CISS 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 13-14 日）

1、美国《法律战》：人工智能宪政主义需从实验室治理走向公共参与

8 月 6 日，美国《法律战》（Lawfare）网站发表其高级编辑、得克萨斯大学法学院人工智能创新与法律项目主任凯文·弗雷泽（Kevin Frazier）的文章《人工智能宪政主义的新研究议程》。文章认为，当前主要人工智能宪法制定与执行主要由人工智能实验室闭门开展，缺乏第三方监督和充分的公共参与，私有模式下的人工智能宪政主义需转向更具公共参与性的民主治理路径。随着人工智能系统自主性提高、人类监督逐渐减少，人工智能模型内嵌的价值观将以用户难以察觉的方式塑造用户的认知与决策。人工智能宪法载明引导模型对齐目标的价值、原则与适用规则，为模型行为搭建基础框架，具有通俗易懂、影响广泛、可持续修订等特点，因此有潜力成为治理工具。然而，当前领先实验室均承认，模型尚不能完全遵循既定价值准则，价值选择与合规验证的裁量权仍主要保留在实验室内部，同时企业出于安全考量，不愿完整公开对齐训练细节，防范被恶意利用。更重要的是，即便模型遵循程度提高，仍需要回答一系列核心问题：模型应

当遵循何种价值、由谁选定、程序如何获得正当性，以及价值冲突时如何裁决。对此，文章提出两种研究思路：人工智能宪政主义不必执着寻找一套普遍适用的“正确价值”，可着力构建能够容纳合理分歧、根据情境透明地呈现不同价值立场的系统。公共层面仍需划定价值多元的边界、规范价值冲突解决程序，并监督开发者恪守既定规则。最后，文章提出涵盖价值选择、程序与权威、技术验证、执行问责四个方向的初步研究议程，邀请更多学者参与讨论。

https://www.lawfaremedia.org/article/a-new-research-agenda-for-ai-constitutionalism

编译：杜宛鸿

2、美国兰德公司：人工智能无人集群或将在台海长期冲突中形成中方优势

8 月 13 日，美国兰德公司网站发表其政治学副研究员扎卡里·伯德（Zachary Burdette）等的文章《探究未来中美冲突下人工智能的作战影响：Camp(ai)gn 兵棋推演初步观察结论》。文章以 2035 年台海冲突为场景完成十轮兵棋推演，研判人工智能自主系统重塑现代战役六项初步研判假说。推演设定中美双方全面部署各类人工智能无人空海陆平台，显示智能无人装备可催生以机器人对抗为主的新型有限低烈度冲突，演化出区别于传统大国战争的升级路径与博弈结局。长期消耗战背景下规模化自主集群具备突出价值，依托本土

制造产能与近海区位，中方在无人装备持续补给层面具备结构性优势。海量无人装备拓展指挥员战术选择空间，但同步加重决策负担，也为盟友开辟本土防御、协同生产等新型参战路径。报告同时认为，攻击敌方数据中心难以形成决定性打击，无法成为人工智能作战体系致命短板。全文推演结论仅为推演假设，文章提出需围绕兵力架构、反制手段、联盟协同、军工产能四大方向和两项兵棋方法论深化专项研究。

https://www.rand.org/pubs/perspectives/PEA5022-1.html

编译：钟珺雯

3、美国 CSIS：网络攻击智能化扭曲企业竞争格局

8 月 7 日，美国战略与国际问题研究中心（CSIS）发表其讲席教授艾玛·苏诺（Emma Surnow）的文章《谁来买单？人工智能驱动网络攻击对经济意味着什么》。文章认为，大语言模型（LLMs）正显著提升网络攻击能力，使得漏洞发现与利用急速自动化。以 Anthropic 的 Mythos 为代表的前沿大语言模型，已能在几乎无人类监督下识别、攻击和修补零日漏洞与 N 日漏洞。然而，网络攻击的代价分配极不均衡。企业受到网络攻击后，单次赎金可达数千万美元。大型跨国企业不仅有实力支付高额赎金，还能够获取最先进的网络安全模型以应对网络攻击。而中小型企业往往无力获取先进模型，境外企业难以获取美国顶尖网络安全模型，更容易成为网络攻击的主要受害者。企业间安全能力的差距进一步加剧市场

