术的发展，人工智能科技开始跨越科学与应用之间的技术鸿沟，实现了从“不能用、不好用”到“可以用”的技术突破^①；国际社会开始迈向人工智能时代。与此同时，人工智能在国家安全和军事领域的颠覆性潜力迅速推动了该技术的武器化进程，美俄之间持续的信息战借此出现了新的变量。

尽管美国在网络冲突时代投入大量国家资源，强化自身军事威慑能力，但它并未因此变得更加安全。不仅全美关键基础设施长期成为全球黑客集中攻击的对象，其秉持的“网络自由”理念也受到广泛质疑及挑战。在这种情况下，美国开始调整自身在网络空间的战略姿态，将信息内容作为一个重要方面纳入其中，并主动尝试利用自身在人工智能领域的优势地位赋能战略转型。2012 年美参谋长联席会议发布名为《信息作战》的条令，首次将由人类思维构成的“信息环境”纳入作战范围^②。2018 年美国陆军发布的《信息作战运作规范》首次公开承认信息战可以作为武器影响对象国，并将获取“信息优势和决策优势”（IA&DD）确立为作战目标^③。这一目标推动美国政府加速相关官僚机制的构建。美国国防部于 2018 年成立了联合人工智能中心，2022 年将其并入国防部首席数字与人工智能办公室。主要负责外交与信息传播的美国国务院也意识到此前的战略失误，在公开文件中承认“全球竞争不仅需要生产、使用或储存数据，还需要将数据作为战略资产来使用”^④。与之对应，国务院将此前用于打击恐怖主义宣传的全球融合中心（Global Engagement Center）转型为专门负责应对大国信息对抗的机构，识别“深度伪造”技术是其工作重心之一。

美国战略界承认信息战中技术和内容具有同等重要性，并将这种主要在网络空间开展的作战与“情报竞赛”（Intelligence Contest）逻辑相关联^⑤。与此同时，

① 谭铁牛：《人工智能的历史、现状与未来》，载《求是》2019 年第 4 期。

② U. S. Joint Chief of Staff, “Joint Publication 3 - 13: Information Operations”. https://irp.fas.org/doddir/dod/jp3_13.pdf, 访问时间：2024 年 4 月 20 日。

③ U. S. Department of the Army, “The Conduct of Information Operations”. <https://irp.fas.org/doddir/army/atp3-13-1.pdf>, 访问时间：2024 年 4 月 20 日。

④ U. S. Department of State, “Enterprise Data Strategy: Empowering Data Informed Diplomacy”. <https://www.state.gov/wp-content/uploads/2021/09/Reference-EDS-Accessible.pdf>, 访问时间：2024 年 4 月 20 日。

⑤ Robert Chesney, Max Smeets, “Policy Roundtable: Cyber Conflict as an Intelligence Contest”. <https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/>, 访问时间：2024 年 4 月 20 日。

步入人工智能时代后，美国成为尖端技术的引领者，也具有将人工智能技术军事化以赋能自身信息战的实力。不过，当前美国国内政治态势在某种程度上限制了该国将技术优势有效转化为战略优势。美国国内长期存在着以追求政治稳定和国家安全为目标的“国家安全派”、以确保美国民众数字隐私不受国家安全部门侵蚀为目标的“数据隐私派”，以及以确保经济收益最大化为目标的“经贸利益派”。这三股力量在美国政府、国会与民间进行持续不断的博弈与制衡，限制了美国在军事安全领域引入新兴技术的尝试。前国家安全局雇佣人员爱德华·斯诺登于2013年曝光美国政府大规模监控行动“棱镜门”事件，叠加美国国内政治极化态势加剧，显示上述三方博弈态势愈演愈烈。作为美国当代隐蔽行动法律基石的《对外情报监控法》第702条争取美国国会重新授权的过程异常艰难，正是这种情势的集中写照^①。在此背景下，美国以人工智能技术强化信息战能力的尝试面临一定程度的阻碍，迫使美国官方长期以“事实核查”（Fact-checks）等官方主导的方式应对外部威胁^②。

