战略与安全
SECURITY & STRATEGY
清华大学战略与安全研究中心
CENTER FOR INTERNATIONAL SECURITY AND STRATEGY TSINGHUA UNIVERSITY

CISS 海外信息专报

（2026 年 8 月 5-7 日）

1、英国国际战略研究所：人工智能压缩核决策时间加剧国际战略风险

7 月 31 日，英国国际战略研究所（IISS）发表斯坦福大学国际安全与合作中心研究员特隆德·阿恩·温德海姆（Trond Arne Undheim）的文章《无控制的核指挥：人工智能与升级不透明性问题》。文章认为，中美俄等国正将人工智能技术融入核指挥、控制与通信系统（NC3），这可能会压缩决策时间并削弱人类对核武器的实质控制。文章认为，人类避免军事灾难的关键在于拥有充裕的决策时间进行场景判断，但人工智能技术应用将系统反应时间从 15 至 30 分钟缩减至 5 分钟内，使人类退化为被动批准机器建议的附庸。同时，因军事人工智能系统的底层限制逻辑不可见且难以验证，各国无法判断对手系统在危机中的推荐意图，从而引发信任崩塌，迫使各国加速人工智能武器化应用，陷入恶性循环。随着中等强国进一步发展军事人工智能武器，多极环境下的误判风险陡增。文章建议，各国必须在 2025 至 2035 年这一现代化窗口期将战略决策时间作为核心变量，建立以算法验证、技术信任与强制人工干预为核心的治理框架，重新夺回人类对核

指挥的控制权。

https://www.iiss.org/online-analysis/survival-online/2026/07/nuclear-command-without-control-ai-and-the-problem-of-escalation-opacity/

编译：孙韵雯

2、美国 CSIS：前沿人工智能治理方式趋同而范围分化

8 月 3 日，美国战略与国际问题研究中心（CSIS）发表欧洲议会社会党政治顾问劳拉·卡罗利（Laura Caroli ）与瓦德瓦尼人工智能主任阿洛克·梅塔（Aalok Mehta）的研究报告《迈向联邦框架：来自州和国际前沿人工智能监管的经验教训》。报告认为，美国州级立法与欧盟及行业自律规范已经形成“治理方式趋同、治理范围分化”的格局，并且州级经验可为未来联邦框架提供重要基础。具体而言，安全框架的制定与公开、风险评估以及风险缓解已成为普遍接受的治理基线，安全防护措施与举报人保护也获得广泛采纳，其中第三方评估要求在不同法案间反复增删，反映各方尚未就独立审查的必要性达成共识。这种趋同并非欧盟规则外溢所致，而是学界专家、产业代表与民间组织持续参与多个立法进程、在互动中协同演化的结果。然而，各框架在治理对象上仍存在显著差异，涵盖模型覆盖范围、责任主体界定、风险类别划分以及灾难性风险界定标准。欧盟采取了范围更广的监管思路，美国州立法则逐渐收缩为对大型模型开发者施加较为

有限的义务。目前形成的治理共识仍是各方能接受的最低标准，尚不足以真正应对灾难性风险，持续性的事后监督与透明披露机制应与预部署审查相互补充，共同构成完整的治理体系。

https://www.csis.org/analysis/toward-federal-framework-lessons-state-and-international-frontier-ai-regulation

编译：杜宛鸿

3、美国兰德公司：人工智能应急产品供给失衡

8 月 4 日，美国兰德公司发表高级政策研究员杰西卡·詹森（Jessica Jensen）、全球国防研究员格伦·伍德伯里（Glen L. Woodbury）等学者撰写的研究报告《人工智能与应急管理未来：市场供给与落地路径》，系统梳理全美适配应急场景的人工智能产品现状。研究发现 1179 款相关产品市场供给分布极不均衡，近半数产品为通用人工智能工具，并非专为应急场景定制，单一产品只能覆盖局部业务，完整处置流程需要多款工具叠加使用，大幅抬高部署成本。产品落地存在多重硬性门槛，约五分之一人工智能工具属于配套组件无法独立运行，超七成依赖持续网络连接，在断网环境下难以使用；多数厂商不公开定价，缺少全天候技术支撑，同时几乎所有产品都存在用户隐私数据处理风险，并缺少合规认证。地方、部落应急部门普遍受资金、技术人员、IT 基建限制，人工智能普及进度远慢于公用事业、医疗机构等关联单位。报告提

