

引用格式:王恺乐,刘昊,陈云伟.美国关键技术管制的信号感知体系研究.中国科学院院刊,2026,41(3):617-629,doi:10.3724/j.issn.1000-3045.20250418001.

Wang K L, Liu H, Chen Y W. Research on signal perception system of key technology regulation in the United States. Bulletin of Chinese Academy of Sciences, 2026, 41(3): 617-629, doi: 10.3724/j.issn.1000-3045.20250418001. (in Chinese)

美国关键技术管制的 信号感知体系研究

王恺乐¹ 刘昊^{1,2*} 陈云伟^{1,2}

1 中国科学院成都文献情报中心科技创新评价研究中心 成都 610299

2 中国科学院大学 经济与管理学院 信息资源管理系 北京 100190

摘要 分析关键技术管制信号感知体系运行机制,揭示美国对外技术遏制的深层逻辑和基本程序。通过文献梳理与信息挖掘,分析美国关键技术管制信号感知体系存在前端技术感知与技术锁定、中端技术评估与风险识别及后端技术管制响应与动态制裁等结构特征,进一步探讨美国在关键技术管制信号感知中的参与主体与角色定位、弱信号情报感知的来源与机制、评估的模式与方法、制裁手段等。对美国关键技术管制信号感知体系的研究,为我国应对美国主导的技术“脱钩”风险,构建自主可控技术治理体系提供参考。

关键词 科技安全,关键技术,情报感知,威胁响应,弱信号

DOI 10.3724/j.issn.1000-3045.20250418001

CSTR 32128.14.CASbulletin.20250418001

科技领域安全是国家安全的重要组成部分,在总体国家安全观中占据重要地位并发挥关键作用^[1]。建设适应科技竞争与国家安全的科技情报事业发展体系,是应对长期国际科技战略竞争、服务国家安全特别是科技安全,促进我国科技情报事业治理体系和治理能力现代化发展的必然要求^[2]。近年来,科技情报研究持续向科技安全领域拓展,如科技安全风险监测

预警体系构建^[3]、科技人才安全服务^[4]、科技发展动态与科技实力评估^[5,6]、科技安全实践^[7]及科技安全保障^[8]等,关键技术管制方面的态势感知研究也日益成为大国科技竞争背景下科技安全情报研究的重要内容。

近年来,美西方国家不时在一些领域推出“泛安全化”手段^[9],特别是美国频频以“技术威胁”为由

*通信作者

资助项目:中国科学院青年创新促进会人才专项项目(2023183),国家自然科学基金专项项目(L2424111)

修改稿收到日期:2026年3月3日

不断升级管制手段，扩大对其他国家在关键技术领域和技术实体方面的限制等。根据美国商务部公布的实体清单，中国实体企业在清单中的占比从2018年的20.7%升至2024年的32.5%。在美国的“337调查”^①中，中国企业占比近40%，且美方频繁对进入其核心市场的中国高科技企业实施调查和制裁^[10]。

然而，现有研究主要集中在技术感知的后端，即受管制后分析所实施的技术制裁、出口管制及其影响等方面^[11-14]，较少从前端研究所谓“技术威胁”的具体形成过程，以及形成过程中是否存在一种可被感知的信号等。本文从科技情报视角提出美国在关键技术管制的信号感知概念，分析美国技术威胁感知体系并将其划分为三大核心模块——前端技术感知与技术锁定、中端技术评估与风险识别、后端技术管制响应与动态制裁，尝试从情报链角度揭示美国关键技术管制的信号感知体系。

1 “技术威胁”感知动因分析

1.1 技术权利方面的战略焦虑

美国将他国技术崛起视为“零和博弈”，这种思维源于根深蒂固的霸权焦虑，体现为对技术权利结构性转移的深层恐惧。根据Gilpin^[15]的霸权维护理论，当主导国察觉到挑战者在技术产业综合实力上的崛起威胁时，会通过系统性压制来延缓权力转移进程。例如，20世纪80年代，针对日本半导体产业的崛起，美国不断从贸易规则、知识产权上对其进行打压，最终导致日本半导体产品的全球市场份额从50%以上迅速衰退至20世纪90年代的20%左右^[16]。

1.2 国家安全方面的权衡考量

美国以“国家安全”为由，将技术制裁上升至战略层面。2022年美国《国家安全战略》将技术定

位为“当今地缘政治竞争的核心”，强调“美国需加强自身技术优势，深化与盟友合作，塑造技术领域的国际规则，强化对国际技术生态的掌控力”^[17]。2024年美国白宫科技政策办公室（OSTP）发布的《关键和新兴技术清单》进一步强化这一逻辑，提出“关键新兴技术将重塑世界，美国必须确保其安全与价值观”。2024年8月，美国商务部工业和安全局（BIS）以“违反美国国家安全和外交政策利益”为由，将63个俄罗斯实体列入管制清单^[18]，这些实体主要涉及俄罗斯的军事、国防工业、无人机生产及敏感货物运输等领域。

1.3 经济保护主义与产业链利益

美国对关键技术进行管制的另一逻辑，与其经济保护主义倾向及全球产业链利益再分配需求密切相关。自15世纪重商主义理论确立至今，关税及在现代经贸体系中衍生出的技术壁垒，始终被视为实现贸易盈余和保护本土产业的重要工具。现代战略贸易理论指出，政府通过选择性干预可帮助本国企业在尖端技术领域获得竞争优势^[19]。在这一理论框架下，美国对企业的技术封锁，本质上是运用保护主义工具遏制竞争对手的技术迭代能力，维护本国战略产业的主导权。美国一方面依赖全球化分工降低创新成本，另一方面又试图通过“小院高墙”策略阻断技术外溢。这种“技术民族主义”实质上是将产业链安全议题工具化，服务于其国内利益集团对高附加值环节的独占诉求。