集中度，扭曲竞争格局。文章建议，企业必须放弃事后修补的被动策略，在生产周期全面引入“设计安全”（secure-by-design）框架；头部人工智能企业应探索“安全即服务”模式，由服务商依托前沿人工智能代为扫描漏洞，而非向客户直接开放模型，补齐中小型企业的防御短板。政府应提供清晰、可预期的模型分发监管框架，并明确网络攻击法律责任边界，依靠问责机制倒逼企业提升产品安全性。

https://www.csis.org/blogs/charting-geoeconomics/who-pays-what-ai-powered-cyberattacks-mean-economy

编译：孙韵雯

4、美国兰德公司：前沿人工智能双重用途的生物学基准解读方法

8 月 6 日，美国兰德公司网站发表其研究员格兰特·埃利森（Grant Ellison）等人的文章《解读前沿人工智能双重用途的生物学基准：测量、饱和与代际分析》。文章认为，基准测试作为评估前沿人工智能生物学能力的常用方法，正面临饱和与解读困境：高分成绩无法直接反映模型的新增能力或现实生物风险。为此，文章提出了一种系统性分析策略，将 8146 个基准项目整合为统一语料库，运用项目反应理论（IRT）将人工智能系统与专家基线置于同一测量尺度，并使用通用分类法标记任务类型，从而识别仍具区分度的项目、近期模型提升的领域，并解读基准表现与生物风险的可能关联。研

究发现，尽管前沿人工智能已经在一部分基准项目上达到饱和，但整个语料库并未完全失效，仍存在一批高难度、高区分度的项目超出当前模型能力范围，并能有效区分不同代际的系统。具体而言，Gemini 3.0 Pro 相较于 2.5 Pro 在困难项目上有所进步，Gemini 3.1 Pro 则继续提升，且在专家故障排查、故障识别相关的高信息量样本上表现更佳。此外，仅选取信息量最高的前 10%项目，其对模型能力的估计值与完整数据集的结果相关性高达 99%，表明高效抽样能够有效评估前沿性能。尽管这些基准数据在推广到现实场景时存在局限，但通过精细分析方法能够提取有效的测量信号，揭示实际进展，并有助于理解人工智能在双重用途生物学中的潜在影响。

https://www.rand.org/pubs/research_reports/RRA5055-1.html

编译：张佳延

5、美国兰德公司：能源供给成为美国人工智能基础设施扩张关键制约

8 月 11 日，美国兰德公司网站发表其高级经济学家伊斯梅尔·阿尔西涅加斯·鲁埃达（Ismael Arciniegas Rueda）等人撰写的研究简报《评估人工智能数据中心的能源潜力：比较选址适宜性的框架》。报告认为，随着前沿人工智能模型推动算力需求快速增长，能源供给能力正成为制约美国人工智能基础设施扩张的重要因素，数据中心选址已成为影响人工智能竞争力的战略问题。大型人工智能数据中心开发商普遍

优先选择电网并网，其可靠性要高于单纯依靠现场发电的模式。未来挑战不仅在于增加电力供应，更在于提升电力输送能力。为评估不同地区建设潜力，兰德构建了涵盖能源供应、能源系统、配套投入、环境因素以及治理和社区因素五个维度的评估框架，并分析美国 22 个潜在地点。不存在各维度均完美的选址，所有选址均需要在供电、基建、环境、治理之间权衡取舍。现有基础设施条件是决定数据中心建设可行性的重要因素，具备变电站、电力输送网络和工业用地基础的旧工业园区、联邦设施以及退役电厂更具建设优势。印第安纳州罗克波特电厂（Rockport Power Plant）能源潜力最高，预计到 2030 年可提供约 4.2 吉瓦电力容量。由于新建输电和配电设施面临审批、监管和建设周期限制，美国电力系统可能难以支撑最大规模集中式人工智能数据中心建设，未来需更多依靠基础设施复用、现场发电和分布式算力布局。

https://www.rand.org/pubs/research_briefs/RBA3845-3.html

编译：高美琳

6、美国《国家利益》：奖励前置或致黎巴嫩改革落空

8 月 12 日，美国《国家利益》网站发表保卫民主基金会研究分析师艾哈迈德·沙拉维（Ahmad Sharawi）与高级研究员戴维·达乌德（David Daoud）的文章《特朗普的黎巴嫩竞赛》。文章认为，黎巴嫩总统奥恩上月访美成果丰硕，特朗普以政治、经济和军事手段拉拢贝鲁特，防止伊朗借美伊停火