出分阶段行动方案，建议搭建全国人工智能应急产品评估平台、分层培训体系与跨行业协作联盟，打通技术供给与基层应急落地的壁垒。

https://www.rand.org/pubs/research_reports/RRA4625-1.html

编译：钟珺雯

4、美国兰德公司：用于安全工程垂直整合的安全推理数据中心策略

8 月 4 日，美国兰德公司发表其高级人工智能安全研究员史蒂夫·科默（Steve Comer）等人的文章《安全推理数据中心：一种用于安全工程的垂直整合策略》。文章认为，前沿人工智能系统的快速迭代，使得模型盗窃、操纵与误用风险日益加剧，而普通商业云环境难以满足高安全性部署需求。为此，文章提出“安全推理数据中心”（SIDC）策略，在高风险环境中确保已训练模型在推理阶段的机密性与完整性。该策略的核心优势在于：使用经过验证的现有商用硬件即可实现，无需基础研究突破；安全设计与模型本身及硬件堆栈无关，具备良好通用性。SIDC 的典型应用包括：保护国家安全环境中商业人工智能系统的机密性与完整性；应对战略性或生物技术等危险性能力出现时的紧急托管需求；以及作为开发高安全训练数据中心的试验场。设计上，SIDC 遵循“从概念到电路”的垂直整合思路，采用面向系统的安全分析方法（STPA-Sec），从不可接受的损失倒推确定安全约束，并将其

逐级转化为具体需求与实现机制，最小化功能冗余，并通过形式化验证等手段确保关键组件的可信性。早期部署须聚焦三项工作：尽快确定实施机构并启动详细工程设计；尽早选择应用场地，优先利用现有政府设施以压缩工期；立即对形式化验证协议和单向数据流等关键安全组件进行原型测试，以降低技术风险并避免后续延误。

https://www.rand.org/about/people/c/comer_steven_f.html

编译：张佳延

5、卡内基国际和平基金会：人工智能制造环境性不确定性，助长暴行否认

7 月 30 日，卡内基国际和平基金会官网发表前牛津大学高级信息控制研究员马莎 •阿利马尔达尼（Mahsa Alimardani）与数字人权组织 DeCenter 创始人阿夫萨内 •里戈特（Afsaneh Rigot）的文章《生成式人工智能与战争中的暴行否认》。文章认为，部分国家正在借助人工智能在战争中制造环境性不确定性，也即通过制造让一切事实都变得值得怀疑的信息环境以否认战争暴行。生成式人工智能将公众的怀疑心理武器化。人工智能生成的谎言不必加以核实，由此引发的怀疑心理即可让受众质疑真相。文章认为，当前的任务是保护记录暴行的人以及那些确保他们的证据能够完整传递的过程，以便真实的记录在受到伪造指控前得以保存。一方面，应保证暴行记录过程能够安全进行，借助数字工具支持证据采集、加密

存储和安全传播，同时加强隐私保护和风险防范，降低见证者面临的人身安全危险。另一方面，应建立多层次信任机制，完善内容来源与真实性验证机制，并强化内容全生命周期的跟踪管理，以提升暴行证据的可信度与可验证性。

https://carnegieendowment.org/research/2026/07/generative-ai-and-atrocity-denial-in-war

编译：程果

6、美国布鲁金斯学会：海外人工智能数据中心带来国家安全风险

8 月 3 日，美国布鲁金斯学会发表人工智能与新兴技术倡议副主任德里克·贝尔（Derek Belle）与人工智能与新兴技术倡议主任埃尔哈姆·塔巴西（Elham Tabassi）等人的文章《在海外建设前沿人工智能数据中心对国家安全的影响》。文章认为，前沿人工智能基础设施选址正由商业决策转为战略选择，美国需在经济竞争力与国家安全之间重新权衡国内外算力中心布局。受电力、电网接入、审批及地方反对等因素制约，美国算力基础设施或向海外转移，但由此将产生四类风险：一是芯片、训练数据、专有软件和模型权重等资产可能遭到窃取或破坏；二是设施受东道国法律监管，面临数据披露和运营干预；三是长期依赖境外设施可能赋予东道国对美结构性影响力；四是地缘政治不稳定地区的数据中心存在物理安全风险。文章强调，美国应根据工作负载、所有权、