受制于政治体制、经济状况与科技能力的掣肘，步入人工智能时代后，俄罗斯并未在相关尖端技术研发方面取得突破，在推动人工智能技术融入军事领域方面同样不及美国。但在俄罗斯人工智能科技治理体系逻辑影响下，该国对于“人工智能技术如何影响信息战”具有更为深刻的理解，亦能够更加有效地实现从技术到战略的转化。2010年以来，俄罗斯逐渐形成了由储蓄银行主导的民用人工智能治理体系和以俄罗斯国防部“先期研究基金会（Фонд перспективных исследований）”主导的军事人工智能科技研发投入体系，两者均隶属俄联邦政府统一领导且彼此平行。这种治理体系背后，是俄罗斯希望“采用非市场化模式，将有限资源集中于少数特定领域”，从而以局部技术突破来推进非对称竞争优势的基本逻辑^③。信息战作为俄罗斯在“灰色区域”内实现非对称优势的关键领域，自然成为人工智能技术布局的重点。

① Preston Marquis, “FISA Section 702 Reauthorized for Two Years”. <https://www.lawfaremedia.org/article/fisa-section-702-reauthorized-for-two-years>, 访问时间：2024年4月30日。

② U. S. Department of State, Global Engagement Center, “Disarming Disinformation: Our Shared Responsibility”. <https://www.state.gov/disarming-disinformation/>, 访问时间：2024年4月20日。

③ 有关俄罗斯人工智能治理路径的系统性分析，参见封帅：《建构非对称竞争优势的尝试：俄罗斯人工智能治理体系的结构与逻辑解析》，载《俄罗斯学刊》2022年第2期。

在战术方面，俄罗斯的政治体制能够令相关部门有效搜集发动信息战的必要数据，而无需考虑数据隐私或数字伦理的掣肘。2014 年俄交通部要求全国电信运营商安装第三代“侦查活动措施体系”（Система оперативно – разыскных мероприятий）合规设备，允许俄联邦安全局监控和远程访问对象服务器^①。2016 年俄罗斯颁布“亚罗瓦娅法”（Закон Яровой），要求该国电信服务商和社交媒体平台将用户数据存储期延至三年，同时允许联邦安全局访问相关内容。此类措施能够为俄罗斯相关部门提供大量元数据，以服务于信息战战略中人工智能技术的研发。美国智库研究显示，自 2014 年以来，“互联网研究机构”的工作机制明显呈现由“人工主导”转为“由人工智能驱动”的过渡趋势，并对社交媒体的信息生态环境产生了深远影响^②。一方面，生成式人工智能能够通过构建愈加逼真的虚假信息或视频实现伪旗（False Flag）等战略欺骗活动。美国指责俄罗斯在 2014 年克里米亚危机和 2022 年俄乌冲突前夕采取了相应的战术^③。另一方面，经过训练的程序化机器人根据受众特征来分发对应内容，以固化特定群体的思维并制造对立分裂。美国针对俄罗斯干涉 2016 年美国总统大选的指控中就包括了诸多相关内容^④。

在人工智能技术赋能下，俄罗斯在信息战中的叙事能力进一步提升。在美国研究人员看来，俄方能够在有效实现信息去政治化的基础上，从不同叙事角度对同样内容进行加工，并借助人工智能在社交网络平台上实现具有针对性的消息分发，从而在美国社会内部或美国和盟友之间“打入楔子”^⑤。相比之下，美国政

① Adam Satariano, Paul Mozur, Aaron Krolik, “When Nokia Pulled Out of Russia, a Vast Surveillance System Remained”. <https://www.nytimes.com/2022/03/28/technology/nokia-russia-surveillance-system-sorm.html>, 访问时间：2024 年 4 月 20 日。

② Renee DiResta et al., “The Tactics & Tropes of the Internet Research Agency”. <https://int.nyt.com/data/documenthelper/533-read-report-internet-research-agency/7871ea6d5b7bedafbf19/optimized/full.pdf>, 访问时间：2024 年 4 月 20 日。

③ U. S. Embassy and Consulates in the United Kingdom, “How Russia Conducts False Flag Operations”. <https://uk.usembassy.gov/how-russia-conducts-false-flag-operations/>, 访问时间：2024 年 4 月 20 日。

④ U. S. Department of Justice, “Report on the Investigation into Russian Interference in the 2016 Presidential Election: Volume I of II”.