协议保全真主党。但问题在于，美方奖励跑在了贝鲁特落实承诺之前。6 月 26 日框架协议明确规定，美国新援助和以色列分阶段撤军须以黎巴嫩在全国范围内经核查地解除真主党武装为前提。然而，黎巴嫩的实际执行远未达标：目前仅在三个试点区有限部署，且黎军未公开证明其已解除真主党武装或拆除其基础设施；全国解除武装方案内容保密、执行停滞，金融反制措施（如冻结真主党相关金融机构）也未取得实质进展。更令人担忧的是，黎巴嫩领导人已开始弱化协议约束力：总理萨拉姆称协议是“政治性而非法律性”约束，奥恩则颠倒顺序，要求先撤军再解除武装。文章警告，提前给予奖励只会鼓励贝鲁特以“存在”代替“落实”，真主党则可从试点区战术撤退，待以色列撤军和国际关注消退后卷土重来。文章强调，特朗普抗衡伊朗在黎影响的战略方向正确，但华盛顿不应为尚未兑现的承诺买单；美黎关系应基于实际成果而非空头许诺。

https://nationalinterest.org/blog/middle-east-watch/donald-trumps-lebanon-race

编译：白一冰

7、美国布鲁金斯学会：开放权重模型对美国人工智能领导地位至关重要

8 月 10 日，美国布鲁金斯学会（Brookings）发表其技术创新中心非常驻高级研究员约翰·维拉塞尼奥尔（John Vill

asenor）的文章《为什么开放权重模型对美国的人工智能领导地位至关重要》。文章认为，封闭模型内部的运行机制和训练方式不公开，开源模型的训练数据等信息都向公众披露，处于封闭模型和开源模型两端之间的被称为“开放权重模型”。这些模型能够部署到本地设备，决定模型如何解读数据并输出结果的“权重”是公开的，但通常不公开生成这些“权重”的方法。开源模型和开放权重模型是帮助下一代研究者和创业者学习人工智能的重要工具，在需要低延迟和高可靠性的场景中优势明显。开放权重模型也能够促进更健全、更丰富的人工智能应用生态。一些观点经常批评开放权重模型所带来的安全风险，事实上封闭模型也同样存在安全漏洞。文章提出两点政策建议：其一，中国的开放权重模型非常出色，美国不应以所谓国家安全威胁为理由发布关于中国人工智能模型的禁令，而是应该加快创新、开发更好的美国开放权重模型。其二，美国的人工智能产业被几家封闭模型提供商所主导，将导致权力过度集中等诸多问题。开放权重模型能够促进美国发展多元化、民主化的人工智能生态系统。

https://www.brookings.edu/articles/why-open-weight-models-are-crucial-for-american-ai-leadership/

编译：高靓瑜

8、美国卡内基国际和平基金会：美军人工智能扩散面临多重障碍

8 月 10 日，美国卡内基国际和平基金会发表 GovAI 研究员杰克·斯特克勒（Jake Steckler）的文章《应对美国军队人工智能扩散的障碍》。文章认为，尽管美国白宫要求军队“积极采用”人工智能，国防部也提出建设“人工智能优先”的作战力量，但人工智能在美军中的应用仍主要集中于情报、目标识别和后勤等辅助性领域，尚未达到改变战争方式的程度。文章以自主无人机为案例，认为美军人工智能转型面临技术、文化、官僚程序、政治、工业基础、测试评估、系统整合和监督等八类障碍。文章认为，在和平时期及有限战争条件下，美军长期军事优势形成的文化惯性、缓慢的政治和官僚程序以及工业基础弱化，均将阻碍人工智能大规模扩散。自主无人机还面临目标识别、复杂环境决策、算力与能源限制、电子战干扰以及训练数据不足等技术问题。乌克兰战场表明，人工智能已能够提高无人机的作战效能，但目前多数无人系统仍需要人工操作，完全自主化仍存在较大技术限制。文章指出，大规模战争可能通过强化政治意愿、加快研发和简化审查程序来降低部分障碍，但一些技术和工业问题无法在短期内解决。文章建议，美国国防部应立即扩大人工智能人才队伍，鼓励军方承担更多工业和作战风险，并加大对小型专业企业的投资，通过快速淘汰失败方案推动生产和试验。同时，测试、评估和监督机制应当改革而非取消，应加强红队测试和试验环境建设，明确能力开发及跨系统整合的最低要求，并保留对武力使用具有实质意义的人类权威和问责机

