

美国认知安全战略：建构脉络、演进特点与影响评估

李 艳 崔文龙 桂畅旋

内容提要：美国注重认知影响的思维惯性根植于历史与文化之中。从一战起，美国认知安全理念从无意识逐步转向有意识；冷战时期，美国大量积累认知战经验，并将其制度化和理论化；冷战后期，美国认知安全战略布局基本成形；新时期社交网络、人工智能、算法分发等新技术对传统信息生产方式和传播结构造成冲击，美国认知安全观念与策略也相应调整与深化。纵观美国认知安全战略演进过程，其核心理念不变但主要目标对手不断调整，机制范式不变但机构部门调整。当前，美国通过强化技术赋能拓展认知安全空间、丰富认知战手段，认知安全策略显现建构主义倾向，认知安全议题亦成为其加固联盟的重要基石。未来，科技创新能力对认知安全的影响将进一步加深，军事领域的认知战与物理战界限将更趋模糊。在总体国家安全观指导下，加强战略预置、丰富战术机制、全面评估新兴技术风险与机遇是有效应对认知安全风险的应有之义。

关键词：中美关系 | 美国安全战略 | 认知安全 | 认知战

作者介绍：李艳，中国现代国际关系研究院科技与网络安全研究所所长、研究员，主要研究网络安全战略与国际治理、新兴技术与国家安全；崔文龙，中国现代国际关系研究院科技与网络安全研究所研究助理，主要研究网络意识形态安全；桂畅旋，《中国信息安全》杂志社副总编、高级工程师，主要研究网络信息安全。

百年未有之大变局与新一轮新兴技术变革同频共振的时空背景下，大国博弈暗流涌动、诡谲多变，新一轮全球转型与大国博弈不断带来新的安全议题，不断拓展国家安全问题域。其中，以人工智能为代表的新兴技术发展推动社会信息生产方式和传播结构经历深刻调整，以“信息收集无人化、编码机器化、

算法推送智能化”^①为特征的智能传播涌现使得认知问题“安全化”现象日益凸显，认知安全已然成为国家安全的重要内容。在乌克兰危机、巴以冲突中，物理域与认知域混合、虚拟网络与实体社会系统交织的作战态势充分印证了这一点。需要厘清的是，本文所提出的“认知安全战略”与常见的“认知战”（Cognitive Warfare）不尽相同。众所周知，从历史维度来看，“认知战”并不是一个新概念，只不过在不同时空条件下会呈现出鲜明的、阶段性的时代特征。当前的认知战更多表现出以网络、大数据、算法、人工智能等新兴技术为支撑手段，旨在改变个人、集体和社会的思想观念、价值判断、行动策略的一种综合的攻防形态；而“认知安全战略”则是从国家安全战略的维度去探析其应有的战略定位与政策布局。因此，从这个意义上讲，认知战只是认知安全战略的组成部分和具象形态，认知安全战略是其背后的底层逻辑与深层驱动力。美国不仅是最早将认知理念引入战域概念的国家之一，近年来更是积极推动体系化实践，逐步将认知安全战略纳入国家安全战略体系，并将中国视为主要战略目标与行动对象。在中美竞合博弈“白热化”和新一轮科技革命背景下，深入研究美国认知安全战略对维护国家安全具有重要的理论价值和战略意义。

一、由“术”及“道”：美国认知安全战略生成的基本脉络

美国注重认知影响的思维惯性植根于历史与文化之中。自诞生之初，伴随着内在的“正统性诉求”和“合法性危机”，美国一方面迫切需要与欧洲传统秩序进行切割，一方面又需要建构与欧洲强势体系的联系，这种复杂的张力关系长期驱动其粉饰殖民叙事的文化。它通过创造出一套以“民主”和“自由”为核心的价值体系进行自我历史建构和国际体系定位，并成为此后应对内外危机的内在策略。而新技术革命推动认知战从点到面、从偶发向常态、从战域向全域不断演进；国际政治发展和国际关系变化则进一步推动认知战由“术”及

^① 喻国明、鄧慧：《理解认知：把握未来传播的竞争重点、内在逻辑与操作路径》，《编辑之友》，2023年第3期，第58页。

“道”，经历从物理域、信息域到意识域、混合域的转向，逐渐成为美国国家战略意识的重要组成部分。

（一）大战前后：哲思性概念走向框架式战术

中美研究界普遍认为认知战的理念源头可追溯至《孙子兵法》“上兵伐谋”“攻心为上”等论述，但长期以来，其内涵的哲思意味和传奇色彩大于其广泛开展实践的可能性。19世纪，自由主义、民主主义等新意识形态出现，“为（现代）国际关系的行为实践提供了新的合法性策略”，^①美国此时“最早把政治含义引入宣传概念”。^②第二次工业革命后，信息和媒介的影响不断放大，战场逐渐成为物理热战属性和文化宣传属性相交叠的场域，“精神认知层面的破坏与征服是战争的终极目标”。^③由此，美国惯有内生诉求叠加传播格局转向，主动寻求意识形态扩张的驱动力进一步传承延续，形成认知安全战略意识雏形。

第一次世界大战开启了“意识形态斗争折磨着的20世纪的世界”。^④此时，美国作为全球秩序的新晋挑战者，形成与传统欧洲帝国相区别的安全观念，“将道德、自由、民主原则等抽象意识形态提升到国家安全观念中前所未有的高度”。^⑤美国1917年成立公共信息委员会（CPI），着手建构“宣传—认知”路径，其认知域行动开始由无意识转向有意识。二战期间，美国成立战争新闻办公室、美国之音广播电台和战略情报局，着力传播美国流行文化和生活方式。两次世界大战成为西方宣传概念变迁的分水岭，但信息仍受环境封闭、传递量级和抵达效率低下等因素限制。此时期信息本身基本等同于认知，认知施动方主要利用“信息差”干预原始信息投放，可以快速实现宣传动员和认知干预。面对较大体量的信息，受动方如无相关信息储备，很容易形成传播学意义上