⑤ James Lamond, “The Origins of Russia’s Broad Political Assault on the United States”. <https://www.americanprogress.org/wp-content/uploads/sites/2/2018/10/RussianInterference-report1.pdf>, 访问时间：2024 年 4 月 20 日。

府仍旧倾向于通过官方渠道宣扬自身立场，无差别输出意识形态。这种策略在美国掌握道义及科技优势的冷战时期，以及美国仍占据全球霸权地位的网络冲突时期尚可发挥效用。但随着美国陷入对外战争泥潭，其在国际社会的影响力与公信力同时下降，这种策略也不再行之有效。2016 年美情报部门指责俄罗斯干涉美国选举，其中称俄方在社交媒体上利用机器人（Bots）与喷子（Trolls）结合的战术影响选民的投票意图和倾向。此次事件被美国战略界视为一次重大战略失败，其对美国政府与社会造成的负面影响持续至今；而围绕大选这一美国政治体制根基的争执也再度动摇了美国民众乃至全球社会对美国的信心。

（三）美俄信息战的未来走势

2024 年 1 月 8 日，美国国务院全球参与中心发布《反外国信息操纵框架》，明确指出美国将不再沿用“监测—报告”的传统方法应对信息威胁，同时承诺在信息安全领域制定和推行更为积极主动的战略^①。此份报告是拜登政府调整信息战战略的产物，此前经由国会授权、美国国防部在 2023 年 7 月发布的《信息环境行动战略》正式将“信息优势”作为美国军方的战略重心，并明确表示将迅速组建一支由军人和文职专家组成的信息战部队^②。除调整信息战目标、整合并新建高度集中的信息舆论宣传机制外，拜登政府还将自身的多边主义偏好纳入该领域，打造广泛的“信息战同盟”。在美欧贸易与技术委员会（TTC）、四边安全对话机制（QUAD）以及美日韩三边对话机制中，均能够看到与信息舆论竞争相关的要素与内容。上述措施背后反映出美国将改变自后冷战时期以来在信息对抗方面被动消极的防御姿态，并将信息战视为一场“真正的战争”。

为扭转自身在信息战中的相对颓势，美国在进行战略调整并积极备战的同时，也制定了新的策略，即通过公开披露情报争取舆论主动。俄乌冲突爆发前的 2021 年底至 2022 年初，美国政府在国家安全委员会的协调下，持续且大规模向国内外公众提供由情报界事先获取的机密信息，通过预先驳斥来阻碍俄罗斯在信

① U. S. Department of State, “The Framework to Counter Foreign State Information Manipulation”. <https://www.state.gov/the-framework-to-counter-foreign-state-information-manipulation/>, 访问时间：2024 年 4 月 20 日。

② U. S. Department of Defense, “Strategy for the Operations in the Information Environment”. <https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-DEPARTMENT-OF-DEFENSE-STRATEGY-FOR-OPERATIONS-IN-THE-INFORMATION-ENVIRONMENT.PDF>, 访问时间：2024 年 4 月 20 日。

息战中发挥叙事优势^①。在美国专栏作家布特看来，此类举措相当于“给俄罗斯军事机器的齿轮中注入沙子”，足以显示美国政府尝试掌控国际舆论主导权的主动姿态^②。

在调整战略侧重的基础上，美国具备充分动力推动人工智能融入自身战略规划。2020 年美国国防部开始策动其下设联合人工智能中心与参联会共同开展名为“全球信息主导实验”的项目，聚焦人工智能在信息战领域的多种应用。此外，负责研发军用高科技的行政机构国防高级研究计划局同样将识别深度伪造技术作为未来科技研发的重点。考虑到美国在人工智能技术领域的领先地位，这种技术优势转化为战略优势的速度将只增不减。

尽管如此，美国国内愈演愈烈的政治极化态势或将限制信息战战略的有效推进。在“为反对而反对”的政治环境内，针对虚假信息和错误信息的反制将面临阻碍。此前，为反击源自俄罗斯方面的信息冲击，美国政府试图介入抖音海外版（TikTok）、脸书（Facebook）、推特（Twitter）以及照片墙（Instagram）等主流社交媒体的信息过滤机制，但遭遇政府内外诸多网络自由理念支持者的抨击和抵制。拜登执政以来，国会共和党人将攻击目标集中于国务院全球参与中心这一美国信息战的关键机制，称其对媒体审查的行为严重违背美国宪法第一修正案^③。在可以预见的未来，国家安全与言论自由这一组美国国家安全史中长期无法化解的矛盾将继续限制美国信息战的推进。

