



CISS 海外信息专报

(2026 年 7 月 30-31 日)

1、美国兰德公司：人工智能时代需应对网络攻击和自主合成病原体等安全问题

7 月 23 日，美国兰德公司发表人工智能、安全与技术中心创始主任塞拉·内沃（Sella Nevo）的文章《守护人工智能时代的未来——塞拉·内沃问答》。文章认为，一年内或将出现能按指令生成世界级软件的模型，而数学领域科研发现效率有望提升十倍乃至百倍，从而在安全、材料科学等领域释放巨大潜能。文章同时警示，最紧迫的风险在于网络攻击。人工智能赋能的网络进攻能力正在快速迭代。他担忧能够自主执行端到端网络入侵的模型将扩散，大幅拉低网络犯罪的技术门槛，引发规模空前的网络安全灾难。内沃领导的人工智能、安全与技术中心（CAST）依托在人工智能和生物技术领域的研究积累和在美国国家安全领域的公信力，在美政策制定、实验室安全评估及为各国政府提供专业研判等工作中发挥关键枢纽作用，有效连接技术、安全与政策群体。他参与的“金丝雀计划”评估显示，前沿模型现已能协同云端实验室合作设计存在重大生物安全隐患的产品，接近自主合成病原体的水平。在近期研究中，他为美国和前沿人工智能实验

室提供了构建高安全性数据中心的建议，旨在抵御国家级攻击，提升关键系统安全防护能力。

<https://www.rand.org/pubs/commentary/2026/07/safeguarding-the-future-in-the-ai-era-qa-with-sella.html>

编译：张佳延

2、美国兰德公司：需建立结构化风控体系以应对生成式人工智能漏洞

7月30日，美国兰德公司发表研究员埃利·阿尔哈贾尔（Elie Alhajjar）等人的报告《识别与刻画人工智能漏洞的结构化方法》。报告摒弃按攻击手段分类的传统思路，从大模型完整技术架构溯源风险源头，梳理出31类人工智能专属漏洞。此类隐患大多由概率化学习机制、训练数据缺陷与算法优化取舍引发，并非传统代码漏洞，难以依靠常规系统补丁彻底修复。报告将人工智能全链路划分为训练数据、分词器、Transformer架构、上下文窗口等核心组件，通过威胁、影响两套量化指标评估风险等级，判定训练数据污染、用户交互接口是两大最高风险区域：投毒数据会长期固化模型缺陷，提示词注入等接口攻击门槛极低。传统打补丁模式无法适配人工智能安全治理需求，核心防控手段为数据源溯源校验、架构隔离防护与全流程行为监测。报告提出6项落地举措：要求企业在人工智能设计阶段嵌入组件级风险评估，研发适配随机攻击场景的安全检测工具，建立统一人工智能漏洞收

录规范，把数据层管控列为安全优先事项，通过多层风险补偿机制缓释结构性隐患，为可信人工智能政策与工程落地提供标准化分析框架。

https://www.rand.org/pubs/research_reports/RRA4983-1.html

编译：钟珺雯

3、美国布鲁金斯学会：美国国会应尽快建立联邦层面的人工智能治理法律框架

7月17日，美国布鲁金斯学会发表“湾城资本”董事总经理大卫·拜尔（David Beier）和学会治理研究与技术创新中心高级研究员马克·麦卡锡（Mark MacCarthy）的文章《国会必须通过一项新的联邦人工智能治理法》。文章认为，当前美国人工智能治理体系过度依赖行政命令、出口管制和企业自律，缺乏统一、稳定且具有法律约束力的联邦监管框架，因而难以有效应对前沿人工智能技术快速发展带来的安全风险。作者建议美国国会尽快制定新的联邦人工智能治理法案，通过建立市场许可制度、推行强制第三方审计机制以明确各个主体的法律责任，构建长期稳定的治理体系。文章认为，人工智能治理应从自愿承诺转向强制监管，所有前沿人工智能模型在公开部署前均应接受经认证的独立机构审计，并由联邦机构依据统一标准颁发许可。监管重点应聚焦对公共利益具有重大影响的“实质性风险”，包括人工智能驱动的大规模网络攻击、关键基础设施破坏、生物武器设计与病原

体合成，以及人工智能系统失控等可能威胁国家安全和公共安全的风险。针对当前美国国会相关草案提出的“开发者与部署者”的分类方式，作者认为这种方式无法适应人工智能产业的实际运行模式，容易形成监管漏洞，建议将所有向公众提供人工智能模型的主体统一纳入监管范围。此外，联邦政府应在涉及网络安全和生物安全等国家安全领域保留统一监管权，同时赋予各州在消费者保护、数据隐私等领域保留地方监管职能的空间。

<https://www.brookings.edu/articles/congress-must-pass-a-new-federal-law-on-ai-governance/>