① [英]巴里·布赞、乔治·劳森著，崔顺姬译：《全球转型：历史、现代性与国际关系的形成》，上海人民出版社，2020年，前言第2页。

② 刘海龙：《西方宣传概念的变迁：起源与早期的争论》，《国际新闻界》，2007年第4期，第10页。

③ [德]卡尔·冯·克劳塞维茨著，时殷弘译：《战争论》，商务印书馆，2016年，第8页。

④ [美]小约瑟夫·奈等著，张小明译：《理解全球冲突与合作：理论与历史（第十版）》，上海人民出版社，2018年，第115页。

⑤ 杨楠：《霸权的惯性：美国国家安全委员会与美国国际战略》，社会科学文献出版社，2022年，第62页。

“皮下注射”式的传播效果，如同“中弹”一般被迅速改变认知。典型案例如英军向德军前线抛撒传单、希特勒对挪威大使播放突袭波兰影片开展“电影攻心”等舆论战、心理战。而美国关注文化域和社会域的宣传策略尤具特点，如二战时期成立泛美事务协调员办公室（OCIAA）和战时信息办公室（OWI），前者意在对冲轴心国宣传攻势，后者“向全世界讲述美国的故事”。二战后，美国国务院还试图邀请苏联派出留学生和文艺团队赴美交流，以期通过文化平台加强影响力塑造。

（二）冷战以来：战术实践反哺理论发展

20世纪40至60年代，美苏全球冷战态势逐渐成形。“史密斯—蒙特法案”在国务院、国防部、参谋长联席会议的支持下获国会通过，美国认知战略主干部门就此确立。随后，美国成立国家安全委员会及中央情报局，改组美国新闻署、国际信息与教育交流办公室（OIE），组建公共外交咨询委员会、国家心理战略委员会，先后出台实施《美中关系白皮书》和国家安全委员会第34号、第59/1号、第166/2号文件等，逐步展开外国信息宣传、公共外交影响等行动配合遏制政策的“道德讨伐”和文化攻势。与此同时，美国推动“知更鸟行动”（Operation Mockingbird）等大规模对苏宣传活动，动员社会各界人士和组织在国内外进行宣传渗透：一方面强调自身行为的被动性，一方面展示美式文化特色和制度优越性。由此，其认知战略基本理念和行动机制逐渐明确，即全面渗透目标国政治、经济、社会、文化等各层面，通过公共外交和宣传渠道等软性和隐秘方式，广泛开展舆论包围和心理战。但由于同期冷战愈演愈烈，美国同时应对中苏两大国导致内部频繁论争、施政策略加速调整，实践成果难以迅速转化上升为系统的战略理论。

20世纪70年代前后，国际格局出现松动。西欧国家和日本纷纷崛起，法国脱离北约、智利发生政变等重大事件不一而足，美苏两大集团都在不断调整战略以应对新的国际局势和环境。同期，以电视为代表的大众媒介迅速发展，并推动信息传播结构变革，美国“宣传—认知”范式开始转向“信息控制—认

知”范式。至此，美国基于整体遏制战略的思路和美苏冷战的具体实践已积累了较为丰富的宣传舆论战经验，而国际战略环境转向和大规模热战退场则进一步推动战略研究的更新迭代。以托马斯·谢林（Thomas Schelling）、罗伯特·杰维斯（Robert Jervis）和罗伯特·阿克塞尔多德（Robert Axelrod）等为代表的一批学者先后将社会心理学、博弈论、知觉现象学等理论引入国际战略形势分析和政治决策过程，逐步搭建起较为完整的微观层次国际政治心理理论框架，为美国国家认知安全观念走向成熟奠定了理论基础。

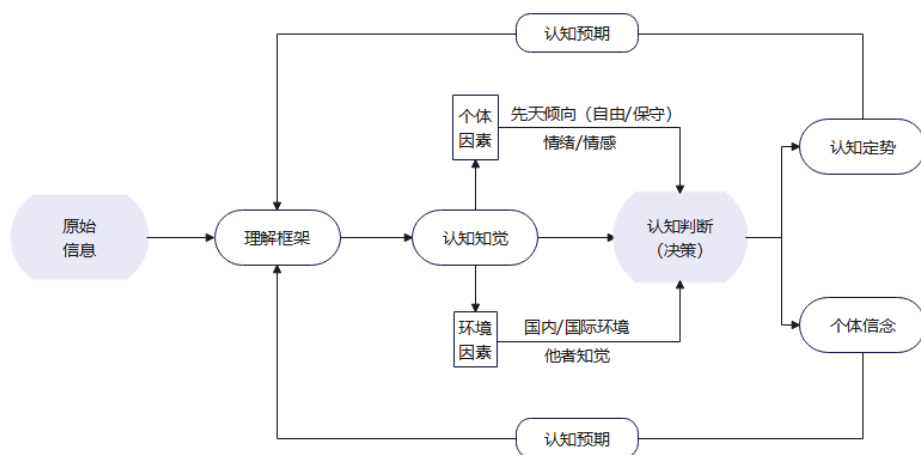


图1 罗伯特·杰维斯认知知觉体系及安全要素示意图

资料来源：作者自制。

杰维斯等学者将认知交互视为一个复杂的系统（见图1），包含理解框架、认知知觉、认知判断等关键节点，^①既含有个体心理层面的流转过过程，具有一定的规律性，也体现个体和社会相交织的潜在影响，伴随大量偶发与不可预测事件。从此视角看，认知战本质是施动和受动双方以信息为介质开展的认知知觉争夺，最终战略目标是影响对方决策。因此，无论是心理战、舆论战亦或信