反观俄罗斯，其在冷战后致力于寻找技术和地缘政治的交叉点，长期将信息战和网络战等非对称性工具作为对外战略的核心组成部分。这种战略思维令该国在人工智能技术治理与研发领域不及美国的情况下仍能扭转颓势，并掌握主动。考虑到人工智能时代信息战技术的特点，俄罗斯仍将不遗余力发挥自身高度集中的体制与机制优势，摆脱数字伦理的限制。俄将利用新兴技术赋能对外宣传工具，并将其与有限军事行动进行结合和综合运用，以实现制造“战略迷雾”并

① 张帆：《以公开披露情报为武器：乌克兰危机期间拜登政府对情报的另类使用及其战略逻辑》，载《美国研究》2022 年第 5 期。

② Max Boot, “Why the U. S. Ramped Up Its Information War with Russia”. <https://www.cfr.org/in-brief/why-us-ramped-its-information-war-russia>, 访问时间：2024 年 4 月 20 日。

③ Steven Lee Myers, “State Dept. ’ s Fight against Disinformation Comes under Attack”. <https://www.nytimes.com/2023/12/14/technology/state-department-disinformation-criticism.html>, 访问时间：2024 年 4 月 20 日。

掌控叙事主导权的目标。

随着自身力量的变化和俄罗斯战略的调整，俄罗斯在推进信息战方面的局限性也随之显现。从技术上看，俄罗斯过于注重创造信息战中的非对称竞争优势，为此推行了强政府主导下军事技术发展优先的治理策略。这种策略有助于俄罗斯在短期内获得战略收益，但在某种程度上以牺牲人工智能产业环境为代价，与数字时代主流国际科学研究体系“由下至上”的基本特征相悖^①。长期看来，这种动员式的治理模式或将导致俄罗斯在接下来的人工智能时代无法有效释放民间创新能力，具有不可持续性。随着美国军方大举开发和部署基于人工智能的反信息战技术，俄罗斯现有策略的边际效应将持续递减。

另一方面，俄罗斯长期将信息战作为自身对外战略重心的行为将不可避免地削弱该国的公信力。早在1999年，信息安全领域的知名学者约翰·阿奎拉就曾提醒政府应备加注意信息战中潜在的道德成本^②。随着冷战结束后俄罗斯综合国力的下降以及美国持续的舆论攻击，国际社会有关俄罗斯的负面信息持续存在。为此，俄罗斯自2000年以来尝试利用该国优秀的文化和艺术资源扩大自身知名度与影响力，巩固其在俄语区的文化主导地位^③。与此同时，俄罗斯仍在“灰色区域”内建构反西方的叙事与文化。美国借助自身在战后国际社会中的宣传霸权，积极披露甚至妖魔化俄罗斯信息战及其负面影响，将其建构为虚假信息和错误信息的制造者，对冲了俄罗斯积极释放自身软实力的努力。乌克兰危机后，俄罗斯因信息战而付出的道德成本越来越高，美国民调机构皮尤中心调查显示，自2019年以来，几乎所有中等收入国家对俄罗斯国家和现政府的负面情绪都以年

① Samuel Bendett, “Russia’s Artificial Intelligence Boom May Not Survive the War”. <https://www.cnas.org/publications/commentary/russias-artificial-intelligence-boom-may-not-survive-the-war>, 访问时间：2024年4月20日。

② John Arquilla, “Ethics and Information Warfare”, in Zalmay Khalilzad, John White, Andy Marshall ed., *The Changing Role of Information in Warfare*, RAND Cooperation Press, 1999, pp. 379–401.