编译：高美琳

4、美国 CFR：人工智能经济收益取决于综合能力而非单一技术领先

7月29日，美国对外关系委员会（CFR）发表高级研究员丽贝卡·帕特森（Rebecca Patterson）的文章《人工智能的经济赢家》，讨论人工智能发展如何重塑各国经济表现与地缘经济格局。文章认为，未来人工智能领域的经济受益者并不一定是掌握前沿模型的国家，而可能是在技术研发、技术应用、产业基础和全球供应链中具有综合优势的国家。美国和中国虽然处于人工智能研发前沿，但两国能否获得广泛经济收益仍取决于人才、资本、基础设施和公共政策社会支持等条件。中国近年来在人工智能科研和人才领域快速追赶，

美国则在资本投入方面占据明显优势。此外，芯片、关键矿产、能源和数据中心等供应链环节成为影响人工智能发展的重要因素。文章进一步分析，美国依靠科技企业、芯片设计和云基础设施保持领先，但面临供应链脆弱性、能源限制和社会接受度不足等挑战；中国拥有丰富的数据资源、较强的能源供给能力和政策支持，但先进芯片短缺限制其发展。同时，中国台湾地区、荷兰、日本等经济体凭借半导体制造、光刻设备和关键材料等环节获得供应链影响力。文章强调，人工智能时代不存在单一国家独立获得优势的路径，各国未来经济表现将取决于创新能力、应用能力以及在全球产业链中的地位。

<https://www.cfr.org/articles/ais-economic-winners>

编译：张方琼宇

5、美国 CFR：中国的全球好感度超过美国

7月27日，美国对外关系委员会（CFR）发表其全球卫生高级研究员黄严忠（Yanzhong Huang）的文章《中国的全球好感度超过美国，发生了什么》。7月15日，皮尤研究中心发布的报告显示，在其所调查的大多数国家中，人们对中国的好感度已经超过了美国。文章认为，这并非突如其来的变化，而是再次确认了已经显现的发展趋势。首先是因为中国对自身软实力建设的投入开始取得成效。中国化的生活习惯（即 Chinamaxxing）在社交媒体上迅速传播。同时，中国

的发展模式逐渐成为值得借鉴的对象，美国如今部分产业政策也明显借鉴了中国模式。其次是因为皮尤研究中心的调查中，近一半国家属于中等收入国家。非洲、拉丁美洲、东南亚等区域的新兴经济体中，人们对中国的好感度明显超过富裕国家。最后是因为美国软实力不断下降，正在失去盟友的认同。但是，对美国好感度的下降没有直接转化为对中国相应规模的上升，中国在美国盟友伙伴中的支持率仍然有限。此外，中国的邻国，如印度、日本、菲律宾和韩国，仍对美国保持较高的好感度。

<https://www.cfr.org/articles/china-now-outranks-the-united-states-in-global-favorability-what-happened>

编译：高靓瑜

6、美国《外交政策》：美沙核协议是特朗普的外交失职

7月27日，美国《外交政策》网站发表美国前驻埃及大使丹尼尔·C·库尔策（Daniel C. Kurtzer）与卡内基国际和平基金会高级研究员亚伦·戴维·米勒（Aaron David Miller）的文章《特朗普与沙特的核协议是外交失职》。文章认为，特朗普政府与沙特民用核合作协议突破美国核不扩散政策底线，是其外交决策失序和战略短视的集中体现。首先，协议内容存在重大隐患。该协议允许沙特在本国进行铀浓缩，却未充分纳入国际原子能机构监督机制，并突破美国与阿联酋“123协议”确立的防扩散标准，缺乏充分的商业、经济和

民用核能依据。其次，谈判过程暴露外交能力不足。美方谈判代表忽视沙以关系正常化在核协议中的重要性，协议内容未涉及巴以问题，而特朗普随后单方面追加沙特与以色列关系正常化条件，反映其谈判准备不足、政策前后矛盾。最后，协议将带来负面影响。短期来看，协议将削弱美国核不扩散政策与信誉，使其遏制伊朗铀浓缩立场陷入矛盾，并为伊朗质疑美国可信度提供借口，也可能损害与以色列的战略互信。历史与战略层面，协议可能埋下类似 1957 年向伊朗提供核技术最终酿成长期安全危机的隐患。沙特核协议与俄乌冲突、加沙计划及近期与伊朗签署的谅解备忘录，均反映特朗普政府外交准备不足、谈判失当和缺乏专业监督。对此，文章强调，美国国家安全不应继续由缺乏战略经验的业余人士主导。

<https://foreignpolicy.com/2026/07/27/trump-nuclear-saudi-arabia-deal-iran-israel/>

编译：贺宇希

7、美国布鲁金斯学会：特朗普政府削减国税局预算的影响

7 月 28 日，美国布鲁金斯学会（Brookings）发表其高级研究员埃利斯·陈（Ellis Chen）的文章《特朗普政府削减国税局预算，拖累报税季表现》。文章认为，特朗普政府 2025 年削减美国国税局（IRS）工作人员规模，对 2026 年报税季纳税人服务造成负面影响，与官员宣称机构人员配置充足的说法相矛盾。由于人员削减，IRS 虽在报税季前后重新招聘