^① 参见[美]罗伯特·杰维斯著，秦亚青、魏玲译：《国际政治中的知觉与错误知觉》，上海人民出版社，2023年。

息宣传战,都可视为是以认知战为目的的表现形式。同时,大众传播媒介的发展强化了舆论对决策的影响,认知安全场域从战场扩散至社会公共空间,涉及群体从军事人员扩散至一般民众,牵一发而动全身的复杂机制和广泛影响不断推动认知安全成为国家安全战略要素。

(三) 世纪之交:信息战框架下的新定位

冷战后期,美国政府将杰维斯等学者的理论体系进行战略化延伸。1981年,里根在出席美国军事学院毕业典礼的致辞中讲述乔治·华盛顿智胜敌人的案例,并引用“不战而屈人之兵”的论述,明确新国际局势下美国政府的战略策略取向。1983年,里根签署第77号国家安全决策指令(NSDD),明确情报界与国务院、新闻署、国际开发署以及高校、工商界、非政府机构紧密协作体系,宣传范式与全域信息控制深入融合,以公共舆论外交维护国家安全的战略理念显现。1993年,克林顿在总统就职演说中宣称“最强的力量是我们的思想”,将“在全球范围内扩展民主共同体”列为美国对外政策的三大支柱之一,^①战术化的认知战理念加速演化为战略化的认知安全战略体系。

此时期,军事领域成为美国认知战略演进的“头部”区域。20世纪90年代美国围绕海湾战争兴起军事大讨论期间,认知战概念仍被认作依附于信息战概念、具有新兴意味的替代化表述。而世纪之交,网络信息技术迅速发展,一方面推动大众媒介宣传范式革新,一方面引领信息武器化发展趋势。例如,美国国防部2001年《网络中心战》报告首次将“认知”作为信息作战框架下的重要战域提出,称认知域(Cognitive Dimension)涉及意识、价值观、公共舆论等领域,是信息作战的三大空间之一,代表未来战争的发展方向。^②2006年,认知域概念进入美军《联合信息作战条令(JP3-13)》文件。2012年11月,美国《联合信息作战条令》将认知域作为与物理域和信息域相并列的单独战域。^③

① 王国章编译:《美国历届总统就职演说》,中国商业出版社,2017年,第244页。

② See “Innovative Solutions to Improve Cognition,” NATO Innovation Hub, Cognition Workshop, <https://innovationhub-act.org/wp-content/uploads/2023/12/210601-Cognition-Workshop-Report-v3.pdf>.

③ 施庆庆:《美军联合信息作战条令的发展与特点》,《军事历史研究》,2009年第1期,第115页。

但是,受限于初代互联网技术发展的不够充分,美国对于认知攻防的研究与实践未能迅速深入,无论是2017年时任美国空军参谋长大卫·古德芬(David Goldfein)提出的“认知战”(当前认知战的普遍用语已从 Wars of Cognition 发展为 Cognitive Warfare)转型趋势,^①还是时任美国国防部情报局局长文森特·斯图尔特(Vincent Stewart)宣称认知战为“第五代战争”,依然是在信息分析和数据共享的范畴内讨论认知安全问题。

(四)新时空背景下:认知安全观念进一步深化

人工智能、算法分发、增强现实、脑认知科学以及社交网络的持续高速发展冲击着传统的信息生产方式和传播结构,导致一方面传统认知战的致效手段受到冲击,一方面认知域开展战略竞争的主体、介质和手段极大丰富。与此同时,“通信技术以及社交媒体使得经济和政治不满情绪得以爆发”,^②任何局部的、偶发的、非预期的事件都有可能引发形成国内甚至国际层面的集体性事件,认知问题的安全价值和战略价值进一步抬升。因此,“仅在内容写作元素上进行操纵已经无法获得大众传播时代的强劝服效果”,^③“信息差”开始转向“认知差”,“信息争夺”开始转向“认知争夺”,兴盛于一战、二战和初代互联网时期的“宣传—劝说”内在框架体系^④升维为直抵“制脑权”的观念争夺和认知建构。与此同时,技术飞速发展必然会对国家安全的稳定状态造成现实冲击,^⑤包括网络安全在内的传统安全已不足以确保国家安全,认知战从“灵光一现”

① Wilson Brissett, “The Need for Speed,” October 9, 2017, <https://www.airforcemag.com/article/need-speed-russia-korea-china/>.

② [美]小约瑟夫·奈等著,张小明译:《理解全球冲突与合作:理论与历史(第十版)》,上海人民出版社,2018年,第371页。

③ 喻国明、刘彧晗:《从信息竞争到认知竞争:策略性传播范式全新转型》,《现代传播》,2023年2月,第131页。

④ “宣传—劝说”通常指传播学史中“旧宣传”时期的舆论引导路径,强调宣传是一种单向度的、高效的、预设目标的定向传播。随着传播科学的发展和现代行为科学的进步,“新宣传”将“宣传”“舆论”等概念放到组织与公共关系的框架中加以理解,“宣传—劝说”路径逐渐被“说服”“态度”“对话”“议程设置”等概念所替代。

⑤ 封帅:《国家安全学视域下的人工智能安全研究:议题网络建构的初步尝试》,《国际安全研究》,2023年第1期,第30页。

式的战术理念转为与物理战平等且共生的战略概念。

2016年后,美国持续构建完善多域战中的“认知域”理念,将认知视为基于脑科学和神经科学研究的新战域,强调大脑将成为战场的一部分。2020年北约盟军转型司令部下属的创新中心发布《作战2040:北约在未来将如何竞争》项目报告,强调人类大脑成为继天空、陆地、海上、太空和网络之后的第六大作战领域;2022年,美国《国家安全战略》报告将认知战提升到与物理层面作战同等重要的战略地位,认知域(或称脑域)完全独立;2023年,美国国会参众两院将“大国竞争背景下的信息空间对抗”作为关注点,《美国情报界年度威胁评估》报告更是聚焦重点国家全球“影响力活动”,认知安全概念逐步走向具象化。随后,以美国为主导的北约合作网络防御卓越中心(CCDCOE)将提高认知能力作为首要任务;北约修定盟军联合理论条令(AJP-01),纳入“行为中心方法”(Behavioural-centric),以对目标受众进行话语分析并影响其认知和行动。同时,美国国防部及各军种频繁发布战略条令等文件,包括国防部2023年《国防部网络战略》非机密摘要、《陆军条令出版物3-13:信息》、《太平洋空军2030战略》等均强调“塑造战场”“观念影响”“战略叙事”等认知作战理念。