1.4 地缘政治博弈与意识对抗

技术制裁已成为美国全球技术战略的工具，通过将技术标准之争上升为“民主科技同盟”的文明冲突之争来达到其地缘政治博弈与意识对抗的目的。2022年4月，美国、欧盟等60个国家和地区共同签署《互

① 337调查是美国国际贸易委员会(International Trade Commission, ITC)依据美国《1930年关税法》第337节的有关规定,针对进口贸易中的知识产权侵权行为以及其他不公平竞争行为开展调查,裁决是否侵权及有必要采取救济措施的一项准司法程序。

联网未来宣言》，实质上将技术标准与特定政治理念绑定，试图将技术竞争包装为价值观对抗。

2 关键技术管制信号感知体系的基本框架与功能定位

2.1 基本框架

美国对关键技术管制信号的感知分为3个主要阶段：关键技术管制信号感知主体实现技术感知与技术锁定，评估主体实现对技术的评估与风险识别，响应主体则实行技术管制响应与动态制裁。而在这一过程中参与主体通过黑箱机制、灰箱机制与白箱机制等弱信号感知机制收集多源信息情报，从而完成对“技术威胁”的感知、评估与制裁（图1）。

2.2 参与主体与功能定位

将美国参与关键技术管制信号感知响应的主体分为核心层、协调层和配合层（图2）。

核心层主要包括美国联邦政府机构。BIS负责识别涉及国家安全的两用技术和新兴技术，实施许可证制度限制技术输出；美国财政部外国资产办公室（OFAC）负责金融制裁与资产封锁；美国国防部（DOD）负责识别和评估军事技术威胁，定期评估武器系统和太空资产等嵌入式技术的漏洞；美国商务部下属的美国国家标准与技术研究院（NIST）负责制定技术标准和提供计划保障，如NIST根据《综合贸易

和竞争力法案》提出关键技术计划。

协调层主要为顾问协调与情报机构。国会研究服务部（CRS）为国会提供量子信息、人工智能（AI）、5G通信等领域的全球研发动态评估，揭示技术转移风险；总统科技顾问委员会（PCAST）提供技术咨询；美国白宫科技政策办公室提供科学技术建议并推动跨部门科技政策制定；美国国家科学技术委员会（NSTC）配合美国白宫科技政策办公室工作，协调科技决策过程；美国联邦调查局（FBI）负责技术与人员调查；美国中央情报局（CIA）获取技术海外交易情报；美国国家安全局（NSA）通过全球监控网络截获通信数据，识别潜在威胁行为模式。

配合层主要包括智库和专家。美国国际战略与国际研究中心（CSIS）、新美国安全中心（CNAS）等智库发布战略与技术风险报告；学术界专家推动“技术脱钩”理论研究；技术专家负责技术漏洞分析与供应链依赖评估。

3 “技术威胁”弱信号情报感知分析

弱信号指那些模糊且容易被忽视，但可能预示重大变化或威胁的早期迹象^[20]。本文中，“技术威胁”弱信号情报感知是指通过对早期、模糊、碎片化且易被忽视的征兆性信息情报的分析，识别“技术威胁”迹象并及时采取措施降低科技安全风险的能力。以下

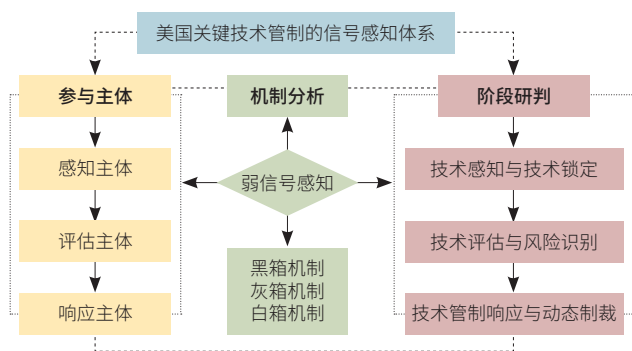


图1 美国关键技术管制的信号感知体系

Figure 1 Signal perception system for key technology regulation in the United States

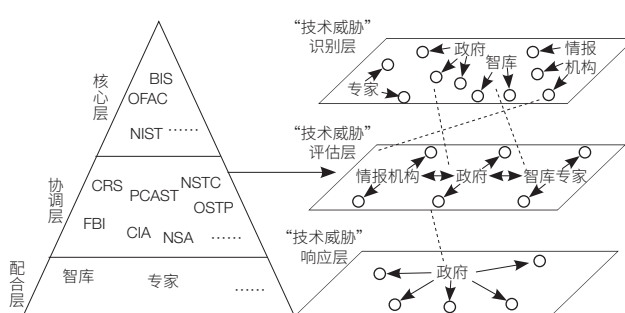


图2 美国关键技术管制的信号感知体系参与主体结构

Figure 2 Main structure of signal perception system involved in regulation of key technologies in the United States

将从情报来源与机制2个方面分析美国如何进行“技术威胁”的感知。

3.1 “技术威胁”弱信号情报来源分析

美国对“技术威胁”的感知已经形成覆盖智库、政府、企业、媒体等的蛛网式情报网络，实现了从线性监测向复杂适应系统的转变。

3.1.1 情报来源点1：智库

美国智库在感知“技术威胁”中扮演“战略瞭望塔”角色，通过系统性研究构建威胁全景图。例如，2023年5—6月，美国科技政策智库乔治城大学安全与新兴技术中心（CSET）联合新美国安全中心连续发布了名为《控制通过云服务访问先进计算：美国决策者的选择》系列报告^[21,22]，指出虽然芯片出口受管制，但企业仍可通过美国云服务访问其所需的先进AI算力，建议政府将此纳入监管。2024年1月，拜登政府提议要求美国云计算公司确定外国实体是否正在访问美国数据中心以训练AI模型。