③ 郭金峰：《俄罗斯软实力建设：理论、工具及绩效》，载《俄罗斯东欧中亚研究》2020年第5期。

均两位数增长^①。如何继续推进信息战略以实现自身战略目标，同时弱化日趋增加的道德成本，将成为未来俄罗斯政府面临的重大挑战。

三 人工智能时代国家信息战的风险与挑战

美俄为争取信息优势进行了长期而持续的博弈，两国在该领域战略态势的变化既源自传播技术的革命性突破，更是双方政府围绕相关技术进行战略考量，并依据相应战略投入具体应用的结果。美国在冷战结束后一度坚信自身的霸权优势能够带来道义优势，忽略了信息内容在网络空间中的重要意义；但在完成战略调整后，美国迅速将其在人工智能领域的技术优势转化为战略优势。相比之下，俄罗斯政府始终维系着对信息战的依赖，将其视作国家安全战略的关键部分。对此，俄罗斯积极策动颠覆性技术融入自身战略，在网络冲突时代依靠社交媒体弥补与美国乃至西方世界之间的差距，并在人工智能时代继续通过技术赋能强化信息战能力。随着人工智能继续发展，美俄将继续依据技术发展优化自身的信息战策略，这将不可避免地深化人工智能军事化和信息武器化趋势，为国际治理设置阻碍，并推动人类社会步入“后真相时代”。

（一）人工智能时代“信息武器化”态势将持续深化

当前，世界正经历百年未有之大变局，国际政治态势处于急剧变动的进程之中，国家间在政治、经济、社会、文化等领域的矛盾加剧，地缘政治竞争与大国博弈重回历史舞台。在这种时代背景下，人工智能技术的突破势必使国际社会遭遇前所未有的新兴风险。正如美国乔治城大学法学院教授罗莎·布鲁克斯在其专著中所指出的，战争形态正在随着人类社会的演进而悄然发生变化，行使暴力的手段也随之变得更为多元，最终结果将是“一切都成了战争，军事涵盖了一切”^②。该趋势正是当前国际社会“泛武器化”现象的真实写照。其中，“信息武器化”既是

^① Moria Fagan, Jacob Putshter, Sneha Gubbala, “Large Shares See Russia and Putin in Negative Light, While Views of Zelenskyy More Mixed”. <https://www.pewresearch.org/global/2023/07/10/large-shares-see-russia-and-putin-in-negative-light-while-views-of-zelenskyy-more-mixed/>, 访问时间：2024 年 4 月 20 日。

^② Rosa Brooks, *How Everything Became War and the Military Became Everything*, Simon & Schuster, 2016.

国家间常态化信息战的结果，也将是人类社会面临的重大挑战^①。借助大数据、机器学习和自动化系统，国家精准操控信息的能力将极大增强，国家间进行信息竞争的方式也将更为隐蔽。在这种情况下，国家的政治安全和社会安全及个人的数据安全和隐私权利均将受到侵蚀。

2022年初爆发并延续至今的俄乌冲突成为观察人工智能时代信息战态势的重要案例。俄罗斯与以美国为首的西方阵营展开了持续且高烈度的信息战。此次冲突展现了社交媒体与人工智能在塑造全球叙事中扮演的关键角色，是未来国家间信息战形态的集中写照。根据长期跟踪虚假信息的非政府组织“新闻守卫”（NewsGuard）的研究，危机期间，许多主流社交平台新用户在注册后平均40分钟内就会收到带有价值观诱导性的信息，其中大量内容和图片是动过手脚的虚假信息，经深度伪造技术产生的视频也充斥其中^②。尽管社交媒体公司采取一系列举措限制此类内容，但相关信息生成速度极快且能够绕过自主审查机制^③。这种情况导致与俄乌冲突相关的信息环境被严重污染，也令信息战中的防御国面临艰难的选择，即接受国内舆论环境乃至政治机制被影响的事实，或承受冲突升级的风险进行反制。

（二）人工智能时代“信息武器化”的治理困境

国际社会限制虚假信息传播的尝试可以追溯至第二次世界大战前。1936年多国签署《关于利用广播促进和平的国际公约》，承诺在广播节目中避免散播战争、暴力、种族仇恨和歧视等负面或虚假的信息^④。此后，尽管国际组织在不同历史时期均尝试就虚假和错误信息推出各类法律规制，但限制力极其有限。随着

① Rand Waltzman, “The Weaponization of Information: The Need for Cognitive Security”. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf, 访问时间：2024年4月20日。