综上所述,从国家安全战略角度看,“认知安全”是一个外延较为宽泛的概念,“国家安全涉及的各个领域,都存在不同程度的认知安全内容”,因而可从政治、经济、军事、文化等多角度进行观察。对认知安全内涵实质的理解则可从主体安全状态切入,即“确保个体、社会和国家等主体在不同认知层面免受扰害的客观状态”。^①更进一步则可划分为三个维度层次,认知安全作为一个宏观层面的概念,在国家战略实践中,特别是在信息社会环境下,通常体现为“话语体系”“国家叙事”“国家形象”“价值观输出”“影响力行动”等中观维度的策略。而具象的微观特点则需观察支撑策略的具体手段,如机制情况,包括涉认知部门机构与运行机制;如信息加工手段,包括情报能力、议程设置

^① 苏志远:《总体国家安全观视野下认知安全的理论阐释》,《情报杂志》,2024年第2期,第43页。

与叙事框架输出能力；如技术支撑手段，包括虚假信息发现核查、研判分析与介入干预能力等，这三个维度层次共同组成国家认知安全战略要素特征。

二、变与不变：美国认知安全战略演进特点

在美国自身强烈“不安全感”和注重价值观输出的传统内在安全思维统摄下，服务于美国霸权的认知安全理念始终未有质变，但其具体策略及认知安全实践不断因应国际环境和技术演进趋势而调适。

（一）核心理念不变，主要目标对手调整

各国国家安全理念通常因应时代环境变化而调整，同时保留核心内容。冷战前，美国将传统军事安全作为关注重点，“9·11”事件后更关注恐怖主义和大规模杀伤性武器等非传统安全领域。但美国对于大国权力博弈的热衷及以零和博弈思维打压别国话语、信念和价值体系的宗旨始终未变。从具体手段上看，美国看重国际社会认知和影响力塑造，“向他国推广自由民主是美国国家安全观始终如一的特点”。^①与此同时，美国国家安全观始终自带“不安全感”，“总是偏执地认为外部存在着对美国的阴谋和威胁”，^②美式的“例外主义”与“灯塔情节”使西方学者“只强调其他国家发起的认知战，以及其可能带来的威胁——似乎西方只是为了进行自我防御而对认知战进行研究”^③。实质上，美国以守代攻的认知安全战略路线在冷战时期完成制度化并一以贯之，即以影响对手心灵和行为的是“事物的影像（象征）而非实质”^④为价值取向，显现为以公共外交政策转向认知塑造的进攻型态势，一方面强化自身作为他国“虚假

① 周琪、付随鑫：《中美国家安全观的分析与比较》，《当代世界与社会主义》，2014年第6期，第21页。

② 张爽：《阴谋论、威胁论与美国国家安全观》，《山西大学学报（哲学社会科学版）》，2011年第5期，第91页。

③ 孙鹏、黄格林：《西方对认知战的研究历程及其特征述评：2008—2021》，《思想理论战线》，2022年第6期第1卷，第123页。

④ [美]约翰·刘易斯·加迪斯著，时殷弘译：《遏制战略》，商务印书馆，2019年，第179页。

信息”“媒介操纵”等“影响力行动”受害者的形象，并以此为借口在全政府设置反影响力行动部门；一方面在全球开展叙事之争与话语之战，建立巩固“价值观联盟”，推行蕴含美式价值观的数字标准、治理理念与关键基础设施。新时空转换仅丰富了美国认知安全手段而未动摇其理念，“认知操纵/管理在为美国从网络信息空间向认知空间霸权扩张中提供着战略性心力支持，是其竭力维系‘隐性帝国’对全球影响‘主导权’的标志性样式”，^①其根本目标始终是维持全球霸权。

美国认知安全战略目标面向全球，主要对手通常设定为具有威胁的主要大国，当前明确视中国为“最主要竞争对手”和“最严峻地缘政治挑战”。从时间节点上回顾，自2010年中国经济总量跃居世界第二，美国开始在其话语体系中强调中国崛起伴生的“影响力威胁”。2010年美国《国家安全战略》报告将中国列为全球新的“关键影响力中心”，美国政府随后频频宣称“对抗中国影响力”以及在亚太、非洲等地与中国“争夺影响力”。2017年美国《国家安全战略》报告提出中国“锐实力”（Sharp Power）概念并延用至今。2020年前后，随着中国（大陆）国内生产总值超过欧盟以及国际影响力进一步提升，美国将中俄加强伙伴关系、在台海问题和南海问题坚定立场以及“东升西降”等表述视为中国重塑国际秩序的表现，基于此不断强化“影响力行动”“信息操纵”等负面概念以支撑其认知行动。拜登政府一直将“对抗中国影响力”“抵消中国影响力以保持美国全球领导地位”列为重点讨论事项；2020年《美国对中华人民共和国战略指针》把“体制之争、价值观之争、意识形态之争”推向中美博弈的前沿。乌克兰危机和巴以冲突爆发后，美国仍不断战略加码：2023年，《美国国防战略》《美国印太战略》报告将“中国影响力”表述调整为“中国全球影响力”，美国务院全球接触中心（GEC）用20种语言发布报告指称“中国塑造全球媒体环境”^②，

① 左军占：《基于战略心力全球影响塑造与控制的认知战争理念》，《思想理论战线》，2022年第4期第1卷，第122页。

② “How the People’s Republic of China Seeks to Reshape the Global Information Environment,” September 28, 2023, <https://www.state.gov/gec-special-report-how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/>.