3.1.2 情报来源点2：技术与情报专家

技术与情报专家凭借专业知识和敏锐洞察，成为美国感知“技术威胁”情报的重要一环。2019年，哈佛大学法学院教授、前奥巴马总统科学技术和创新政策特别助理 Crawford^[23]在《连线》（Wired）杂志撰文指出，美国需重视关键数字基础设施的全球布局，确保本国企业拥有公平参与国际市场的机会，避免因技术标准或准入规则差异导致美国企业竞争力受损。这些观点随后被美国国防部《5G生态系统：对美国国防部的风险与机遇》^[24]报告引用。

3.1.3 情报来源点3：政府文件与政策

政府文件中的重点技术是感知“技术威胁”的重要来源，包括2个方面。① 美国政府文件中的重点技术，被列入其中的技术是美国的重点感知对象。其中，《关键和新兴技术清单》已成为美国国家技术发展的风向标。2020年10月，美国白宫发布《关键与新兴技术国家战略》，详述了美国为保持全球领导

力而强调发展“关键与新兴技术”的计划，提出两大战略支柱，并明确了20项关键与新兴技术的清单。2022年2月，美国政府更新《关键和新兴技术清单》，在原有基础上调整技术领域，新增定向能技术、金融技术、高超音速技术等领域，并详列各领域核心技术子项^[31]。2024年2月的最新版本将核能技术、金融技术分别并入清洁能源技术、数据和网络安全技术领域，同时新增定位、导航和定时技术领域。2024版清单重点加强了AI、数据和网络安全、下一代通信、无人系统、定位导航、空间技术等方面的布局。这些清单所列技术既是美国关键技术领域的优先发展方向，也是其感知“技术威胁”和加强国家安全的重要领域。② “目标国家”政府文件中的技术。例如，2019年俄罗斯总统普京签署命令，批准2030年前俄罗斯国家人工智能发展战略；2022年俄罗斯国防部创新发展总局局长表示俄罗斯军方已成立人工智能技术发展办公室，致力于开发人工智能武器加快推动人工智能技术在军用和特种装备武器领域的应用。而自2022年俄乌冲突爆发以来，美国对俄罗斯实施了半导体制造设备和芯片的禁运，限制俄罗斯获取高科技产品和关键供应链，以削弱其军事和经济能力。

3.1.4 情报来源点4：新闻媒体

新闻媒体作为舆情放大器与认知战前线，是美国感知“技术威胁”的另一重要来源。2019年3月，美国有线电视新闻网（CNN）基于本土基础设施调研指出，部分涉及国防设施的区域在通信技术部署中存在供应链依赖风险。对此，专家提醒应将技术应用场景的安全性评估纳入更系统化的考量^[25]。同年8月，《华尔街日报》通过技术合作案例分析，提醒可能存在的监控风险^[26]。这类媒体舆论使技术威胁成为大众共识，从而使美国政府在后续实施技术制裁时更易获得公众支持。

3.1.5 情报来源点5：头部科技企业

企业是感知“技术威胁”的前沿，尤其是与美国政府关系密切的头部科技企业，其提交的报告或提案往往成为重要的威胁情报来源。2025年3月13日，美国OpenAI公司向特朗普政府提交《人工智能行动纲领》提案^[27]，其中在评估全球技术生态时指出，中国AI企业深度求索（DeepSeek）公司受中国政府资助和控制，是关键基础设施。OpenAI强调DeepSeek将如华为一样，对“民主世界”构成重大国家安全风险。

3.2 “技术威胁”弱信号情报感知机制分析

本文将美国感知“技术威胁”的弱信号机制分为“黑箱”机制、“灰箱”机制与“白箱”机制3类。

3.2.1 “黑箱”机制

“黑箱”机制指无法从开源情报中获取明确的“技术威胁”感知线索，感知过程不透明，但可以从技术制裁结果进行合理推断的机制。美国感知“技术威胁”“黑箱”机制的本质是知识权利、技术权利与政治权利的合谋，涉及特定利益集团与权利结构的互动。少数掌握专业话语权的精英通过非透明的政治网络，将个体立场或商业利益转化为国家战略行动，模糊了公共利益与私人议程的边界。例如，特朗普第一任期内的贸易顾问彼得·纳瓦罗（Peter Navarro）长期渲染“中国威胁论”，是美国发动贸易战的关键设计者。2018年4月，美国商务部以中兴通讯违反美国《出口管理条例》（EAR）为由，实施了为期7年的出口禁令^[28]；2019年5月又将华为及其68家关联公司列入“实体清单”。

3.2.2 “灰箱”机制

美国对“技术威胁”感知的另一机制呈现“结构性灰箱”特征，即在表面程序正当性之下，存在关键信息遮蔽与利益嵌入的制度性模糊空间。该机制通过将行业利益诉求嵌入制度性议程，并借助专业话语体系选择性披露信息，最终在“国家安全审查”“技术风险评估”等合法化框架下，形成具有排他性与模糊

性的决策空间。这种“灰箱化”的运作主要体现在2个层面。① 决策参与主体的多重身份特性。美国智库、产业联盟与政府部门之间构建的“旋转门”网络，使技术政策制定呈现出公私边界消融的特征。以新美国安全中心为例，该中心可查的研究人员中，超过半数具有军队退役或国防部文职背景。2021年新美国安全中心发布《边缘网络，核心策略：保护美国的6G未来》报告^[29]，其政策建议与美国联邦通信委员会（FCC）后续的频谱管理和国际合作行动高度关联。这种身份的转换使“技术威胁”感知既获得学术权威背书，又能通过行政渠道直接转化为技术制裁。② 政策论证过程的方法论遮蔽。例如，美国技术审查机构常以保密性为由，规避对分析模型与数据来源的同行评议。这种利益关联性与方法论“黑箱”的叠加，使技术遏制政策既难以被客观证伪，又倾向于放大威胁叙事。

