# 美发布新版国家网络战略

■王大宁


①

**3月7日，美国白宫发布新版《国家网络战略》报告（以下简称报告）。作为美国在网络空间的顶层设计文件，报告承接特朗普第二任期发布的《国家安全战略》和《国防战略》，以“美国优先、实力至上、进攻前置”为核心逻辑。评论人士称，此报告不仅是一份网络行动计划，更是一份立场强硬的政治宣言和国家动员令。**


②


③

④

图①：美军YFQ-44A无人战斗机。
图②：美军人员对网络基础设施进行检查。
图③：美军研发的便携式网络训练平台。
图④：美军测试无人水面艇。

从篇幅上看，报告仅有7页，远不及特朗普第一任期（2018年）和拜登政府（2023年）发布的版本（分别为40页和39页），实质性内容相对有限。不过，其明确的六大政策支柱，仍为美国后续网络空间的行动部署和资源配置提供了整体框架和优先方向。

## 确立六大政策支柱

一是塑造对手行为。这是报告中最具进攻性的部分，明确表示美国将采取各类网络攻防行动，并通过激励措施调动私营部门力量，共同识别并瓦解对手网络；在对手突破美国的网络系统前先发制人，削弱其能力、提高其行动成本；与盟友合作，为对手制造风险。

二是推行务实监管。报告对美国现行网络安全监管体系提出质疑，承诺将精简法规、减轻合规负担，赋予私营部门更大灵活性，以应对所谓快速演变的网络威胁。

三是升级联邦政府网络。报告提出将加快联邦信息系统现代化建设，包括推行后量子密码学、零信任架构和云转型，优先保障支撑军事情报的国家安全系统；采用人工智能赋能的网络安全解决方案加强防御，降低准入门槛，以便政府采购和使用最新技术，释放出一定采购改革信号。

四是保障关键基础设施安全。报告将关键基础设施的保护范围延伸至供应链，明确点名能源电网、金融系统、数据中心、医院和水务设施，并强调要排除来自对手国家的技术与产品，推广和采用本土技术。同时，推动各州协助联邦政府开展网络安全工作。

五是保持关键技术优势。聚焦于技术竞争的长期博弈，美国将在人工智能与量子领域“双线布局”，提出保护人工智能相关技术的安全，推广后量子密码学和安全量子计算的应用，加速推广生成式和代理式人工智能，以增强网络防御与干扰能力。

六是培养网络人才。报告将网络人才定位为战略资产，提出要通畅人才培养与交流渠道，扫清阻碍产业界、学术界、政府和军队协同培养高技能网络人才的障碍。

## 在继承中转向激进

这是美国自小布什政府以来发布的第4份国家网络战略报告。与此前版本相比，报告带有鲜明的特朗普第二任期施政逻辑，突出了3个转向。

一是总体基调从“攻防并重”转向“全面追击”。进攻性一直是美国网络政策的底色，但往届政府通常在表态和操作中有所保留。特朗普再度执政后，将网络进攻彻底摆上台面。报告明确提出，应对措施不限于网络领域，意味着美国将动用外交、军事、情报、金融甚至意识形态等所有国家力量回应所谓网络威胁，展现出“跨域报复和威慑”的思路。而“摧毁网络”“追捕黑客”“制裁公司”等强硬表述，更表明其政策已从“筑墙防御”转为主动出击、击败对手。

二是核心逻辑转向以“价值观”划线的技术阵营对抗。报告将技术问题高度意识形态化，试图在全球科技领域制造人为“鸿沟”。它将竞争对手定义为“兜售低成本人工智能和数字技术，却暗藏审查与监控”的一方，以此构建叙事框架，联合盟友在人工智能、量子计算等关键领域排挤对手的技术标准和产品，延续“小院高墙”策略。同时强调“规范和标准必须体现美国价值观”，实质是要掌握全球数字治理规则主导权，并将“隐私保护”作为打压对手技术的政治工具。

三是将安全与创新进行深度捆绑。报告虽宣称安全是创新的基石，但其六大支柱均试图解决同一问题：如何在保障网络安全的同时不扼杀技术创新。为此，它一方面承诺简化监管、释放创新活力，另一方面又要求私营部门“识别和破坏敌方网络”，并在平时和战时配合政府实施网络防御。这套组合拳的实质，是将科技企业的商业利益与国家安全深度绑定。