《2024 年美国情报界年度威胁评估》报告称中国“秘密影响力活动咄咄逼人”。^①

（二）机制范式不变，机构部门调整

美国认知安全战略实施路径承袭二战以来尤其是冷战期间的宣传战、舆论战的范式，以全政府姿态开展布局，在国家安全委员会统筹下，协调国务院、情报界、国防部，联动媒体、智库和非政府组织等全社会共同运作，此“三点一线”机构版图不断调试和延伸，近年来呈现两种趋向。

一是全政府大批成立、改组涉影响力和认知研究部门。美国国务院、情报界及国防部 2020 年后以打击虚假信息和防止干扰选举为由大量组建涉“影响力行动”部门，包括国土安全部的打击外国影响力小组委员会（CFITF）、联邦调查局的外国影响力工作组（FITF）、国防军事欺骗办公室（DMDPO）以及国防部影响和认知管理办公室（IPMO）等；中情局还特别以“应对中国这一长期威胁”为优先事项进行机构改革和重组，于 2021 年创设中国任务中心。为有效协调各“影响力”部门形成认知效应，2022 年 9 月经国会特许，在国家情报总监办公室下设外国恶意影响中心（FMIC），协调情报界涉影响力部门的工作并处理虚假信息。

二是加紧开展表现为价值观外交的认知渗透。2016 年起，美国着手将国务院全球公共事务局（GPA）和全球接触中心调整为认知战略主干部门，前者偏重于国内宣传，主要负责向受众有效传达美国外交政策目标；后者偏重于全球宣传，塑造有关美国外交政策和价值观的全球叙事，二者均内设技术研究和数据分析部门以监测和分析受众“画像”和舆情信息。此外，国务院政治军事事务局（PM）、对外援助办公室、国会和公共事务办公室（CPA）、网络空间数字政策局（CDP）等部门均有认知行动职能，承担与美国国际开发署（USAID）、国防部保持联系协调以及促进国会与国内外媒体和公众沟通互动等任务。为进一步适应网络传播时代多媒介渠道复合传播发展趋势，美国

^① *Annual Threat Assessment of the U.S. Intelligence Community 2024*, Office of the Director of National Intelligence, February 5, 2024, pp.7-13.

2018年改建美国全球媒体中心（USAGM），以最大限度地发挥媒体影响力，支撑以美国利益、国家安全和自由等普世价值观为核心的长期战略目标。同时，美国持续强化对外援助部门的意识形态色彩和价值观属性，通过援助支持别国民间组织、研究机构和拉拢“志同道合者”，特别是借助国际开发署、中情局、驻联合国代表等国家安全委员会成员方渠道形成认知塑造合力。

（三）技术赋能理念进一步强化与拓展

认知安全自身携带强烈的技术指向，且美国有发挥技术优势的“抵消战略”（Offset Strategy）惯性。^①2016年总统大选引发“网络干选”风波，美国政府开始将选举中的信息操纵视为互联网时代的新型网络攻击。由于网络干选目标针对国家机器和公民、左右选民投票倾向于无形、效果难以度量但十分现实，美国遂在国家网络安全战略顶层设计中重点关注认知安全。例如，时任共和党参议员罗布·波特曼（Rob Portman）和民主党参议员克里斯·墨菲（Chris Murphy）联合提出“反虚假信息及反宣传法案”，将反外国虚假信息列入政府工作重点，并要求调动全政府部门进行应对。该提案被纳入《2017财年国防授权法》获得通过，并促成国务院全球接触中心的成立。该中心主要负责协调美国政府部门及各类非政府组织的资源，以实质性提升应对恶意宣传和虚假信息的能力。^②

特朗普政府2017年发布的《国家安全战略》报告和2018年《美国国家网络战略》报告均高度关注以虚假信息为主要内容的认知安全，前者将打击虚假信息列为“信息治国方略”（Information Statecraft）的重点之一。拜登政府不断推出虚假信息——“威权主义”挑战“民主秩序”的叙事，要求与盟友进行联合反制，随后进一步着手建立网络安全域下的认知安全保障机制。美国国土安全部科学和技术局、网络安全和基础设施安全局以及商务部下设的国家标

① Bob Work, “The Third U.S. Offset Strategy and Its Implications for Partners and Allies,” January 28, 2015, <https://www.defense.gov/News/Speeches/Speech/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies/>.

② 袁莎：《美国反虚假信息行动：内涵、手段与影响》，《当代美国评论》，2023年第3期，第99页。

准与技术研究所为网络认知战提供基础设施，为网络认知攻防提供技术保障。同时，国土安全部增加“思想和信息监管”的职责；^①该部下属网络安全和基础设施安全局局长珍·伊斯特利（Jen Easterly）称，“有人可能会说我们从事的是关键基础设施业务，而最关键的基础设施是我们的认知基础设施”。^②2022年，国家安全局、联邦调查局、网络安全和基础设施安全局联合发布网络安全信息表（CSI），集体应对深度伪造带来的认知威胁。2023年美国发布《国家网络安全战略》，明确将网络空间列为反映美国价值观的工具。