3.2.3 “白箱”机制

“白箱”机制是指美国形成的多维度、全频谱的“技术威胁”感知方式，其核心是将零散弱信号转化为可操作的威胁情报，通过多源异构数据的地平线扫描与重点数据审查，形成蛛网式技术情报网络，实现全方位威胁感知。技术地平线扫描包括技术市场情报监测、专利分析、科学计量分析、文献分析与快速评估、政府征询公众建议、科学家和决策者研讨会，以及谷歌趋势、投资趋势等关注度分析^[30]。重点数据审查指向特定目标。例如，2009年美国国家安全局通过网络渗透华为深圳总部的服务器，获取1400多个客户的资料和内部培训文件^[31]。随后又以“出口管制”为名，要求全球芯片代工厂（如台积电公司）提交涉华企业订单数据。在数据采集后，政府、智库和相关机构运用算法、专家分析和历史经验识别潜在威胁模式。例如，美国人工智能国家安全委员会（NSCAI）就负责识别美国在技术优势、国际合作与竞争趋势等方面的态势。

4 美国“技术威胁”评估模式与方法分析

4.1 评估模式

4.1.1 法律框架下的标准化评估模式

法律框架下的标准化评估模式依据美国现有关键法律框架中的技术与威胁事项，实施“技术威胁”评估。《国防生产法案》强化了对关键技术的供应链控制。《出口管制改革法案》（ECRA）将“新兴技术”和“基础技术”纳入出口管制范畴，并授权BIS对这2项概念进行具体定义。《国际紧急经济权力法案》（IEEPA）授权总统在国家安全受威胁时实施制裁。这些法案为美国《出口管理条例》提供法律基础，BIS依据EAR定期评估技术并更新实体清单和其他出口管制清单。在此法律框架下，美国执行对“技术威胁”的流程化评估，包括评估是否涉及军事用途、是否影响美国技术领先地位、是否存在供应链风险等。

4.1.2 多部门联合评估模式

多部门联合评估模式是美国通过整合多个部门，利用情报共享、技术评估和法律工具，将技术问题上升为国家安全议题，形成跨领域政策输出的评估模式。2023年，美国司法部和商务部成立“颠覆性技术打击小组”^[32]，旨在遏制其他国家非法获取美国敏感技术，重点关注超算和超大规模计算、AI、先进制造设备及材料、量子计算、生物科学等领域^[33]。该小组成员来自美国联邦调查局、国土安全调查局和14个美国检察官办公室。通过多部门协作，该小组能够综合分析司法部和商务部的情报数据，快速完成技术威胁评估。

4.1.3 国际协调与盟友互动模式

国际协调与盟友互动模式将多部门联合评估扩展至国家和国际组织层面。其核心目标是填补技术

评估与管制漏洞、强化单边制裁效果、构建全球性技术壁垒。该模式既利用盟友的技术、市场和情报资源，又通过政治联盟将技术议题“泛安全化”。例如，美国通过“五眼联盟”获取技术扩散情报和评估技术风险；同时，与欧盟、日本等盟友实施同步技术管制，并组建“芯片四方联盟”（CHIP4）等，协调技术出口政策。

4.2 评估方法

4.2.1 制定战略评估框架

美国建立了系统的战略评估框架，从技术、对手生态和国内生态3个维度评估他国技术威胁。该框架评估技术的市场成熟度、技术瓶颈、地缘政治战略价值和商业价值等因素。2025年2月，美中经济安全审查委员会（USCC）举行“中国制造2025”听证会，在此框架下深入分析了中国在生物技术、民用航空、机器人与AI等高科技产业的发展现状、潜在优势及对美国构成的挑战^②。

4.2.2 多维度情报数据分析

美国结合自上而下的数据驱动和自下而上的专家驱动方式，通过多维度情报数据分析技术实力的真实水平和全球相对地位。同时运用多学科模型，结合专家意见对关键技术领域进行深入解析，评估“技术威胁”。美国科学基金会（NSF）发布的《保障美国的未来：关键技术评估框架》采用了这一方法。

4.2.3 闭门会议研讨

美国通过闭门听证会与机密备忘录等非透明方式评估技术威胁，构建“决策信息茧房”，排除异议。2023年9月，美国国会举办“AI洞察论坛”，美国参议员与埃隆·马斯克、比尔·盖茨、扎克伯格等科技领袖闭门讨论AI监管与安全风险，达成符合美国利益的技术监管共识。

② U.S.-China Economic and Security Review Commission. Made in China 2025—Who is winning?. (2025-02-06)[2025-03-29]. <https://www.uscc.gov/hearings/made-china-2025-who-winning>.

5 美国“技术威胁”感知的决策响应分析

在对“技术威胁”进行响应决策时，美国主要采用技术出口管制、经济制裁与域外效力实施、供应链重塑战略、贸易资源管控与国际同盟建立，以及技术人才限制与拉拢手段（表1）。

5.1 技术出口管制

美国对技术出口的管制涵盖技术和产品本身及其承载载体（实体）。通过全面管控各类技术形式，美国有效遏制技术的转移与扩散。管制范围主要包括军用技术、军民两用技术、核技术等领域，同时对技术承载实体实施管制。

军用技术出口管制主要依据《武器出口管制法》（AECA）及其配套《国际武器贸易条例》（ITAR）执行。ITAR规定对军品出口、再出口或转移，军事技术数据向外国人发布，国防服务活动，以及与禁止国家和不合格实体相关的活动均需管制。美国国防部的国防贸易管制局（DDTC）通过《美国军需品清单》（USML）明确列出受管制军品项目。军民两用技术出口管制主要由《出口管制改革法案》（ECRA）和《出口管制条例》构成。2018年通过的ECRA特别加强了对“新兴技术和基础性技术”的管控，将重点从“军事用途”转向“全面保持美国的技术领先地位”。即使某些技术不具军事用途且不属于“军民两用物项”，仍可能被纳入管控范围^[34]。核技术领域则主要依据《1954年原子能法》执行管制。在实体管制方面，主要工具包括《实体清单》（EL）、《未经核实清单》（UVL）、《最终军事用户清单》（MEU）及《被拒绝人员清单》（DPL）。这些工具弥补了USML和《商品管制目录》（CCL）在技术识别上的滞后性。