② NewsGuard, “WarTok: TikTok Is Feeding War Disinformation to New Users within Minutes—Even If They Don’t Search for Ukraine – Related Content”. <https://www.newsguardtech.com/misinformation-monitor/march-2022/>, 访问时间：2024年4月20日。

③ Christian Perez, “Information Warfare in Russia’s War in Ukraine: The Role of Social Media and Artificial Intelligence in Shaping Global Narratives”. <https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/>, 访问时间：2024年4月20日。

④ League of Nations, “International Convention Concerning the Use of Broadcasting in the Cause of Peace”. <https://treaties.un.org/doc/Publication/UNTS/LON/Volume%20186/v186.pdf>, 访问时间：2024年4月20日。

传播虚假消息成为一种司空见惯的非胁迫性干涉手段，越来越多的国家开始担心迅速发展的深度伪造技术将被大规模应用于干涉他国内政或侵犯主权。从国际法的角度看，除非传播深度伪造信息的行为能够被证明是“刻意传播暴力威胁”并造成平民伤亡，否则将不受武装冲突法或其他国际法律规制的约束^①。在网络法专家迈克尔·施密特看来，由于国家会通过各类手段将行动限制在低于动能战争的“灰色区域”内，信息战将面临和网络战类似的溯源困境^②。在大国竞争的时代背景下，国家在如何制约深度伪造技术方面更加难以达成一致。

人工智能时代的信息战中，数字科技巨头具备与国家旗鼓相当的影响力。乌克兰危机期间，脸书、优兔（YouTube）、照片墙和 WhatsApp 等社交媒体均采取了较为明显的亲西方姿态，对源自俄罗斯方面的信息进行严格审查，优兔甚至在全球范围内屏蔽了与俄罗斯官方媒体相关的报道；相比之下，这些平台对乌克兰政府发布内容的限制要少得多^③。这也成为俄乌冲突中俄罗斯处于话语弱势地位的原因之一^④。与国家不同的是，私营部门并非“政府手中的工具”。在美国欧亚集团总裁伊恩·布雷默看来，2016 年美国大选之后政府与私营部门之间的相互指责，以及 2021 年特朗普支持者冲击美国国会山事件后企业相比政府更加激烈的反应，都能显示当代数字私营部门具有发挥政治影响的意愿和能力^⑤。在数字巨头有足够力量重塑全球秩序的时代，信息在国家间传播扩散所产生的效果将更具不确定性。

（三）“后真相时代”的中国战略选择

在百年未有之大变局及大国竞争复归背景下，大国有足够动力诉诸基于人工

① “Hitoshi Technology in the Age of Information Warfare”. <https://lieber.westpoint.edu/deepfake-technology-age-information-warfare/>, 访问时间：2024 年 4 月 20 日。

② Michael Schmitt, “‘Virtual’ Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law”, *Chicago Journal of International Law*, Vol. 19, No. 1, 2018.

③ Will Oremus, “In Ukraine, Tech Platforms Abandon the Illusion of Neutrality”. <https://www.washingtonpost.com/technology/2022/03/12/duckduckgo-russian-disinformation-unbiased-search-results/>, 访问日期：2024 年 4 月 20 日。

④ Alyssa Demus, Khrystyna Holynska, Krystyna Marcinek, *The Nightingale Versus the Bear What Persuasion Research Reveals About Ukraine’s and Russia’s Messaging on the War*, RAND Corporation Press, 2023, p. 5.

⑤ Ian Bremmer, “The Technopolar Moment: How Digital Powers Will Reshape the Global Order”, *Foreign Affairs*, Vol. 100, No. 6, 2021.