随着社交机器人、大数据在战争宣传动员中发挥重要作用，算法操纵大量运用到政治舆论场，以社交媒体为代表的网络空间逐渐成为美国推进认知安全战略的枢纽。2023年全球有超过50亿社交媒体用户，占全球总人口的62.3%，人们平均每天在社交平台上耗时超过2.5小时。^③当前全球月活跃用户超过20亿的社交媒体平台Facebook、YouTube、WhatsApp、Instagram均被美国科技巨头垄断且有美国政府深度介入，2022年推特泄密文件就显示网络安全和基础设施安全局网络安全咨询委员会成员长期参与社交媒体平台内容审查。^④2022年美国斯坦福大学网络观察室和社交平台分析公司Graphika联合发布《未闻之声：五年来“亲西方秘密操纵舆论运动”的评估》报告，详细披露美国利用社交媒体操纵全球舆论行为。2023年12月，该网络观察室被共和党指责与国土安全部和国务院联系密切，以“反虚假信息”为由操纵社交媒体信息、影响选举公正，最终导致实验室核心人员离开、核心业务变更。该事件进一步曝光美国利用社交媒体平台将虚假信息武器化的行为。

① Erin Dwinell, “Biden’s Homeland Security Department Still Engaging in Censorship,” April 11, 2023, <https://www.heritage.org/homeland-security/commentary/bidens-homeland-security-department-still-engaging-censorship>.

② Maggie Miller, “Cyber Agency Beefing Up Disinformation, Misinformation Team,” November 10, 2021, <https://thehill.com/policy/cybersecurity/580990-cyber-agency-beefing-up-disinformation-misinformation-team/>.

③ “Digital 2024: 5 Billion Social Media Users,” <https://wearesocial.com/cn/blog/2024/01/digital-2024/>.

④ Victor Nava, “Who Is Vijaya Gadde, the Twitter Exec Involved in Censoring Post’s Hunter Biden Laptop Bombshell?” <https://nypost.com/2022/12/03/twitter-files-who-is-vijaya-gadde-the-twitter-exec-involved-in-censoring-posts-hunter-biden-laptop-story/>.

与此同时,美国政府还频繁利用信息过载和虚假信息导致的网民认知困难,率先编织“重大事件解释框架”来引导受众理解和判断相关问题,通过重复投放强行开展议程设置,并为博人眼球掺入大量情绪化元素。2024年3月,路透社披露特朗普曾授权中情局成立小型特工队对中国发起社交网络秘密战略行动,包括用虚假网络身份传播涉华负面言论,抨击中国“一带一路”倡议,向海外新闻媒体发布诽谤性情报,操纵东南亚、非洲和南太平洋地区的公众舆论等,“该行动至今可能仍在进行中”。^①美军也多次开展有关场景模拟技术和数据机器人的实战演练,大规模发布可以相互印证的虚假信息,而后运用大规模机器人水军在社交媒体平台快速扩散并跟帖引导舆论发酵,误导公众认知。

(四) 认知安全成为美国加固联盟重要基石之一

冷战结束后,美国主导联盟体系以巩固全球影响力、制衡对手并扩大战略纵深。此后,“价值观联盟”构想始终“或明或暗地贯穿于美国政府的战略部署之中”。^②可以说,“价值观联盟”策略是美国隐性的认知安全战略的重要表征。而拜登上任更是将“价值观联盟”作为修复联盟关系的重要抓手,通过刻意分化“民主”和“专制”的“两类国家”,通过军事合作、基础设施建设、技术标准输出等非直接方式,持续打造旨在孤立目标对象的功能化联盟,形成涉及经济、政治和技术的影响力包围圈。

但是,美国在具体实践中长期面临联盟内部利益不统一、理念设定虚化泛化的问题。为此,以多国大选为契机,美国将“虚假信息”“媒介操纵”“干预民主进程”等认知安全议题作为持续加固“价值观联盟”的推动力,如同北约组建针对所谓“威权政府资助虚假信息发布”的快速反应小组,同七国集团建立应对虚假信息的快速响应机制,与欧盟加强反虚假信息协调等。2022年初,

① Joel Schectman and Christopher Bing, “Exclusive: Trump Launched CIA Covert Influence Operation Against China,” <https://www.reuters.com/world/us/trump-launched-cia-covert-influence-operation-against-china-2024-03-14/>.

② 蒋蕊韩、吴艳东:《美西方构筑“价值观联盟”的动因、表现及中国应对》,《国外理论动态》,2023年第6期,第18页。

美国与北约、澳大利亚、日本联合提出在 6 年内建立以美国为主导的网络认知战合作体系。乌克兰危机和巴以冲突爆发后，美国加大推进“民主对抗威权”的叙事力度，捆绑“威权主义”“专制政体”等意识形态化概念，构建价值观联盟新形态。2024 年，美国先是与英国、加拿大共同提出《打击外国国家信息操纵框架》，并与芬兰、意大利、拉脱维亚等国签署谅解备忘录，而后又提出抵御全球数字操纵的“民主路线图”（Democratic Roadmap）和“数字团结”（Digital Solidarity）理念，渲染炒作“数字威权”与“价值观威胁”，寻求与盟伴在捍卫信息完整、保护全球选举和其他民主进程等认知议题上达成共识。

三、“制脑”博弈：美国认知安全战略发展趋势

数字时代，信息安全呈现泛在化特点，与其他安全的融合度不断提升。近年来，人工智能等新兴技术的快速发展使得认知塑造呈现新的演进特点。美国在延续认知安全观念和策略的基础上，不断强化对新兴技术与认知安全的捆绑，加速提升认知战的技术含量，意图以科技优势扩大认知优势；不断强化认知塑造的长期化和隐性化，意图打造和保持先发优势；不断强化认知安全相关基础研究，将现实战场作为认知前沿技术的应用场。未来，中美脑域认知博弈将更趋激烈。

（一）科技创新能力成为决定认知安全的关键要素

从认知安全发展规律看，历次信息传播技术的迭代均成为推动认知战发展的关键驱动力，因而认知安全问题自带的强烈新兴技术属性即是其天然特性。然而，新兴技术发展规律内含不安全属性，科技创新能力与认知安全的密切联系也不断凸显。从美国历史特别是冷战史看，美国具有“技术民族主义”的传统，一方面注重自身科技创新能力建设，加强对科学研究与技术研发的管理与支持，政府长期保持与大型科技企业的复杂关系；另一方面不惜以破坏全球贸易秩序和正常技术合作为代价，利用政治、经济和联盟等手段遏制别国技术发