制。

https://carnegieendowment.org/research/2026/08/confronting-the-barriers-to-ai-diffusion-in-the-us-military

编译：罗方婕

9、美国《外交事务》：制度激励使美总统陷入不必要战争

8 月 12 日，美国《外交事务》网站发表史汀生中心高级研究员艾玛·阿什福德（Emma Ashford）的文章《美国对战争的致命吸引力：总统使用军事力量的反常动机》。文章认为，特朗普曾承诺结束战争而非发动战争，但其第二任期 18 个月后，美国再次深陷中东战争。尽管美军取得若干战术成果，但美国并未获得真正战略胜利，伊朗在部分方面反而拥有更强影响力。文章认为，美国反复陷入可避免战争，并非仅由个别领导人决定，而是受结构性激励推动。美国总统发动军事行动成本较低，国会长期放弃战争监督，庞大的全球基地网络和军事部署能力使动武更容易；媒体、盟友和地区伙伴也常推动美国介入冲突。与此同时，美国领导人习惯为边缘战争设定最大化目标，难以在未实现承诺目标前退出，因而陷入“容易开战、难以脱身”的循环。美国公众对战争后果相对隔绝也降低了反战压力。志愿兵役制、远程作战技术和战争成本的分散化，使多数美国人只感受到通胀、债务和资源消耗等间接影响。但这些成本并不小：中东战争持续消耗精确弹药和拦截器，挤占印太、欧洲等更重要战略方向的资

源，削弱美国应对中俄等大国竞争的能力，并损害其作为全球公共产品提供者的信誉。文章认为，美国若要打破战争惯性，不能只依赖承诺结束“永久战争”的领导人，而必须改变制度激励，包括减少前沿基地、恢复国会对战争和军费的约束、限制对边缘战争的追加拨款，并削弱国防部与军工企业之间的利益循环。否则，美国将继续被一连串永久冲突束缚，最终丧失自主配置战略资源的能力。

https://www.foreignaffairs.com/united-states/americas-fatal-attraction-war

编译：刘晓

10、美国《外交政策》：西岸而非加沙应成为特朗普的优先事项

8 月 11 日，美国《外交政策》网站发表布拉格国际关系研究所（Institute of International Relations Prague）副研究员阿兹里尔·伯曼特（Azriel Bermant）的文章《约旦河西岸而非加沙，应成为特朗普的优先事项》。文章认为，特朗普政府的加沙路线图已陷入僵局，应将政策重点转向遏制约旦河西岸日益严重的暴力局势。以色列与哈马斯都极不可能履行条款，所谓加沙路线图陷入进退两难困境，几乎没有成功的可能。而约旦河西岸正酝酿更严重的危机，尽管西岸的巴勒斯坦恐怖威胁已大幅下降，但以色列政府正煽风点火使得局势可能一触即发。一方面，大选之际的以色列政府为讨好右翼

支持者，进一步推动定居点扩张并主张吞并西岸，纵容暴力定居者针对巴勒斯坦人的袭击；另一方面，以政府削弱巴勒斯坦权力机构财政的举措正加剧双方武装冲突风险。文章强调，特朗普在西岸问题上比在加沙拥有更大的政策影响力，应重新制裁极端定居者并约束内塔尼亚胡，以稳定西岸局势，避免加沙问题路线图因此彻底失败。

https://foreignpolicy.com/2026/08/11/trump-israel-west-bank-gaza-palestinians-settlers-hamas-netanyahu-election/

编译：贺宇希

11、美国《外交政策》：瓦解国际刑事法院不符合美国利益

8 月 10 日，美国《外交政策》网站发表耶鲁大学杰克逊全球事务学院高级研究员珍妮·迪·乔瓦尼（Janine di Giovanni）与清算计划（Reckoning Project）幕僚长克里斯托弗·基普·黑尔（Christopher Kip Hale）的文章《拆除国际刑事法院不符合美国利益》。文章认为，今年 7 月美国国务卿马尔科·鲁比奥宣布推行一项旨在“系统性瓦解”国际刑事法院（ICC）的运动，特朗普政府此前也多次针对 ICC 采取制裁措施。文章认为，依据《罗马规约》设立的 ICC 是全球处理最严重罪行的唯一常设司法机构，当前的案件情况也印证了其不会威胁美国主权，美国此次行动的真实目的并非保护主权，而是要保留实施暴行却无需承担后果的特权。文章强调，美国 70 年来始终是“权力必须受法律约束”理念的重要倡导者，这份公