5.2 经济制裁与域外效力实施

美国通过经济手段对目标国家或实体施压，促使其遵守政策要求。这不仅直接影响目标国的经济稳定，还影响其关键技术发展和国际合作，从而实现间

接技术制裁。美国的经济制裁分为直接经济制裁和法律域外效力两类。直接经济制裁采用分级管控：一级制裁通过资产封锁、禁止交易等手段实施国家级打击；二级金融制裁通过制裁名单精准锁定特定实体，利用美元霸权迫使全球金融机构配合；行业制裁则通过限制技术输出与合作，削弱目标国特定产业竞争力，主要针对能源、国防及高科技领域^[35]。美国的经济制裁主要由美国财政部外国资产控制办公室（OFAC）负责执行，其管理的制裁清单包括《特别指定国民和被封锁人员清单》（SDN）、《非特别指定国民和被封锁人员清单》（Non-SDN List）、《非SDN军事综合体企业清单》（NS-CMIC）、《行业制裁识别名单》（SSIL）等。

在域外效力方面，美国制定了《反海外腐败法》（FCPA）等长臂管辖工具。该法于1977年制定，旨在禁止美国企业向外国公职人员行贿，经过1988年和1998年2次重大修订，逐步将管辖范围扩大至外国企业与自然人。法国阿尔斯通公司就是一个典型案例。该公司在核电站建设领域处于行业领先地位，但因与美国通用电气公司存在直接竞争，遭遇美国域外管辖，导致多名高层管理人员因涉嫌贿赂被美国当局逮捕，该公司也被处以巨额罚款^[36]。

5.3 供应链重塑策略

美国应对“技术威胁”的重要手段是供应链重塑，通过联盟式供应链、法律与财政“组合拳”及威慑施压等方式重塑全球产业链布局，降低对竞争对手的关键技术依赖，巩固技术霸权地位。例如，在联盟式供应链方面，美国发起CHIP4，将中国排除在全球半导体供应链联盟之外。在法律与财政方面，美国通过《芯片与科学法案》提供527亿美元补贴，吸引台积电、三星等企业在美建厂，同时要求受补贴企业不得在“受关注的国家”扩产芯片。通过《通胀削减法案》，美国将新能源汽车税收优惠限定于北美组装和盟友电池材料，迫使宁德时代改用技术授权而非直接

投资进入美国市场。美国还通过威慑施压手段迫使他国加入供应链重构。例如，2023年4月中国对美光（Micron）启动网络安全审查后，美国要求韩国政府敦促三星、SK海力士不得填补美光可能留下的市场空缺，以阻止中国通过韩国企业维持存储芯片供应链稳定，同时巩固美国在半导体产业链中的主导地位。

5.4 贸易资源管控与国际同盟建立

美国采取双管齐下的策略，一方面通过贸易资源控制阻断竞争对手的技术升级路径，另一方面将资源供应链向政治盟友倾斜，建立排他性技术联盟，实现对技术的联合封锁。

2025年4月，美国国立卫生研究院（NIH）发布《实施更新：增强NIH受控访问数据的安全措施》文件，宣布自4月4日起，禁止受关注国家/地区访问NIH受控访问数据存储库及相关数据，从源头阻碍技术升级。美国贸易代表办公室（USTR）作为制定和调整国际贸易、投资、知识产权等政策的核心机构^[37]，于2018年启动“301调查”，审查中国的技术转让、知识产权及创新领域的法律、政策和做法。基于调查结果，特朗普总统签署备忘录，限制中国企业对美投资和并购，并对中国进口商品加征高额关税^[38]。美国通过关税壁垒（高额进口关税）和非关税壁垒（进口许可证制、配额制、本国商品优惠等），限制外国商品自由进口，保护本国技术在国内外市场的竞争力。

此外，美国通过技术联盟加强技术标准合作与协调，在关键领域制定排他性标准。美国主导的《关于常规武器和两用物品及技术出口控制的瓦森纳安排》建立了技术管制的多边协同框架，通过军事装备和军民两用技术双清单体系实施战略性出口控制。该机制2023年完成第17次扩容，新增人工智能训练芯片、量子计算软件等12类战略性技术管制，形成覆盖半导体、基础电子、前沿计算等领域的立体封锁体系。美国与日本、印度、澳大利亚组成的“四方安全对话”

（Quad）成为技术标准合作平台。2019年5月，美国领导32个国家通过首个5G通信安全规则《布拉格提案》（*Prague Proposal*），从政策、安全、技术、经济方面探讨建立跨国一致的技术准入评估机制^[38]。

5.5 技术人才限制与拉拢

美国采取双向策略应对技术人才问题。一方面，加强对技术领域合作的评估，如收紧中国留学生和学者签证政策，限制敏感技术人员交流。另一方面，美国积极争夺全球技术人才，如《芯片与科学法案》就授权NSF通过“未来半导体计划”（Future of Semiconductors）支持半导体技术研发和人才培养。

6 结语

本文研究美国对关键技术管制信号感知的3个主要阶段，即前端技术感知与锁定、中端技术评估与风险识别、后端技术管制响应与动态制裁，并分析核心层、协调层和配合层的参与主体与定位，揭示美国“技术威胁”情报感知体系在识别情报来源、评估模式方法和响应决策手段等流程和运行机制。“技术威胁”感知体系是一套复杂决策系统，也是今后一段时期构建体系化科技安全情报范式的主攻方向之一。本文从技术情报范式、感知研究能力、预警协调能力等方面提出思考启示。