运营控制及东道国战略契合度确定海外部署条件，并通过技术、合同和外交手段降低风险。

https://www.brookings.edu/articles/the-national-security-implications-of-building-frontier-ai-data-centers-overseas/

编译：高美琳

7、美国兰德公司：美公众对医疗 AI 认知提升却信任退化

8 月 3 日，美国兰德公司发表由哈佛医学院麻醉学助理教授本杰明·雷德（Benjamin Rader）等撰写的研究报告《美国成年人口结构和政治认同对医疗保健领域生成式人工智能认知趋势》，比较了 2023 年 5 月与 2025 年 11 月两项全国性调查，分析美国成年人对医疗领域生成式人工智能的认知与态度变化。两项调查分别覆盖 3130 名与 3088 名受访者，通过 Outbreaks Near Me 平台收集数据。结果显示，美国公众对生成式人工智能的认知度近乎翻倍，自称频繁听说相关讨论的比例从 2023 年的 26.5%升至 2025 年的 42.9%。但认知提升并未转化为接受度增长。对人工智能主导初级诊疗和治疗表示认可的受访者比例几乎没有变化，仅分别下降 1.0 与 0.7 个百分点；认为人工智能在诊断和避免偏见方面优于临床医生的看法同样停滞。不同群体的态度走向出现显著分化。共和党受访者在四项指标上均更趋正面，民主党受访者则全面下滑，两党立场在 2025 年发生逆转。18 至 34 岁群体认知度增幅最大，却对人工智能主导诊疗的接受度下降最多。亚

裔与太平洋岛民受访者对人工智能诊疗的评价趋向负面，西班牙裔对人工智能主导治疗的接受度下降 12.0 个百分点。结论认为，医疗人工智能的信任并未随曝光自然增长，反而正沿党派身份和人口学特征固化。若政策制定者和医疗系统在推广人工智能时不加以针对性的信任建设，可能加剧而非缩小现有的健康不平等。

https://www.rand.org/pubs/external_publications/EP71364.html

编译：张方琼宇

8、美国《外交事务》：“后新自由主义”时代的贸易平衡构想

8月5日，美国《外交事务》网站发表公共公民组织（Public Citizen）全球贸易观察创始人兼前主任洛丽·沃拉赫（Lori Wallach）的文章《贸易平衡的正确方式：新自由主义秩序之后何去何从》。文章认为，新自由主义贸易体系未能带来预期的全球繁荣与安全，反而加剧经济不平等、产业失衡和供应链脆弱。当前，中国长期贸易顺差与美国混乱的关税政策共同推动旧贸易秩序危机，未来应建立以贸易平衡、公平竞争以及劳动、环境标准为核心的新贸易体系。首先，文章批评新自由主义贸易体系偏向大型跨国企业利益。20 世纪 90 年代以来的贸易规则从传统关税扩展至服务监管、知识产权、政府采购、数字贸易等领域，限制各国产业政策空间，强化垄断企业优势。其次，现行贸易体系导致全球失衡加剧。中国、德国等经济体长期贸易顺差，全球失衡具有结构性特征，

美国长期贸易逆差则导致其制造业衰退。由此，文章提出“后新自由主义贸易体系”方案，主张以贸易平衡为目标，允许成员国降低内部关税、提高外部关税，并通过汇率、资本管理等方式调整失衡；且各国应保留产业政策空间，通过关税配额和反补贴机制支持国内产业。新贸易秩序还应纳入劳动、环境和反垄断标准，以避免企业通过降低劳工和环境标准获得竞争优势，并限制大型企业垄断市场。文章强调，美国未来仍可凭借市场优势推动新的贸易规则。

https://www.foreignaffairs.com/united-states/right-way-balance-trade

编译：贺宇希

9、美国 CFR：美国为何出手干预托举日元汇率

8 月 4 日，美国对外关系委员会（CFR）发表其专家布拉德·W·塞策（Brad W. Setser）的文章《美国为何出手干预托举日元汇率》。文章认为，美财长贝森特 8 月 3 日证实美国于 7 月 31 日出售欧元储备买入日元，称其旨在遏制汇率波动、降低亚洲市场风险，并强调稳定的日元不仅对美国乃至整个地区至关重要。这是美国自 2011 年以来首次与日本联合干预汇市，此前日元上月刚触及四十年低点。作者称，此类行动极为罕见，美国上一次支持日元还是在 1998 年亚洲金融危机期间，而 2011 年干预方向相反。尽管财政部拥有干预汇市的法律权限，但过去几十年通常避免此类操作。就

