美发布新版人工智能行政令

■王大宁

6月上旬，美国总统特朗普签署“促进先进人工智能创新与安全”行政令，旨在加强网络安全防御，并建立联邦政府与先进人工智能模型开发商之间的自愿合作框架。该行政令历经波折后最终“面世”，反映出特朗普政府在人工智能治理政策上对技术创新与国家安全的复杂权衡。

①

②


③

图①：美空军XQ-58A无人战斗机。
图②：美海军“游骑兵”号无人水面舰艇。
图③：美陆军测试无人自主战术车辆。

构建交流监管框架

该行政令明确，对前沿模型网络不设强制许可或预先批准，但保留对其能力的评估机制。美国人工智能企业在公开发布前沿模型前，需“自愿”向政府提供模型并进行“前置安全评估”。

强化联邦与关键基础设施网络安全防御。行政令要求：国家安全系统委员会优先提升国家安全系统的网络防御能力；国防部加强自身信息系统安全保护；网络安全和基础设施安全局发布指令，加强联邦民用网络安全，推广人工智能辅助防御技术，并为州、地方政府及关键基础设施运营商提供网络安全工具和服务便利。此外，联邦官员可确定漏洞检测技术研发的拨款项目，同时拓宽网络安全专业人员的联邦招聘渠道。

设立人工智能网络安全信息交流中心。行政令指示美国财政部联合国家安全局、网络安全和基础设施安全局及其他联邦机构，共同组建该中心。中心以自愿合作为基础，联合人工智能企业与关键基础设施运营商，建立有组织的漏洞发现与修复机制。主要任务包括：协调漏洞扫描、验证已发现的漏洞、确定修复优先级等。

建立针对前沿模型网络能力的自愿评估机制。行政令在形式上维持特朗普政府“不干预创新”的立场，但实质上为联邦机构（特别是国家安全局）开辟了通过自愿渠道提前接触前沿模型的制度化路径。行政令要求相关机构在60天内制定一套保密的基准测试流程，用于评估人工智能模型的网络安全能力，以判定相关系统是否应被认定为“受覆盖的前沿模型”。

相比此前媒体披露的初始版本，行政令定稿最显著的变化是将自愿审查期限从90天缩短为模型发布后的30天内。根据相关要求，参与企业在将“受覆盖的前沿模型”提供给其他合作伙伴之前，可向美国政府提供最多30天的访问权限。业界应与政府合作，遴选“可信赖的合作伙伴”，使其能够访问指定模型，以加强关键基础设施网络安全，并在保密环境下开展网络威胁追踪。

新规折射多重考量

该行政令是特朗普政府在“创新优先”与“国家安全关切”之间妥协的产物。一方面，它放弃拜登政府时期及此前更广泛的监管思路，强调避免对创新产生“寒蝉效应”；另一方面，它承认先进人工智能系统可能带来网络安全风险，通过设立漏洞共享、能力评估和信息交流中心等机制，为联邦政府保留监督窗口。整体上，行政令将治理焦点从广泛的监管与安全议题，收缩至纯粹的网络安全与关键基础设施防护，体现了“去监管”政治承诺与安全需求之间的折中。具体表现在：

紧扣“美国优先”与全球人工智能霸权目标。行政令既依托政企自愿合作机制，借力企业模型提升美国关键基础设施网络防御能力，也为民用部门提供受保护的前沿模型；同时，通过“可信合作伙伴”遴选规则，试图构建由政府主导的外部认证体系，变相输出美式人工智能安全标准，形成准入门槛“小圈子”。

“自愿参与”与“硬性约束”并存。行政令多次使用“自愿参与”“非强制”“自愿合作”等表述，以降低企业界对监管的抗拒心理，避免过度监管。但若受管制前沿模型认证标准确立，将反向倒逼人工智能企业向政府及市场证明自身安全性与可靠性，使“软性约束”具备向“硬性标准”转化的条件。

变相深化人工智能领域的政企合作。行政令将主要落地机构设定为国家安全局与网络安全和基础设施安全局，意图通过前沿模型测试构建新型“人工智能军工复合体”，确保前沿模型使用权掌握在政府手中。同时，国家级信息交流中心的设立，便于在国家层面建立“以人工智能防人工智能”的共同防御体系。