展，将科技问题极端国家安全化。

美国 2024 年总统大选周期开启后，民主、共和两党频陷虚假信息旋涡，拜登和特朗普均成深度伪造目标，客观上促美国各方更加清晰地意识到新兴技术牵涉的认知安全风险，进一步将科技创新能力作为其认知安全战略的着眼点和发力点。当前，美国国务院、国土安全部、国家情报总监办公室等频频宣称虚假信息是“全球民主最严重的威胁之一”，将深度伪造列为“塑造地缘政治的要素”；美国智库兰德公司、哈德逊研究所等发布报告渲染媒介和信息操纵技术代表了“第四次工业革命”，生成式人工智能成为“颠覆性政治力量”。主观上，美国不断抬升虚假信息与深度伪造的战略威胁性，实质是技术问题泛国家安全化的策略延续，意在为其进一步强化的对华科技封锁提供合理性。客观上，人工智能大模型存在价值偏见已具备相当程度的共识，技术话语权与认知安全塑造能力的相关性未来确将不断提升。因此，继对华封锁芯片硬件后，近期美国众议院外交事务委员会主席迈克尔·麦考尔（Michael McCaul）和美中战略竞争特别委员会主席约翰·穆勒纳尔（John Moolenaar）等国会议员谋划限制中国使用人工智能大模型软件，并提案限制中国人在美从事人工智能相关工作。而与此同时，美国国家科学基金会（NSF）、小企业管理局（SBA）等机构均推出促进缩短新兴技术研发落地周期的政策措施。此外，美国还利用人工智能技术持续开展认知防御技术行动，开发出 OmniSpeech、RESIST-2、Semafor 等虚假信息与深度伪造识别、溯源和取证工具包。

在认知安全策略的驱动下，未来美国将进一步强化在人工智能、大数据、芯片等与认知安全高相关科技领域的技术封锁，通过加强相关技术产品出口管制、构筑“小院高墙”、强化政企研合作等方式护持其新兴技术优势。而在科技安全策略的驱动下，美国将延续捆绑高科技与价值观的做法，给数字空间和生成式人工智能打上“民主”“人权”标签，通过引领人工智能治理、打造“反虚假信息联盟”等方式塑造技术话语权，并以此强化意识形态阵营对立，继而推广基于美式价值观的数字标准和数字基础设施。受此影响，未来国际社会中技术强国与弱国之间的“数字鸿沟”及其伴生的“认知鸿沟”或将进一步

扩大，中美意识形态对抗的主要形式与实际效果将更多取决于新兴技术驱动下的认知战手段的应用。

（二）未来认知战将更加注重“长线塑造”

新时空条件下，非国家行为体日益增长的作用及社会层面的全球化使得体系效应（System Effects）不断增强，国家价值观体系安全成为国家安全的核心。认知安全虽表现为即时性和突发性，但其内在态势的形成是一个长期的过程，如乌克兰危机和巴以冲突中，冲突双方的认知立场分歧均基于深层的知识结构、感情与认同分歧。客观上，新技术生态正进一步强化文化身份的分化、个体认知塑造的可能性以及传统国家边界的游离；主观上，美国根深蒂固地笃信自身价值观具有普适性，“很难坐视后发国家在全球治理中拥有更大的影响力”。^①在此趋势影响下，美国战略偏好将从现实主义逐步向建构主义范式调整，更注重不断开展隐性认知影响和长线认知塑造。

近年来，美国尤为注重将政府和智库的公开报告作为塑造全球认知的武器。2023年初，美国国会众议院美中战略竞争特别委员会成立后，频繁举行听证会并发布政策报告，借中美互派留学生、TikTok等议题渲染中国认知威胁。美国国家情报总监办公室发布的《2023年美国情报界年度威胁评估》报告及国务院全球接触中心大量报告将中俄塑造为试图“暗中影响”国际舆论、“刻意制造认知偏见”的负面形象；国土安全部在《2024年国土安全威胁评估》报告中将外国错误、虚假及恶意信息定为四类高风险威胁之一；微软威胁研究院等机构长期渲染外国政府组织的“黑客攻击”和“网络勒索”。美国智库相应强化对“信息操纵”和对外影响力的研究，如布鲁金斯学会发布《在社交媒体上维护2024年选举》、兰德公司发布《拆除影响力运作的虚假信息业务》等报告。此外，美国还对国际组织、非政府研究机构提供资金和官方数据支持，促其产出更多具有全球影响力且展示美国观点的报告。

^① [英]巴里·布赞、乔治·劳森著，崔顺姬译：《全球转型：历史、现代性与国际关系的形成》，上海人民出版社，2020年，第272页。

与此同时，美国还不断探索通过“战略解密”（Strategic Declassification）塑造短期认知，“长短结合”搭建隐匿化建构和输出影响力威慑策略。2023 年，美国国防大学《棱镜》杂志和《联合部队季刊》都曾刊文复盘乌克兰危机前情报披露的细节，称美国曾在乌克兰危机前通过情报外交等方式，分别向英法德等盟友以及俄罗斯详细披露俄拟出兵乌克兰计划，在短时间内组建拉拢“遏俄挺乌”阵线，并对俄形成了快速威慑。此举虽未直接阻止冲突爆发，但对冲了俄罗斯“特别军事行动”叙事，致俄陷入国际舆论被动。巴以冲突期间，冲突双方各自围绕希法医院爆炸事件进行叙事，制造认知混乱；美国国家安全委员会发言人约翰·柯比（John Kirby）通过披露秘密情报支持以色列关于哈马斯在医院窝藏武器的说法，成功引导国际主流舆论认知。此范式被中情局局长威廉·伯恩斯（William Burns）称为“战略解密”，^①即有意公开披露某些秘密情报，在社交媒体、主流网站等多渠道多话语风格迅速扩散、相互印证策应，形成“正义叙事”以左右国际认知。