战略收益而言，该行动至少暂时阻止了日元进一步贬值可能带来的破坏性风险。日元疲软会施压其他亚洲货币，也可能使中国难以继续允许人民币缓慢升值。所有亚洲货币普遍偏弱，这与特朗普政府再工业化的目标相悖。关于日元和日本经济前景，作者认为围绕日元疲软存在过多负面情绪。日本经常账户有可观顺差，政府拥有大量外部资产，净债务相对GDP趋于下降，财政赤字约占GDP的1%，今年有望实现基本财政盈余，经济基本面好于美国。日本真正需要的是日本央行提高政策利率。最终，重建可信的干预威胁和一系列加息应能稳定日元，日元已严重超跌，偏离基本面。此外，日本投资者若改变对冲其庞大海外资产的态度，也可能为日元带来实质支撑。

https://www.cfr.org/articles/why-the-u-s-intervened-to-prop-up-japans-yen

编译：王一凡

10、报业辛迪加：特朗普“中美G2”构想冲击亚洲安全格局

8月3日，报业辛迪加网站发表新德里政策研究中心战略研究部名誉教授布拉马·切拉尼（Brahma Chellaney）的文章《中美G2格局对亚洲安全意味着什么》。文章认为，特朗普近期大力宣扬的“G2”概念是一个高度不稳定的构想，这可能会增加“单极亚洲”格局出现的可能性。文章认为，该构想与培育广泛合作伙伴网络来维护稳定的“自由开放的印

太”战略不同，主张仅由美国和中国通过直接谈判来塑造区域与全球秩序，本质是以牺牲多边外交为代价推动双边交易，从而削弱中等国家的战略权重，进而降低美国的影响力。文章认为，特朗普政府系统性降低了四边机制（Quad）的优先级，最新的国家安全战略仅对该机制一笔带过，美国国防部也将原先的“印太”表述改回“太平洋”，表明美国原本推行的自由开放印太战略正在逐步瓦解。同时，日本面对这一严峻风险，进一步坚持自由开放的印太愿景，将印度作为印太架构中不可或缺的核心支柱。文章强调，特朗普政府将“印太”表述中的“印”移除、推行 G2 构想，对中国而言是标志性的地缘政治胜利。因此，避免亚洲形成单极格局的关键在于维持自由开放的印太框架，这一目标需得到广泛民主国家联盟的共同支持。

https://www.project-syndicate.org/commentary/trump-g2-concept-is-far-inferior-to-the-free-and-open-indo-pacific-vision-by-brahma-chellaney-2026-07

编译：李泓静

11、美国《国家利益》：无人机时代美军优势面临挑战

8 月 4 日，美国《国家利益》网站发表国家安全商业领袖协会（Business Executives for National Security）副主席拉蒙 • 马克斯（Ramon Marks）的文章《为何美国仍未准备好迎接无人机战争新时代》。文章认为，在霍尔木兹海峡与伊朗的

对抗中，美军正面临高技术无人机和精确制导导弹的严峻挑战。此前在红海与胡塞武装的较量已预示了这一问题，即便动用两个航母战斗群，商业航运量仍下降 50%，保险费用飙升，战略效果并不显著。文章认为，美国自二战以来依靠“抵消战略”维持技术优势，核威慑为第一次，侦察打击复合体为第二次，人机协同与人工智能为第三次，但第三次尚未在实战中取得决定性成果。相反，伊朗已发展出射程 900 英里的海巴尔·谢坎弹道导弹和成本仅 3 万美元、射程 1600 英里的“见证者”无人机，能用数量优势压倒美军的昂贵防空系统。美军用数百万美元的拦截弹打击数万美元的无人机，这种成本模式不可持续。虽然五角大楼正紧急推进新系统和战术，如为驱逐舰改装反无人机装备、空军探索无人机与 F-35 协同作战，但从零开始构建全面的无人机与导弹作战优势尚需时日。如果不能有效应对这些威胁，冲突和多极不稳定将不可避免地扩散至其他地区。

https://nationalinterest.org/feature/why-the-us-still-isnt-ready-for-the-new-era-of-drone-warfare