信力是美国的重要资产。而特朗普政府打击 ICC 的举措相当于直接放弃此资产，将严重损害美国的国际信誉。同时，瓦解 ICC 将对全球正义造成灾难性影响。文章认为，那些旨在记录相关事务，且有朝一日能够对此进行评判的机构，能够保持凝聚力，拥有充足的资源，从而能屹立不倒。但美国若逐块拆解国际刑事法院，则意味着选择了另一种路径。

https://foreignpolicy.com/2026/08/10/icc-trump-campaign-rubio-sanctions-international-justice/

编译：李泓静

12、美国 PIIE：美国企图在试图支撑日元时鱼与熊掌兼得

8 月 11 日，美国彼得森国际经济研究所（PIIE）发表高级研究员莫里斯·奥布斯特费尔德（Maurice Obstfeld）的文章《美国企图在提振日元时兼得鱼与熊掌》。文章认为，美国财长贝森特于 7 月 31 日联合日本当局干预汇市提振日元，是美方自 1998 年以来首次入市干预日元汇率。然而，这一干预行动非但未能彰显美国的外交承诺，反而暴露了美方政策逻辑的深度混乱。从贸易角度看，美国一面通过 301 条款对日加征关税并要求其在美投资 550 亿美元，直接构成了日元贬值的内在压力；另一面却试图通过干预汇市来掩盖这一矛盾。从货币政策看，美方主张强美元与国际储备地位，但干预汇市的本质是追求弱势美元；同时，美方干预系因担忧日本为抛售日元而大量减持美国国债，从而加剧美债市场的脆

弱性。此外，贝森特“鼓励”美联储调整外国和国际货币当局回购机制（FIMA），试图以此稳定美债利率并辅助其金融外交，此举严重背离了该工具设立的初衷，进一步模糊了货币政策与财政主导的界限，威胁美联储独立性。文章强调，美日汇率走势根本上取决于两国财政与货币政策差。这种不愿触及根本政策调整、企图“鱼与熊掌兼得”的汇市干预纯属短期敷衍，终将沦为徒劳无功的无效举措。

https://www.piie.com/blogs/realtime-economics/2026/trying-prop-yen-us-wants-have-its-cake-and-eat-it-too

编译：陈奕好

13、美国进步中心：特朗普政府干涉 2026 年中期选举以巩固“帝王式总统”权力

8 月 12 日，美国进步中心（American Progress）高级研究员迈克尔·索赞（Michael Sozan）和本·奥林斯基（Ben Olinsky）发表文章《特朗普政府干涉 2026 年中期选举以巩固帝王式总统权力》。文章认为，特朗普政府已攫取史无前例的行政分支权力，并正在执行一项颠覆 2026 年中期选举的计划来巩固其权力，并在不受问责的情况下继续推进其政策议程。政治学和历史学证明，具有帝王式思维的领导人旨在破坏和控制选举，以确保他们及其盟友留任。基于已被证伪的大规模选民欺诈这一谬论，政府的多管齐下计划包含 15 项环环相扣的策略，旨在使符合条件的美国人更难行使其投票

权。文章警告，这 15 项策略构成美国历史上对民主最严峻的威胁，总统正试图通过行政权力人为制造少数派统治。但其独裁剧本亦存在依赖各方默许的致命弱点。文章呼吁州官员、法院、国会、公民社会与跨意识形态公民捍卫宪法权利，防止民主倒退。宪法未授予总统控制选举的任何权力；相反，宪法将举行自由公正选举的主要权力赋予各州，并以国会作为后盾。

https://www.americanprogress.org/article/the-trump-administration-is-interfering-in-the-2026-midterm-elections-to-entrench-the-imperial-presidency/

编译：王一凡

编译：白一冰、高靓瑜、罗方婕、刘晓、贺宇希、李泓静、陈奕好、王一凡、杜宛鸿、钟珺雯、孙韵雯、张佳延、高美琳

审核：刘源、郑乐锋、周武华、申青青