（1）加快技术情报范式升维，构建新型全球技术竞争情报图谱，推动情报研究从跟踪式向预见性技术战略预警转变。通过技术领域多源异构实体的统一，解决概念-实体-关系语义网络映射问题，对专利、学术文献、资本流动及行业报告等信息进行层次化抽象，实现多模态语义对齐。结合时序预测与异常检测等方法，对技术成熟度、创新产出速率及投资热度进行动态监测，捕获潜在的技术突变点，进一步研判明确关键技术节点、核心研发机构及供应链关键环节，并将进出口物流数据纳入整体视图，形成对关键技术风险的实时全景感知。

表1 美国“技术威胁”响应制裁手段

Table 1 US responds to sanctions for “technological threat”

制裁类型		法律依据/决策标准	主要执行主体	管制工具与手段
技术出口管制	军用技术出口管制	《武器出口管制法》(AECA) 及其施行条例《国际武器贸易条例》(ITAR)	美国国防贸易管制局(DDTC)	《美国军需品清单》(USML)
	军民两用技术出口管制	《出口管制改革法案》(ECRA)、《出口管制条例》(EAR)、《针对关键技术和相关产品的出口管制框架》	美国商务部工业与安全局(BIS)	《商品管制目录》(CCL)、《商业国家目录》(CCC)
	核技术出口管制	《1954年原子能法》	美国能源部(DOE)、美国核管理委员会(NRC)	—
	实体管制	《出口管制条例》(EAR)	美国商务部工业与安全局(BIS)	《实体清单》(EL)、《未经核实清单》(UVL)、《最终军事用户清单》(MEU)、《被拒绝人员清单》(DPL)
经济制裁与域外效力实施		《国际紧急经济权力法》(IEEPA)、《国家紧急状态法》(NEA)、《反海外腐败法》(FCPA)	美国财政部外国资产控制办公室(OFAC)	《特别指定国民和被封锁人员清单》(SDN List)、《非特别指定国民和被封锁人员清单》(Non-SDN)、《非SDN军事综合体企业清单》(NS-CMIC)、《行业制裁识别名单》(SSIL)等
供应链重塑策略		—	美国联邦政府	联盟式供应链
	供应链重塑策略	《芯片与科学法案》《通胀削减法案》等	美国联邦政府	法律与财政组合拳
		—	美国联邦政府	威慑施压
	贸易管控	《1974年贸易法》《1988年综合贸易与竞争法》	美国贸易代表办公室(USTR)	“301调查”、关税壁垒措施、非关税壁垒措施
贸易资源管控与国际同盟建立	技术同盟	—	各签约国政府	强化多边联盟的技术标准合作与协调、关键领域制定排他性技术标准
	科研数据库资源限制	《关于防止受关注国家获取美国人大规模敏感个人数据及美国政府相关数据的行政命令》	美国国立卫生研究院(NIH)	禁止受关注国家/地区访问NIH受控访问数据存储库及相关数据
技术人才流动限制	签证与学术交流管制	《经济间谍法》	美国司法部(DOJ)、美国众议院等	“中国行动计划”、留学生审查等
	国际人才竞争干预	《人工智能安全、可靠和可信发展行政令》《芯片与科学法案》等	美国国家科学基金会(NSF)	放宽人才绿卡申请、项目与资金支持等

(2) 加强“技术威胁”感知研究能力建设。在国家层面设立科技安全预警机构，在人工智能、半导体、航空航天、生物医药等战略领域设立战略科学家领导的领域研判小组，以场景化预警报告和全景风险

图为核心产出。科技安全预警机构应构建跨学科人才队伍，长期开展技术风险评估研究工作，开发面向企业和科研院所等创新一线的技术安全评分工作。

(3) 建立跨部门跨行业的协同治理框架。构建由

产业主管部门、科技行政部门、网络安全主管机构及宏观经济主管部门共同参与的国家技术安全联席决策机构,实现统一指挥、快速决策,以保证风险评估报告能够及时转化为行政行动。同时,建设统一的技术情报共享平台,将海关、税务、金融监管等多源数据接入,实现跨部门数据治理、标准化和隐私合规,并对企业提供自查接口,形成信息的双向流通。积极参与与多边技术管制框架,推动技术安全信息交换协定的签署,并在主要国际伙伴之间建设联合监测中心,实现跨境情报共享与协同响应,形成从感知、评估到制裁的全链条、全周期的预警与防御体系。