编译：白一冰

12、美国“堡垒”网：伊朗战争削弱特朗普海湾人工智能战略

8 月 3 日，美国“堡垒”时评网站发表卡内基国际和平基金会研究员阿拉斯代尔·菲利普斯·罗宾斯（Alasdair

Phillips-Robins）和萨姆·温特·利维（Sam Winter-Levy）的文章《伊朗如何摧毁特朗普的海湾人工智能协议》。文章认为，特朗普政府推动向阿联酋出口先进人工智能芯片、支持其建设大型数据中心，同时对伊朗发动军事行动，削弱了海湾人工智能合作的经济基础。此后，美国又取消对阿联酋先进芯片及敏感技术出口限制，在未获得相应回报的情况下放弃了原有谈判筹码。文章认为，2025 年 5 月特朗普政府批准在阿联酋和沙特建设大型人工智能数据中心，并承诺芯片出口以严格安全措施为前提。但协议推进过程中，出口许可审批迟缓，围绕安全要求和投资承诺的谈判陷入僵局，相关合作进展受阻。文章认为，对伊朗发动军事行动进一步削弱了海湾人工智能项目的可行性。战争导致外国技术人员撤离、供应链受阻、保险成本上升，伊朗还袭击了亚马逊在阿联酋和巴林的数据中心，并威胁打击 OpenAI 在阿联酋建设的“Stargate UAE”项目，使海湾地区建设和运营大型人工智能基础设施面临更高风险。特朗普政府随后取消了对阿联酋先进人工智能芯片及其他敏感技术出口的限制，使阿联酋能够采购大量芯片、建设大型数据中心并部署先进模型，而美国并未获得新的安全承诺、技术转让限制或阿联酋调整对华关系等交换条件。文章认为，此举削弱了美国对先进人工智能技术的控制力，也增加了关键技术泄露风险。文章最后指出，特朗普政府最终在未获得相应回报的情况下放弃了美国在人工智能领域的重要战略筹码。

https://www.thebulwark.com/p/how-iran-blew-up-trumps-gulf-ai-deals-uae-united-arab-emirates

编译：罗方婕

13、美国《外交事务》：武力难以给中东带来稳定秩序

7 月 30 日，美国《外交事务》网站发表得克萨斯农工大学荣誉退休教授 F·格雷戈里·高斯三世（F. Gregory Gause III）的文章《新旧中东：声怒之战》。文章认为，尽管经历了一系列看似剧烈的冲突与政权更迭，但中东地区的深层结构和根本矛盾并未改变。伊朗在遭受重创后，通过反制措施成功保住了政权并在地区博弈中重获主动；海湾国家依然在美伊之间寻求艰难平衡；黎巴嫩、叙利亚等阿拉伯国家软弱分裂，无法有效管控非国家武装，导致外部势力持续干涉；以色列虽然削弱了哈马斯、真主党等代理人，但并未解决根本的政治争端，反而因拒绝巴勒斯坦自决和加速吞并西岸而使自身陷入无休止的冲突循环。文章认为，中东实现稳定的关键在于加强阿拉伯国家的中央集权，终结外部势力资助民兵组织的企图；与伊朗达成包含核问题与霍尔木兹海峡管理的可持续共存模式的外交努力；以及美国必须向以色列施压，推动兼顾以色列安全与巴勒斯坦自决的政治解决方案。若无这些根本性改革，近年的战乱仅是旧有矛盾的延续，真正的和平依然遥不可及。