在修订中力求平衡

特朗普政府将该行政令的发布时间从5月下旬推迟到6月上旬，内容多有精简和修订，主要出于多重考量。

平衡技术监管与战略压力。Mythos、ChatGPT等前沿模型，具备识别并利用关键基础设施系统漏洞的能力，有可能触及特朗普政府的“安全红线”。部分人工智能业界人士曾对特朗普施压，希望将90天的访问权限压缩至14天，白宫最终敲定30天作为折中方案。同时，特朗普政府还试图稳定人工智能发展进度，以开展所谓“大国竞争”。

平衡民众抗议。近期民调显示，约70%的美国受访者认为人工智能目前发展“太快”，51%的受访者对人工智能技术的发展应用前景和长期社会影响持悲观态度。美国“反人工智能”抗议活动出现政治化乃至极端化、暴力化倾向。特朗普政府此时推出行政令，意在通过技术监控来缓和民众对立情绪。

平衡政坛纷争。在当前的美国政坛，除民主党建制派主张严格监管人工智能外，特朗普政府及共和党内部也存在分歧：一派主张完全放任，扫除一切监管障碍；另一派则主张加强监管以防范风险。行政令既保留“自愿合作”这一基调，让放任派能够接受，又实质性地推动政府对高风险人工智能模型的监督，满足监管派的部分诉求。

后续落地有待观察

行政令出台后，美国近期的人工智能治理方向与范式已基本明确，引发广泛关注。OpenAI、安特罗匹克、谷歌等企业高管认为，这是“向前迈出的重要一步”，期待与白宫开展合作。OpenAI首席执行官奥特曼明确表示，该行政令取得了恰当的平衡，能在“保障开展最好模型的前提下，将网络工具交付给值得信赖的防御者”。消费者银行家协会、软件与信息产业协会、美国律师协会等行业组织也相继刊文以示支持。软件与信息产业协会认为，“自愿参与”这一框架设计有助于跳出强制监管陷阱，可成为美国联邦统一人工智能立法的基础。

美国政府重要智囊团外交关系委员会则从实际运行维度提出几点质疑。一是难以准确界定前沿模型。模型能力随微调和部署场景持续演化，涉密测评难以跟上技术迭代速度，标准过宽会导致监管泛化，过窄则会使高危模型漏过监管。二是落地资源存在缺口。美国联邦网安编制连年缩减，财政部跨界牵头组建网络安全信息交流中心、统筹跨部门测评，权责错位会造成落地效率不足。三是“自愿参与”机制的可持续性存疑。OpenAI等人工智能企业出于规避更强监管的考量大概率会配合，但开源社区、境外落地的小体量前沿模型游离于框架之外，难以实现全域风险管控。

欧盟推出技术主权一揽子方案

■李 海

欧盟技术人员检查网络。

6月上旬，欧盟委员会公布“欧洲技术主权一揽子方案”，提出加强人工智能、半导体、云计算等领域能力，以减少结构性外部依赖，增强欧洲数字自主性与韧性。

根据欧盟委员会发布的新闻公报，方案包括两项立法提案——《芯片法案2.0》和《云与人工智能发展法案》，以及“开源战略”“能源领域数字化与人工智能战略路线图”。相关立法提案在通过并生效前，还将由欧洲议会和欧盟理事会审议协商。

《芯片法案2.0》将依托欧洲在主流芯片方面的技术优势，加快尖端半导体技术能力建设，为人工智能应用提供先进算力基础。《云与人工智能发展法案》旨在扩充欧洲本土算力基础设施，计划在未来5至7年内将欧洲数据中心容量提高到目前的3倍，并加强“应用人工智能战略”在推动技术普及方面的作用。

“开源战略”将推动欧洲在云、人工智能、互联网技术、网络安全和半导体等优先领域扩大开源可选方案的规模，并支持公共行政部门更多使用开源方案，以培育“欧洲制造”的数字替代方案。“能源领域数字化与人工智能战略路线图”则旨在破解“算力狂飙”下的电力瓶颈，推动人工智能和其他数字解决方案在电力基础设施中的应用。