参考文献

- 傅晋华. 科技安全概念演化、问题辨析与体系构建研究. 科学学研究, 2024, 42(9): 1824-1832.
Fu J H. Research on concept evolution, issues analysis and system construction of science and technology security. Studies in Science of Science, 2024, 42(9): 1824-1832. (in Chinese)
- 刘昊, 张志强, 武瑞敏. 建设适应科技竞争与国家安全的科技情报发展体系. 图书与情报, 2022, (1): 39-48.
Liu H, Zhang Z Q, Wu R M. Building a scientific and technological intelligence development system suitable for scientific and technological competition and national security. Library & Information, 2022, (1): 39-48. (in Chinese)
- 刘晓峰, 胡高强, 范兆媛, 等. 科技安全风险监测预警体系构建研究. 中国工程科学, 2024, 26(3): 186-195.
Liu X F, Hu G Q, Fan Z Y, et al. Construction of a technological security risk monitoring and early warning system. Strategic Study of CAE, 2024, 26(3): 186-195. (in Chinese)
- 李维思, 邹亭玉, 毛进, 等. 面向国家科技人才安全服务的科技情报态势感知研究. 情报理论与实践, 2025, 48(6): 20-28.
Li W S, Wu T Y, Mao J, et al. Research on intelligence situation awareness for national scientific and technological talent security service. Information Studies: Theory & Application, 2025, 48(6): 20-28. (in Chinese)
- Jonker M, Romijn H, Szirmai A. Technological effort, technological capabilities and economic performance. Technovation, 2006, 26(1): 121-134.
- Porter A L, Roessner J D, Jin X Y, et al. Measuring national “emerging technology” capabilities. Science and Public Policy, 2002, 29(3): 189-200.
- Evans S W, Leese M, Rychnovská D. Science, technology, security: Towards critical collaboration. Social Studies of Science, 2021, 51(2): 189-213.
- AlDaajeh S, Saleous H, Alrabace S, et al. The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 2022, 119: 102754.
- 李品. 统筹科技发展与科技安全的情报体系框架研究. 情报学报, 2024, 43(3): 357-368.
Li P. Constructing the framework of an intelligence theory system for coordinating science and technology development and science and technology security. Journal of the China Society for Scientific and Technical Information, 2024, 43(3): 357-368. (in Chinese)
- 肖冬梅, 王良晨. 美国技术民族主义制度对中国产业发展的挑战及应对. 科技进步与对策, 2025, 42(17): 44-54.
Xiao D M, Wang L C. Challenges and countermeasures of U. S. techno-nationalism system on the development of China's industries. Science & Technology Progress and Policy, 2025, 42(17): 44-54. (in Chinese)
- 李琪, 叶继元. 面向美国出口管制的关键核心技术竞争情报服务体系构建. 情报杂志, 2025, 44(1): 81-87.
Li Q, Ye J Y. Construction of key core technology competitive intelligence service system oriented to U. S. export controls. Journal of Intelligence, 2025, 44(1): 81-87. (in Chinese)
- 贺德方, 李广建, 汤富强, 等. 国外技术出口管制演进分析与应对策略研究. 中国科学院院刊, 2024, 39(1): 79-94.
He D F, Li G J, Tang F Q, et al. Research on evolution and countermeasures of international technology export controls. Bulletin of Chinese Academy of Sciences, 2024, 39(1): 79-94. (in Chinese)
- 姜辉. 美国出口管制的政策体系及协调机制研究. 情报杂志, 2024, 43(12): 88-94.

- Jiang H. Research on the policy system and coordination mechanism of U. S. export control. *Journal of Intelligence*, 2024, 43(12): 88-94. (in Chinese)
- 14 赛超, 李峥, 刘巍. 制裁冲击与企业风险: 基于美国对华单边管制清单的研究. *金融评论*, 2024, 16(4): 58-86.
- Dou C, Li Z, Liu W. Sanctions shock and corporate risk: A study based on the US control list against China. *Chinese Review of Financial Studies*, 2024, 16(4): 58-86. (in Chinese)
- 15 Gilpin R, War and Change in World Politics. Cambridge: Cambridge University Press, 1981.
- 16 尹小平, 郭懿萦, 李天琦. 美国贸易制裁下日本半导体产业的由盛转衰及其启示. *现代日本经济*, 2023, 42(3): 35-49.
- Yin X P, Guo Y Y, Li T Q. Japan's semiconductor industry's transition from strength to weakness under U. S. trade sanctions and its enlightenment. *Contemporary Economy of Japan*, 2023, 42(3): 35-49. (in Chinese)
- 17 赵明昊. 技术鹰派、国家安全与美国对华战略竞争. *国际安全研究*, 2025, 43(1): 115-132.
- Zhao M H. Technology hawks, national security and the U.S. strategic competition against China. *Journal of International Security Studies*, 2025, 43(1): 115-132. (in Chinese)
- 18 Bureau of Industry and Security, Department of Commerce. Revisions to the Entity List. Washington DC: BIS, 2024.
- 19 张美云, 宋宇. 国家经济安全思想: 马克思主义经济学和西方经济学的比较. *改革与战略*, 2023, 39(3): 34-45.
- Zhang M Y, Song Y. National economic security thought: A comparison between marxist economics and western economics. *Reformation & Strategy*, 2023, 39(3): 34-45. (in Chinese)
- 20 余辉, 吕星仪, 夏文蕾, 等. 科技竞争态势下的技术需求弱信号感知研究. *情报杂志*, 2024, 43(12): 106-116.
- Yu H, Lyu X Y, Xia W L, et al. Research on weak signal perception for technology demand under the intense trend of technological competition. *Journal of Intelligence*, 2024, 43(12): 106-116. (in Chinese)
- 21 Dohmen D, Feldgoise J, Weinstein E S, et al. Controlling Access to Advanced Compute via the Cloud: Options for US. Policymakers, Part I. (2023-05-16) [2025-09-22]. [https://www.cnas.org/publications/commentary/controlling-access-to-advanced-compute-via-the-cloud-options-for-u-s-](https://www.cnas.org/publications/commentary/controlling-access-to-advanced-compute-via-the-cloud-options-for-u-s-policymakers-part-i)
- policymakers-part-i.
- 22 Dohmen D, Feldgoise J, Weinstein E S, et al. Controlling Access to Advanced Compute via the Cloud: Options for US. Policymakers, Part II. (2023-06-05) [2025-09-22]. <https://cset.georgetown.edu/article/controlling-access-to-compute-via-the-cloud-options-for-u-s-policymakers-part-ii/>.
- 23 Crawford S. China will likely corner the 5G market—and the US has no plan. (2019-02-20) [2025-03-12]. <https://www.wired.com/story/china-will-likely-corner-5g-market-us-no-plan/>.
- 24 MedinM, Louie G. The 5G ecosystem: risks & opportunities for DoD. (2019-04-03) [2025-03-12]. https://media.defense.gov/2019/Apr/03/2002109302/-1/1/0/DIB_5G_STUDY_04.03.19.PDF.
- 25 CNN. Huawei connects rural America. Could it threaten the country's most sensitive military sites?. (2019-03-11) [2025-03-12]. <https://edition.cnn.com/2019/03/11/politics/huawei-cell-towers-missile-silos/>.
- 26 Parkinson J, Bariyo N, Chin J. Huawei technicians helped African governments spy on political opponents. (2019-08-15) [2025-03-12]. <https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017>.
- 27 OpenAI. OpenAI's proposals for the U. S. AI action plan. (2025-03-13) [2025-03-29]. <https://openai.com/global-affairs/openai-proposals-for-the-us-ai-action-plan/>.
- 28 张宇燕, 冯维江. 如何理解中美贸易摩擦. *光明日报*. 2018-04-24(15).
- Zhang Y Y, Feng W J. How to understand the trade friction between China and the United States. *Guangming Daily*. 2018-04-24(15). (in Chinese)
- 29 Rasser M, Riikonen A, Wu H. Edge networks, core policy securing America's 6G future. Washington DC: Center for a New American Security, 2021.
- 30 韩秋明. 美国国家关键技术选择的组织过程和主要方法研究. *全球科技经济瞭望*, 2023, 38(2): 1-8.
- Han Q M. Research on the organization process and major methods of the U. S. national key technology selection. *Global Science, Technology and Economy Outlook*, 2023, 38(2): 1-8. (in Chinese)