数千名员工，但仍面临人员不足问题。文章认为，人员短缺迫使 IRS 在税表处理和电话服务之间进行取舍，优先处理税表，导致纳税人电话等待时间增加，获得人工帮助的机会减少。同时，需要人工处理的税表和纳税人文件积压增加，部分退税和案件处理受到延迟。文章认为，技术升级能够改善机构运行，但无法完全替代充足的人力资源，特朗普政府削减 IRS 人员最终削弱了机构服务能力，并使纳税人受到影响。

<https://www.brookings.edu/articles/the-trump-administrations-irs-cuts-undermined-filing-season-performance/>

编译：王一凡

8、美国《国家利益》：全球媒体署独立性面临政治化挑战

7月29日，美国《国家利益》网站发表“无国界记者”组织美国执行主任克莱顿·韦默斯（Clayton Weimers）的文章《为何美国媒体应独立于国务院》。文章认为，特朗普总统提名的美国全球媒体署（USAGM）首席执行官人选莎拉·罗杰斯同时兼任国务院公共外交副国务卿，若获确认，将使该机构沦为国务院下属部门，从而破坏其编辑独立性。特朗普自第一任期起就试图对 USAGM 施加政治控制，2020年任命的 CEO 曾试图清洗被认为不够亲特朗普的高管，最终被法院制止。2025年特朗普再次签署行政令削弱该机构，同样因诉讼受阻。如今他转而试图将整个机构并入国务院。罗杰斯在任期间已因支持外国政治人物、制裁欧洲官员、试图驱逐

研究虚假信息的研究人员而备受争议。已故参议员格雷厄姆生前多次为 USAGM 辩护，并在委员会中成功恢复了大部分被削减的经费。参议院应拒绝罗杰斯的提名，以维护美国新闻自由的核心价值。

<https://nationalinterest.org/feature/why-us-media-should-be-independent-from-the-state-department>

编译：白一冰

9、美国 CFR：特朗普政府介入企业的风险

7 月 27 日，美国对外关系委员会（CFR）发表美国国防部前助理部长劳拉·泰勒-凯尔（Laura Taylor-Kale）的文章《特朗普政府交易企业的做法立足不稳》。文章认为，英特尔股东因反对政府以《芯片法案》补贴换取股权而提起诉讼，这暴露出特朗普政府对联邦法律的弹性解释与越权操作。特朗普政府目前已在英特尔、西屋电气等约 30 家涉及半导体、稀土及关键矿产的企业中强制推行股权交易，五角大楼拟动用 2000 亿美元推进国有化举措。虽然《国防生产法》（DPA）及《芯片法案》旨在通过补贴与贷款激励战略性产业，但特朗普政府将其曲解为政府可直接参股，缺乏明确法律授权且交易结构极不透明。鉴于稀土等关键供应链对国防安全至关重要，单纯依赖市场调节确易造成对竞争对手的依赖，政府适当参股具备一定合理性；但当前缺乏明确标准与利益冲突保护的强硬做法，极易演变为官僚亲疏有别、浪费纳税人资

金及政治分肥。随着《国防生产法》面临 9 月 30 日的重新授权节点，文章呼吁，国会应理清立法授权，明确政府入股的适用条件与监管边界，防止产业政策沦为破坏市场秩序与法治原则的政治工具。

<https://www.cfr.org/articles/trump-administrations-dealing-in-companies-is-on-shaky-ground-2>

编译：陈奕好

10、美国 PIIE：美学生签证新规损害长期经济增长

7 月 27 日，美国彼得森国际经济研究所（PIIE）发表其高级研究员迈克尔·安德鲁·克莱门斯（Michael A. Clemens）的文章《美国一项限制学生签证的新规定将损害美国经济》。文章认为，特朗普政府 7 月出台新规，将国际学生的最长有效期签证限制为四年，到期后学生需自主申请延期。该规则将大幅限制高水平国际人才进入美国经济创新与生产力增长的科学、技术、工程和数学（STEM）核心领域，导致美国经济生产率下降。文章认为，新规官方反恐防欺诈的理由缺乏说服力，其真实目的更可能是配合政府全面排除合法移民政策。然而，新规的干扰会从源头阻止国际学生赴美，加大美国贸易逆差，冲击美国创新与生产力。按保守估计，若每年流入美国的国际学生持续减少三分之一，每年会给美国造成约 2000 亿至 4000 亿美元损失。文章认为，新规还对 OPT 高技能移民通道造成冲击，赋予美国公民及移民服务局

（USCIS）官员极大自由裁量权。文章最后强调，国会可依据《国会审查法》，以新规对美国经济存在巨大影响为由，直接叫停这项新的签证期限政策；法院也可以政府没有认真考虑新规可能带来的巨大经济损害为由介入推翻新规。

<https://www.piie.com/blogs/realtime-economics/2026/new-us-rule-restrict-student-visas-will-hurt-us-economy>

编译：李泓静

编译：陈奕好、贺宇希、高靓瑜、李泓静、白一冰、王一凡、张佳延、钟珺雯、高美琳、张方琼宇

审核：周武华、申青青、刘源、郑乐锋