智能的信息战以争取战略主动，这将令舆论宣传行动变得更加复杂，持续推高国际社会风险。与此同时，国家对信息的塑造和控制将持续削弱公众对传统与新兴媒体的信任并侵蚀信息环境。比起追求难以触及的客观事实，受众群体更倾向于诉诸情感和个人信念；人类社会将随之深陷所谓“后真相时代”（Post-truth Era）。作为当前国际社会首屈一指的影响力大国，中国同样处于“后真相时代”所引发的冲击之中，妥善应对这种冲击则成为未来中国有效统筹发展和安全两件大事的关键。

从政府层面看，中国当前仍处于进一步完善国家信息安全机制建设的关键进程中。考虑到美俄信息战的历史经验，以及当前大国信息战中人工智能的应用态势，中国应当实时评估新兴技术在大国信息对抗中的战略影响、深化对各国信息战背后战略逻辑的理解，在机制构建进程中着重考虑信息内容方面的本体意义，坚持将“内容安全”作为网络信息安全的关键组成部分。在推动《关键信息基础设施安全保护条例》等现有规则进一步细化的过程中，有必要同时搭建相关的虚假信息 and 错误信息内容甄别机制及法律规制。与此同时，数据显示，到 2027 年，中国在网络空间安全专业领域的人才缺口将高达 327 万^①。为了能够给相关机制的发展提供支撑，中国未来应着力培养从事网络安全与信息安全的“后备梯队”。

从社会层面看，“后真相时代”的持续展开再次凸显了媒介素养（Media Literacy）的重要性。美俄信息战迈入网络冲突时代以来，美国民众长期暴露在复杂且多变的信息环境之下。美国民调显示，仅有 38% 的民众表示自己曾经学习过如何分析源自媒体的信息；大量缺乏甄别和判断能力的“媒介文盲”（Media Illiteracy）成为虚假信息的受害者与二次传播者，进而导致美国在信息博弈中的脆弱性^②。在人工智能时代，政治宣传与舆论操控将更具隐蔽性和穿透性，更加凸显出受众群体作为虚假信息和错误信息“首要防线”的重要性。对此，中国应当建立系统性的信息安全教育培养机制，着力提升青少年群体的批判性媒介思维能力和辨识能力。

① 中国教育部高等学校网络空间安全专业教学指导委员会：《网络安全人才实战能力白皮书：攻防实战能力篇》，2022 年 11 月，第 4 页。

② Daniel Dassow, “Journalism Professors Detail Crisis of American’s Media Illiteracy”. https://www.utdailybeacon.com/city_news/journalism-professors-detail-crisis-of-americans-media-illiteracy/article_2d892772-86d2-11eb-b023-5774db3aeb2d.html, 访问时间：2024 年 4 月 20 日。

从传播主体层面看,价值观的吸引力、影响力与同化力是国家在信息战中占优势的关键。在“后真相时代”,舆论宣传的成功与否取决于信息传递者的可信度,而非信息本身的真实性。从冷战时期到人工智能时代,被塑造和扭曲的信息始终存在,但“新闻守门人”(Gatekeeping)的权力和可信度却被一再削弱。后冷战初期,美国依靠基于国际霸权的“舆论霸权”迅速推广自身意识形态;但随着该国对外持续推动全球反恐战争,枪支暴力与种族问题等内部顽疾逐步激化,“舆论霸权”的边际效应持续递减,国内信任赤字逐步加剧,为外部攻势提供了契机。中国提升自身传播效度,关键在于提升国家文化软实力,并在此基础上讲好中国故事。积极弘扬中华民族优秀文化和光荣历史,掌握议题设置与舆论主动权,“西强我弱”的国际舆论格局不是不可改变,不可扭转的。

从国际层面看,中国应发挥自身在人工智能领域的优势,参与主导国际虚假信息治理进程,以期破解生成式人工智能武器化及其造成的信息战泛化难题,在数字领域践行人类命运共同体理念。2023 年 10 月,中国外交部发布《全球人工智能治理倡议》,明确指出“反对利用人工智能技术优势操纵舆论、传播虚假信息,干涉他国内政、社会制度及社会秩序,危害他国主权”^①。中国应以该倡议作为基础,依托联合国框架继续推动国际组织、政府部门、科研和教育机构、企业和社会在人工智能发展与治理领域的协调互动,以开放、包容、公正、非歧视的科技发展环境引领技术发展,令其更加促进文明的繁荣,化解信息战给国际舆论和国际社会带来的风险。

(责任编辑 聂保诚)

^① 中华人民共和国外交部:《全球人工智能治理倡议》, https://www.mfa.gov.cn/web/ziliao_674904/1179_674909/202310/t20231020_11164831.shtml, 访问时间:2024 年 4 月 20 日。