本套计划将建立“自主等级安全评估”认证体系，依据数据存储属地、服务商管控权限、供应链本土化程度和安全防护能力划分服务等级。其中，国防、医疗、政务涉密数据被纳入最高管控层级，相关数据须存储于欧盟本土可控服务器。在公共采购领域，推行欧洲本土优先原则。

上述一揽子方案是欧洲试图摆脱对美国技术依赖的举措。欧盟委员会执行副主席汉娜·维尔库宁表示，这标志着欧洲处理技术主权方式的重大转变。目前，欧洲的电子邮件通信、数据存储与处理及大量政府服务几乎都依托美国技术：德国政府每年向微软公司支付近6亿美元软件许可费，法国大型企业每年从美国科技公司采购的软件和云服务费用超过500亿美元，整个欧元区每年从美国进口的知识产权服务总额已达约2000亿美元。

更关键的是，美国《云法案》赋予美国政府调取本国企业存储在欧盟数据的权力，使欧洲国防与政府等敏感系统面临“一键窃密或被切断”的风险。布鲁塞尔技术前景研究所今年4月的报告显示：多个欧盟国家的国安系统高度依赖美国技术，其中16国被列为“可被美国紧急切断开关的高风险”类别。这种不安全感，是推动欧盟构建以《通用数据保护条例》《数字市场法》等为核心的自主规则体系，并推动主权云、开源软件迁移等措施的根本原因。

法国一直倡议欧盟将核心敏感数据移出美国服务器、扶持本土科创企业，此前应者寥寥。如今美国政策的不可预测性乃至威胁性，使多个欧洲国家重新审视法国的诉求。欧盟委员会主席冯德莱恩强调，欧洲决不能在核心技术上受制于人。欧洲数字中小企业联盟秘书长托法莱蒂称，技术早已超出普通商品范畴，是施加权力和影响力的手段，欧洲必须实现技术自主。

不过，美国仍可通过法律、技术和政治等手段影响和制约欧盟决策。除《云法案》这一法律长臂管辖工具，美国还利用技术路径依赖形成事实上的“锁定效应”，抬高系统迁移门槛；对欧盟内部呼吁强化数字主权的人士施加政治压力乃至实施签证限制，将技术争端升级至政治层面。这些组合拳使欧盟摆脱对美技术依赖步履维艰。此外，相关方案在欧洲内部也引发争议。欧洲数字产业组织“数字欧洲”认为，半导体价值链高度全球化，所谓“含欧量”要求难以操作，可能割裂供应链、削弱欧盟及其下游产业竞争力。

「奥库斯」核潜艇计划生变

■王成文

近日，美国、英国和澳大利亚在“奥库斯”框架下的核潜艇项目出现新动向。5月底，3国防长发表联合声明称，美国海军人员将于今年内开始轮换进驻澳大利亚西部；自明年起，最多4艘美国核潜艇和1艘英国核潜艇将部署至澳大利亚斯特林海军基地；澳大利亚将放弃采购全新核潜艇，改为采购3艘二手核潜艇。上述声明引发澳国内的广泛质疑。

首先是成本问题。澳政府估计，核潜艇项目总投入将高达3700亿澳元（约合2608亿美元），是澳历史上最昂贵、技术最复杂的国防项目之一。尽管澳防长马尔斯称项目总成本仅相当于该国GDP的0.15%，但对于仅有2700万人口的澳大利亚而言，这仍是庞大数字。此外，全新核潜艇换成“二手产品”后，澳方仅能节省有限的维护和运营成本，其向美国支付的巨额潜艇建造成本并未减少。

其次是产能问题。受供应链波动、造船设施老化、熟练工人短缺等因素制约，加之美国须优先保障自身哥伦比亚级战略核潜艇的生产，目前美国造船厂弗吉尼亚级核潜艇的年产能仅为1.1艘，而“奥库斯”原计划要求的年产能为2.33艘。产能提升困难，导致美国难以按时向澳大利亚供货。为保持水下威慑能力，澳大利亚只能斥资对原计划2025年陆续退役的现役柯林斯级常规潜艇进行“延寿”改造，使之延期服役。