报告宣称，要为美国长期保持世界强国地位筑牢网络空间根基。其最终目标仍是维护美国在网络空间的技术优势乃至全球霸权，只是实现手段较以往更加激进：从被动防御转向“持续交锋”和“前置威慑”。它不仅将打击黑客、制裁企业和摧毁基础设施列为常规手段，还将“狩猎式防御”制度化，默许在预判威胁阶段就发起网络攻击，大幅降低了对别国发起网络行动的门槛。

## 折射多重调整动因

报告原定于今年1月发布，虽然有所推迟，但距上版（拜登政府2023年发布）尚不足3年。这是美国国家安全需求、全球格局变化与特朗普执政理念共同作用的结果，折射出美国意图重塑网络空间规则、摆脱国内治理困境的双重考量。

从外部看，全球网络安全格局正在加速重构，美国长期依赖技术霸权维持的网络秩序出现松动。人工智能、量子计算等新技术迅猛发展，深刻改变了网络安全的本质，衍生出的复杂问题加剧了美国的安全焦虑。美国试图通过“主动塑局”，维持自身在网络技术和规则制定上的主导权。

从内部看，美国在网络领域的积弊日益凸显。联邦机构职能重叠、效率低下，拜登政府时期繁冗的监管框架使科技企业陷入“合规泥潭”。与此同时，财政赤字高企、美债规模屡创新高，政府已无力独自承担大规模、高成本的网络防御体系建设，需要探寻更加高效的运行模式，以便借助企业技术激活政府能力，引导企业分摊安全成本。

报告还带有鲜明的特朗普个人色彩。作为奉行“利益至上”的现实主义者，特朗普采用“成本—收益”逻辑，追求“短平快”的战略利益。他将网络空间视为零和博弈的战场，认为被动防御难以形成威慑，进攻才是必要选项。这种思维模式直接将战略推向“务实逐利化”，催生出塑造对手行为的导向与一系列进攻性策略。

## 影响深远落地存疑

报告以主动进攻为手段、以技术优势为支撑、以盟友体系为依托，预计将对全球网络空间的力量平衡与安全格局产生深远冲击。

报告强调联合盟友分担安全成本、构建集体威慑，这将推动美国进一步整合盟友网络力量，打造以意识形态为纽带的网络安全“小圈子”，加剧全球网络空间的阵营对抗，形成“美式联盟”与多元博弈并存的格局，使跨国技术合作与协同治理更加困难。报告还将美国网络行动的进攻性推向新高，使网络空间逐渐演变为实战化博弈的新战场。这种态势下，“擦枪走火”的风险明显上升，国际网络空间规则与治理体系也可能陷入混乱，危及多国网络主权。

在运作机制上，报告强调跨机构协调、盟友责任分摊与公私合作，将给美国自身网络安全体系建设带来一系列变化。然而，有评论认为，新版战略能否落地，仍有待观察。据报道，当前美国相关网络机构和力量正经历“空心化”。过去一年，特朗普政府在政府效率部主导下对联邦网络安全领域进行大规模裁员，就连作为核心机构的网络安全与基础设施安全局也处境艰难，已流失超过三分之一、共计1000余名员工。在此背景下，这份战略的实际可操作性无疑要打上一个问号。

# 美召开拉美峰会「以盾筑篱」

『唐罗主义』升级加码

■王成文

3月7日，美国总统特朗普在佛罗里达州迈阿密主持召开一场名为“美洲之盾”的拉美峰会，邀请12个拉美国家领导人出席。这是特朗普第二任期以来首次面向拉美地区举办区域峰会，也是美国推进“西半球优先”战略、加紧经营美洲“后院”的重要举措。

此次峰会主要围绕安全与经济两大领域展开。安全方面，聚焦打击毒品走私和非法移民，力图构建所谓“美洲安全伙伴关系”；经济方面，则推动拉美国家优先与美国开展能源、农业与投资合作，以及构建关键矿产供应链。