- 31 互联网新闻研究中心. 美国是如何监视中国的: 美国全球监听行动纪录. 北京: 人民出版社, 2014.
Internet News Research Center. How the United States Monitors China: A Record of Global Surveillance Operations by the United States. Beijing: People's Publishing House, 2014.
- 32 陈峰, 彭俊玲. 美国商务部工业与安全局情报工作透视. 情报杂志, 2024, 43(11): 1-10.
Chen F, Peng J L. Research on intelligence work of the bureau of industry and security of U. S. department of commerce. Journal of Intelligence, 2024, 43(11): 1-10. (in Chinese)
- 33 Office of Public Affairs, U.S. Department of Justice. Justice and commerce departments announce creation of disruptive technology strike force. (2023-02-16) [2025-03-29]. <https://www.justice.gov/archives/opa/pr/justice-and-commerce-departments-announce-creation-disruptive-technology-strike-force>.
- 34 陈喆, 陈佳贝, 张子莺. 新安全格局下中国技术安全管制立法的检视与完善. 世界科技研究与发展, 2023, 45(6): 679-692.
Chen Z, Chen J B, Zhang Z Y. Examination and improvement of China's technology safety control legislation under the new security pattern. World Sci-Tech R & D, 2023, 45(6): 679-692. (in Chinese)
- 35 罗兰. 美国的全球经济制裁——跨境合规视角. (2022-11-28)[2025-03-29]. <https://www.deheng.com/yjy/lssd/28012.html>.
Luo L. Global economic sanctions by the United States: A cross-border compliance perspective. (2022-11-28)[2025-03-29]. <https://www.deheng.com/yjy/lssd/28012.html>.
- 36 李玲. 中国应对美国长臂管辖的法律路径. 中国外资, 2025, (1): 100-103.
Li L. The legal path for China to respond to the long arm jurisdiction of the United States. Foreign Investment in China, 2025, (1): 100-103. (in Chinese)
- 37 蔡翠红. 大变局时代的技术霸权与“超级权力”悖论. 人民论坛·学术前沿, 2019, (14): 17-31.
Cai C H. Technological hegemony and the paradox of “superpower” in the age of great change. Frontiers, 2019, (14): 17-31. (in Chinese)
- 38 唐新华. 西方“技术联盟”: 构建新科技霸权的战略路径. 现代国际关系, 2021, (1): 38-46.
Tang X H. Techno democratic alliances: Strategic path for new technological hegemony. Contemporary International Relations, 2021, (1): 38-46. (in Chinese)

Research on signal perception system of key technology regulation in the United States

WANG Kaile¹ LIU Hao^{1,2*} CHEN Yunwei^{1,2}

(1 Scientometrics & Evaluation Research Center, National Science Library (Chengdu),

Chinese Academy of Sciences, Chengdu 610299, China;

2 Department of Information Resources Management, School of Economics and Management,

University of Chinese Academy of Sciences, Beijing 100190, China)

Abstract The purpose of the study is to analyze the operation mechanism of the key technology control signal perception system, and reveal the deep logic and basic procedures of the United States' external technical containment. Through literature review and information mining, this study analyzes the structural features of the U.S. key technology control signal perception system, such as “front-end technical perception and technology locking”, “mid-end technical evaluation and risk identification”, and “back-end technical control response and dynamic sanctions”. It further explores the participating subjects and role positioning of the United States in key technology control signal perception, the sources and mechanisms of intelligence perception of weak signals, the models and methods of technical assessment, as well as the means of technical sanctions. The research on the U.S. key technology control signal perception system provides a reference for China to deal with the risks of the technology decoupling led by the United States and build an independent and controllable technology governance system.

Keywords science and technology security, key technology, intelligence perception, threat response, weak signal

王恺乐 中国科学院成都文献情报中心馆员。主要研究领域为科技安全情报、科技政策等。E-mail: wangkl@clas.ac.cn

WANG Kaile Librarian of National Science Library (Chengdu), Chinese Academy of Sciences (CAS). Her research focuses on scientific and technological security intelligence, science and technology policy, etc. E-mail: wangkl@clas.ac.cn

刘 昊 中国科学院成都文献情报中心创新研究部副主任、副研究员。主要研究领域为科技情报、科技政策等。E-mail: liuh@clas.ac.cn

LIU Hao Associate researcher and deputy director of the Innovation Research Department of National Science Library (Chengdu), Chinese Academy of Sciences (CAS). His research focuses on scientific and technological intelligence, science and technology policy, etc. E-mail: liuh@clas.ac.cn

■ 责任编辑：张帆

*Corresponding author