https://www.foreignaffairs.com/middle-east/new-old-middle-

east-gause

编译：陆知宜

14、美国 CSIS：美国应以“词元政治”统筹对华全球 AI 竞争。

8 月 3 日，美国战略与国际问题研究中心（CSIS）发表未来实验室主任、国防与安全部高级研究员本杰明·詹森（Benjamin Jensen）与该实验室副主任、数据研究员亚西尔·阿塔兰（Yasir Atalan）的文章《词元政治：美国如何与中国竞争构建全球 AI 技术栈》。文章认为，全球 AI 竞争已从模型和芯片延伸至能源、算力、数据中心和应用等全栈体系。词元（Token）是 AI 处理和生成信息的基本单位。谁能以更低成本、更高效率生产词元，谁就可能占据未来国际体系制高点。中国正通过产业政策、国家资本和算力补贴推动 AI 全栈发展，并以低成本开放权重模型扩大国际影响。华为还依托电信网络，向全球南方提供数据中心、云服务和芯片等整体方案。美国虽拥有领先企业和资本市场，也已推出 AI 出口计划、硅和平计划及融资工具，但政策仍较分散。文章主张，美国应制定“多元政治”大战略，由国家安全委员会和国家经济委员会牵头，统筹国务院、商务部、财政部及开发金融机构。美国还应联合盟友和私营企业，在全球南方建设电力、电网、海底电缆和数据中心，并加强对中国 AI 产业融资、技术转运和芯片走私的监测。

https://www.csis.org/analysis/tokenpolitik-how-united-states-can-compete-china-build-global-ai-stack

编译：黄千茹

15、美国 CFR：美选民普遍担忧中期选举公正性

8 月 3 日，美国对外关系委员会（CFR）发表美国外交政策杰出高级研究员詹姆斯·M.林赛（James M. Lindsay）的文章《选民担忧美国选举公正性》。文章认为，一项盖洛普民调显示大量美国选民担忧 11 月的选举无法做到自由和公正：67%的选民担心政治领导人向选举官员施压以改变选举结果，57%担心选票无法得到妥善处理、清点或保护，52%担心投票站附近出现选民恐吓，50%担心个人选票无法被计入。其中，共和党人最担心选票处理和计票问题，而民主党人和独立选民最担心政治压力改变选举结果。文章认为，由于过去民调机构很少持续调查选举公正问题，因此难以将数据进行历史比较，但这本身表明，直到最近，选举公正性似乎才成为重要政策议题。选民的担忧未必会成为现实，因为传统的法律、规范和程序仍将发挥作用。但文章认为，民主建立在被统治者同意的基础上，如果公众怀疑选举结果能否反映其意愿，民主制度就无法正常运转。

https://www.cfr.org/articles/voters-worry-about-election-integrity

编译：刘盈祺

16、美国 CSIS：北美供应链陷“可见性鸿沟”，转口规避成中国产能过剩新通道

8 月 4 日，美国战略与国际问题研究中心（CSIS）发表美洲项目研究员迭戈 •马罗金 •比塔尔（Diego Marroquín Bitar）的文章《可见性鸿沟：人工智能如何阻止美墨加协定下的中国转运》。文章认为，美国海关对货物原产地的验证长期停留在“标签层”，而非追溯其钢、锂、半导体的真实来源。这一“可见性鸿沟”正被中国所谓“产能过剩”利用，通过第三国转口、贴标规避关税，侵蚀北美工业基础。关税等粗放工具仅将贸易流转向别处，无法穿透供应链。标签失灵的直接后果是合规企业与不良行为者被同等对待。北美三国海关互认贸易信任计划、钢铁“熔炼浇铸地”追溯规则、私营部门与政府风险系统的对接试验，正通过分散化实践而非统一蓝图，缓慢构建起供应链透明化基础设施。文章建议，USMCA 审查窗口应成为将零散试验转化为共享政策的契机，并提供四点方案：协调三国贸易数据分类，避免“数字碎片化”；将互认范围从安全审查扩展到原产地与采购数据验证；政府设定可认证标准而非自行搭建平台；标准需覆盖设计与出口环节的中小企业，避免仅大型企业受益。而数字产品护照则可作为解决电动汽车电池等复杂供应链问题的方向。

https://www.csis.org/analysis/visibility-gap-case-north-american-trusted-trade-laboratory

编译：黎彤

编译：陆知宜、黄千茹、郜捷、刘盈祺、黎彤、贺宇希、王一凡、刘晓、李泓静、白一冰、罗方婕、孙韵雯、杜宛鸿、钟珺雯、张佳延、程果、高美琳、张方琼

审核：许嘉伦、钱嘉童、刘源、郑乐锋、周武华、申青青