特朗普提出的强化对西半球干预的所谓“唐罗主义”正在升级加码。峰会前夕，美国已在多个领域对拉美展开全面施压。军事上，继今年初突袭委内瑞拉后，2月中旬美国又主办首届西半球防务峰会，邀请34国军方高层参会，意图整合地区军事资源；经济上，对古巴实施石油封锁，施压墨西哥配合边境管控并加征关税；外交上，国务卿鲁比奥高调出席加勒比共同体峰会，推销美方政策。这些举动正串联成美国操控拉美局势的一张大网，而此次峰会则成为这张网络中又一关键节点。

为强化对西半球的影响力，特朗普在邀请对象的遴选上可谓“煞费苦心”。

在政治光谱上，受邀国家领导人均来自右翼阵营，而巴西、墨西哥、古巴、尼加拉瓜等左翼执政国家均未被邀请，即便是与美国关系有所回暖的哥伦比亚也被排除在外。这并非偶然，而是特朗普有意在拉美拉“小圈子”、推行“阵营化”，意图巩固右翼联盟、孤立打压左翼国家，阻碍拉美地区一体化进程，进而推动拉美政治继续右转、强化美国主导的“代理人秩序”，确保相关国家在内外政策上与美国保持一致。

在资源禀赋上，受邀国大多矿产资源丰富，如由阿根廷、玻利维亚、智利组成的“锂三角”，能够为美国军工和新能源产业提供关键原材料，增强其在电池制造和武器生产方面的优势。美国还以市场准入和关税优惠为筹码，诱使这些国家在矿产、能源、基建等领域向美倾斜，重塑以美国为中心的依附型经贸链条。

在安全合作上，美国以禁毒、反恐、反移民为“外包装”和切入点，意图与此前启动的“南方之矛”军事行动形成一守一攻、互为支撑的战略组合，推动拉美国家配合美国实施边境管控、共享情报、开放军事准入、升级防务协议，将西半球打造成一个隔绝外部影响的“安全堡垒”。显然，“筑墙排他”的所谓“美洲之盾”，其真正护卫的对象并非拉美国家，而是美国的本土安全与霸权地位。

在中东局势引发国内外争议的背景下，特朗普试图在拉美取得外交成果，为即将到来的美国中期选举造势、提振选情。不过，此次峰会的实际成效并不被普遍看好。历史上，美国针对拉美地区曾推出多项计划和倡议，但往往“口惠而实不至”，鲜有真正落地。如今，特朗普试图构建狭隘的小多边合作机制，与拉美国家追求自主发展、推动区域团结、开展平等多元国际合作的诉求相悖。此前拜登政府推出的仅覆盖部分拉美国家的“美洲经济繁荣伙伴关系”成效有限，便是前车之鉴。逆区域潮流而动、构筑藩篱的“美洲之盾”，恐难逃类似结局。


美军CH-53运输直升机参加在拉美地区的军事演习。

# 日本申请加入北约防务项目

■观山海

据日本媒体报道，3月上旬，日本政府向北约提出申请，请求加入该组织的国防技术项目“防务创新加速器”（DIANA）。如果日方请求得到批准，日本将成为首个加入该项目的非北约国家。

北约DIANA项目被定位为“北约版DARPA”，名义上旨在“加速包括人工智能、网络、量子及其他军民两用技术的发展”，实则是以美国为首的北约孵化前沿防务科技、抢占未来军事斗争制高点的重要平台。该项目于2021年在北约布鲁塞尔峰会上正式启动，2023年具备初始运行能力，目前已覆盖人工智能、量子技术、网络空间、自主无人系统、太空安全等七大颠覆性技术领域。其仅面向北约32个成员国的企业开放，若允许日本企业加入，将标志着该项目首次向北约以外的国家开放。

日本申请加入DIANA项目，目标清晰，路径明确。

其一，突破技术瓶颈，尽快补齐军事化短板。加入DIANA项目，有助于日本直接对接北约的训练数据库、仿真测试环境和联合作战标准，快速提升反潜、反舰、防空及情报分析等领域的智能化水平。日本试图以“技术合作”为名，行“扩武结盟”之实，将自卫队打造成“颠覆性技术密集型”力量，进一步摆脱装备与能力限制，冲击“战后体制”束缚。