目前，澳国内对核潜艇项目缺乏审查的担忧与日俱增，议会和公众纷纷要求参与相关质询、辩论和决策。6月2日，澳大利亚非营利组织“和平与安全论坛”发起针对核潜艇项目的公开调查，由5名澳前高官和知名人士组成专门委员会，重点审视项目是否损害澳主权和安全、能否按时在预算内交付、未来可能的核事故和核扩散问题，以及潜艇放射性废料处理等。

作为对核潜艇计划调整的补偿，3国宣布将共同研发先进无人潜航器，预计明年投入使用，用于保护海底光缆和管道等基础设施，并具备监视、侦察、打击、后勤保障等作战能力。评论人士认为，无人潜航器虽以低成本、长续航、易量产等特性，在一定程度上改变了海上作战规则，但也使海底成为高风险战场，误判与冲突概率大增，将给澳本国及地区安全带来负面影响。

据悉，在“奥库斯”框架下，澳方正投入巨资加快军事基础设施建设，以支持美英扩大在澳军事存在。有军事观察人士认为，美前沿军事基地的脆弱性已在近期的中东战事中充分暴露，澳防务深度绑定美国并非明智之举。

“奥库斯”联盟成员测试无人自主水面系统。

美日将在西太举行多场联演

■观山海

近期，日本防卫省宣布，将于6月下旬在西太平洋地区与美国举行“坚毅之龙2026”和“英勇盾牌2026”两场大规模联合演习。

“坚毅之龙2026”于6月20日至30日举行，重点检验日本自卫队和美军实施联合行动时的协调程序和互操作能力。日方参演力量以西部方面队为主，美方由驻冲绳的第3海军陆战远征军牵头。演习课目包括指挥所开设、情报侦察、反舰作战、反登陆、联合实弹射击、补给运输等。其中，陆上自卫队“鱼鹰”运输机将首次部署至宫古岛。

“英勇盾牌2026”于6月22日至7月1日举行，重点在西太平洋地区演练远洋反潜、海上封锁与联合制海等课目。日方由统合幕僚监部与统合作战司令部指挥，参演单位涵盖陆上总队及各方面队、海上自卫队自卫舰队、航空总队、航空支援集团和宇宙作战群等。

备受外界关注的是，美陆军第3多域特遣队所属“堤丰”中程导弹系统与“海马斯”多管火箭炮系统，将借6月至9月日美联演之机，临时部署至海上自卫队鹿屋航空基地。尽管日方称部署期间不实施实弹射击，但有消息披露，“堤丰”系统演习结束后将被转移至驻日美军基地存放。“堤丰”搭载的“标准-6”防空导弹和“战斧”巡航导弹，射程分别可达460千米和1800千米，若借此实现常态化驻留，将成为美国印太“分布式精确打击火力”部署的关键一步。

近年来，日本持续松绑进攻性武器研发与自卫队境外部署限制，主动开放本土及岛屿多处用地供美军扩建设施，配合美军完善第一岛链封锁布局。美日高频联演，反映出双方正将传统双边训练加速转向多域联合作战、岛链分布式部署、远程精确火力运用和战时后勤保障能力建设。其主要意图在于强化日本西南诸岛的前沿支撑属性，提升美日同盟在第一岛链的跨域协同和前沿威慑能力，并将日本民用机场、港口、自卫队基地和驻日美军设施深度嵌入美军西太平洋作战体系。此举将持续冲击亚太地区和平稳定。日本多个在野政党与民间团体已发起请愿与抗议，担忧日本沦为大国博弈前沿，增加本土安全风险。


美海军陆战队参加“坚毅之龙2025”演习。

社址：北京市西城区阜外大街34号 邮政编码：100832 发行电话：（010）68525572 每周一、二、三、四、五出版 全年定价150元 零售每份0.57元 承印单位：解放军报社印刷厂（地址同社址）