从认知致效机理层面看，“锚定偏见”或“确认偏差”反映出认知先发优势的极端重要性：一旦误解形成，反向认知塑造的成本和难度将被极大抬高。美国长线隐性认知塑造的战略偏向会持续累计国际舆论的慢性效应，未来将加剧国际社会对中国的认知偏差。短期的“战略解密”则很有可能在极端情况和突发事件背景下形成认知包围圈，这种短期的快速威慑极易冲击中国的既定计划和执行力。当然，美国长期的隐性塑造将实质性地透支国际受众信任，并面临全球化背景下价值观极化压力和价值取向分裂风险。为此，美国引领构建的各类“微多边”“小多边”联盟一方面将更强调信息共享机制，另一方面会更突出软性意识形态合作。

（三）军事领域的认知战与物理战界限将更趋模糊

军事领域是认知战的原生场景，美国高度关注战场的信息优势与认知优势

^① William J. Burns, “Spycraft and Statecraft Transforming the CIA for an Age of Competition,” *Foreign Affairs*, Vol.103, No.2, Mar/Apr 2024, p.44.

塑造，持续强化将认知相关基础研究率先应用于军事。美国陆军、空军 2019 年相继宣布改组网络战力量，信息认知战是其重要工作职责；国防部 2023 版《信息环境作战战略》（SOIE）强调维持军事行动中的信息优势；网络司令部近年来持续深化“前出狩猎”行动（Hunt Forward）战略和双边技术合作。该战略创立之初以维护选举安全为目的，以共享信息为基础环节，要求收集对手国家开展影响力行动和干预选举的一手信息，并通过定期会议、技术合作、联合演习等方式，与盟友国家、国际组织的网络安全机构建立广泛的合作关系，一举突破了美国国防部禁止派员进入另一主权国家行使任务的限制。目前“前出狩猎”行动已逐步发展为美军维护认知安全的主要行动策略，并且常态化扩大化地开展，不断加剧网络空间军事化和紧张局势。

乌克兰危机期间，美军发挥技术和平台优势，帮助乌克兰广泛收集俄罗斯官兵在社交媒体上的信息以分析其思想动态和行动路线，随后更为注重利用最新技术确立战场认知优势。美国国防部高级研究计划局（DARPA）2021 年起连续启动认知影响力系列研究项目，包括“影响力行动感知”（INCAS）、“动态信息环境下信息传递因素”（MIPs）、“内在认知安全”（ICS）等项目。美国海军研究所成立认知表现研究组（Cognitive Performance Group），以实证研究支撑重大军事战略决策，并开发出 C-IED 工具包以增强小型地面部队认知防御能力。美国智库战略与国际问题研究中心（CSIS）基于多诺万（Donovan）平台开发用于开展战略级兵棋推演的大语言模型，还特别加入了应对外国对手虚假网络信息攻击的模块。2024 年，美军与知名大数据公司帕兰提尔（Palantir）合作，在全球美军司令部推广 Maven 智能系统——可汇集分析来自卫星、社交媒体和其他多种来源的数据，作为其全球信息优势实验（GIDE）和盟军联合全域指挥与控制系统（CJADC2）全球全军种战斗指挥网络的组成部分。美国国防部首席数字和人工智能办公室（CDAO）还开发出 Tradewinds 平台，帮助各种规模高科技企业迅速向国防部推介自身新兴技术并快速投入应用。

综上，美军已将认知战内嵌于军事战略与行动的全链条之中，无论是战前

准备，还是战时行动，尤其是非战时的认知塑造铺垫与准备均全面跟进，一如既往地配合军事行动的基础上，对军事行动的效果起着越来越重要的作用。2022 年，兰德公司发布报告《破坏威慑：审视技术对 21 世纪战略威慑的影响》，宣称先进的影响力活动、信息操纵、叙事控制“正在改变战争的特征”。随着现代战争的不断演进，尤其是技术的加持，这种边界日益模糊，在一定程度上甚至将推动未来战争成为“平战一体”的冲突形态。

纵向梳理美国认知安全战略理念演进脉络才能有效拨开认知域的“战争迷雾”。百年来，美国的认知安全理念发展始终较为超前和大胆，善于建构基于自身意识形态体系的认知框架，并及时运用技术革命成果进行有效赋能。当前美国认知安全战略仍处于演进变化之中，未来虽将加强认知机理研究、与人工智能等新兴技术结合，以及塑造长期的隐性影响力，但其认知安全观念不会发生实质性改变。

新技术加持与国际形势更趋严峻的背景下，认知安全已成为国家安全重要基石，有效应对该领域风险挑战可考虑从三方面着手。一是全面加强认知安全领域布局。在总体国家安全观指导下，对全时、全域、全手段认知塑造可能带来的战略影响进行风险评估，夯实认知安全理论研究基础和法治保障，推动多元治理，带动社会认知安全素养提升。二是战术机制应更加灵活多样。认知攻防态势转换变化快、偶发性强，认知安全策略需不断因应变化调整，可考虑组建反虚假信息、反影响力等认知安全专门机构，突破长期以来以宣传应对认知的非对称局面。三是高度重视新兴技术蕴含的认知风险与机遇。重点关注技术背后的文化霸权、意识形态话语权和“数字鸿沟”加剧等风险，警惕美国将人工智能技术武器化，同时进一步鼓励技术创新，增强中国在生成式人工智能领域竞争力，借助新兴技术打开中美认知博弈突破口。

（责任编辑：王锦）