其二，突破身份限制，实现“准北约成员”地位跃迁。近年来日本步步为营：从成为北约“全球伙伴国”，到常态化出席北约峰会；从正式加入北约合作网络防御卓越中心，到参与北约为乌克兰设立的“综合援助计划”，直至此次申请加入DIANA项目。一连串动作环环相扣，意在实质性实现与北约的“全链条嵌入”式防务合作，助力自卫队向“可对外参战、可联盟作战”的常规军事力量转型。

其三，突破地理界限，牵引“欧洲—印太”跨区域安全联动。日本反复强调欧洲与印太安全不可分割，极力充当北约印太化的桥头堡，助推北约将防务触角伸向亚太，把本地区热点问题强行纳入西方阵营议程。北约则可借助DIANA项目平台对非北约国家开放，将“印太化”口号落地，以“技术跨洋延伸”替代“成员跨洲扩张”，用“创新网络抓手”牵动“阵营深度整合”。

日本与北约在防务技术领域的全面耦合与彼此捆绑，将重塑亚太乃至全球军事技术竞争格局，加剧全球科技的阵营化风险，最终损害自身与本地区的共同安全。亚太地区的未来，在于对话而非对峙、合作而非结盟、开放而非壁垒。科技不应也不能沦为军备竞赛乃至军事扩张的工具。

### 技术霸权踏破伦理底线

# 洞察美军与AI企业的分合玄机

■李 海

美国国防部近期对两家本土人工智能企业采取了截然不同的态度，引发外界关注。一边将安特罗匹克公司列入供应链风险名单，并单方面终止合作合同；另一边则迅速与OpenAI达成深度合作。这一鲜明反差，折射出美国军方在推进人工智能军事化进程中，对技术伦理与企业自主权的强硬姿态。

据外媒3月6日报道，美国国防部以“构成供应链风险”为由，将安特罗匹克公司及其人工智能模型Claude列入黑名单，并终止双方价值2亿美元的合同。值得注意的是，这类标签通常针对外国企业。几乎同一时间，OpenAI迅速“补位”，宣布接受美国政府所有合作条件，并与国防部达成协议，将其先进人工智能模型部署于军方机密网络。

回溯美军与两家公司的合作历程，这一反差尤为耐人寻味。2025年夏季，美国国防部主动与安特罗匹克公司展开合作，后者一度成为军方最倚重的人工智能合作伙伴，其Claude模型也是唯一获准进入美军涉密网络的商业大模型。然而仅半年后，形势急转直下，因该公司拒绝移除模型中的两项安全限制，即禁止用于国内大规模监控和全自主致命武器，国防部不仅终止合作，更罕见地将其等同于外国企业处置。与此形成对比的是OpenAI的迅速转身。这家曾明确反对与军方合作的企业，自2024年起逐步放宽立场，最终在此次事件中完成从技术创新企业到军方重要伙伴的转变。

这一系列动作并非孤立事件，而是美国国防部推行人工智能“无限制军事化”原则的集中体现。美国今年1月发布的“人工智能加速战略”明确提出，要将美军打造为“人工智能优先”的作战力量，让人工智能从辅助工具上升为贯穿情报、指挥、杀伤、保障全流程的核心支柱。为实现这一目标，军方要求技术供应商无条件服从作战需求，清除任何可能阻碍军事应用的伦理限制。

美国国防部将安特罗匹克公司列入黑名单，意在杀鸡儆猴，迫使整个人工智能行业接受“作战优先、伦理让路”的规则，为发展“自主武器、全域监控、智能杀伤链”扫清制度和舆论障碍。讽刺的是，尽管Claude模型在美国国内被封禁，但在美国近期的中东军事行动中，该模型据称仍在发挥作用。

这场风波揭示了美国科技领域政企关系的潜在逻辑：当国家利益与霸权目标被置于首位，即便再顶尖的技术、再有原则的企业，也必须俯首听令，任何坚持伦理底线的行为都可能被排除在合作之外。有分析认为，讲求“安全与伦理”的企业受罚，迎合退让者获订单，这种“逆向激励”或导致行业伦理底线全面失守。当权力可以左右技术方向，当霸权可以撕裂伦理底线，人工智能军事化的失控风险将与日俱增。

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）