软件协议 / 模型权重 / 芯片算力底座 / 人类共同进步

出口管制对开源人工智能未来的影响

Vikrant Rathore

当技术管制不仅越过代码与模型权重，更深入晶圆、存储与万卡硬件集群：从思想公地到高墙关口的纪实与博弈推演。



23

AI 与芯片关口

05

生物医药

12

光伏装备

出口管制对开源人工智能未来的影响

Vikrant Rathore / CC BY-SA 4.0 Third-party materials retain their own copyrights and licenses. See NOTICE.

Jennifer Yuan, Vicky Ni, Ronak Rathore, Kanak Rathore
版本 2026-11-02
© 2026, Vikrant Rathore; original work CC BY-SA 4.0
2026-11-02
本书借助 GuideDog 构建，并获 Jennifer Yuan, Vicky Ni、Ronak Rathore 与 Kanak Rathore 鼎力协助。

目录

01. 知识设卡之日：当思想遇上海关岗亭 7
- 一个周五午后，两套截然不同的时钟 7
- 不装一个木箱，知识如何跨越国境 8
- 决定命运的四个法律档位 9
- 这对两支团队意味着什么 9

02. 四十道技术关隘：全景管制图谱 11
- 监管者如何用尺规丈量一种思想 11
- 看懂技术红线而不被红线绊倒 11
- 人工智能、算力芯片与超万卡集群（23 项管制点） 12
- 生物医药与基因治疗平台（5 项管制点） 14
- 光伏晶硅材料、超薄硅片与产线装备（12 项管制点） 14
- 这对两支团队意味着什么 15

03. 心智与硅基：模型、芯片与万卡集群 17
- 老面酵种、面包店窗口与铸铁烤炉 17
- 前沿大模型核心技术的三条触发红线（ `266504X` ） 18
- 数据安全红线（ `266501J` 与 `266504X(1)` ）及自主智能体（ `266505X` 与 `266502J` ） 18
- 中国 AI 清单深处的硬件底座：算力芯片、先进存储与万卡集群 19
- 这对两支团队意味着什么 19

04. 开放模型：公开发布与私有转移 21
- 开放许可只是发布的一部分 21
- 从具体文件开始 21
- 中国：当前登记与目录提案分开 21
- 美国：单独判断管辖 22
- 对开放模型的可能影响 22
- 独立审查及其局限 22
- 实用的发布记录 22
- 这对两支团队意味着什么 23

05. 生命的代码：基因平台与共享良方 25
- 留住活字印刷机，让良方典籍传遍天下 25
- 全球未公开全新靶点与生物安全红线 26
- 这对两支团队意味着什么 26

06. 将阳光装进机器：光伏工艺与核心装备 27
- 光伏组件畅行全球，“秘密厨房”设闸留存 27
- 注释 4：当物理装备 本身 就是核心配方 28
- 这对两支团队意味着什么 28

07. 华盛顿的守门人：算力芯片与模型权重 29
- 扼守全球算力的物理引擎 29
- 2026 年 1 月半导体新规：只是“允许敲门”，绝非敞开大门 29
- 美国 AI 模型权重规则（ `4E091` ）一波三折的奇特法律命运 30
- 华盛顿身旁另外两道闸门：跨境美元资本与大批量敏感数据 30
- 这对两支团队意味着什么 30

08. 两套边界体系与官方审批实操指南 31

同一座项目桥梁两端相遇的两种监管哲学 31
分步实操指南：如何办理信息登记或申领官方出口许可 32
中国篇：主管政府部门、法定审批时限与核验通讯录 33
美国篇：联邦监管机构、SNAP-R 电子申报流程与核验通讯录 34
这对两支团队意味着什么 35

09. 日常情境与实战：读者田野指南 37
我还能把 DeepSeek、Qwen 或其他开源模型下载到自己的电脑或服务器上运行吗? 37
既然软件挂的是 MIT 或 Apache 2.0 宽松协议，物理硬件管制还会影响开源 AI 吗? 37
如果海外用户通过网页对话使用我们的 AI 应用或调用云端 API，这算出口大模型吗? 37
我们的实验室和服务器都留在国内，但境外投资方正在收购公司控制权，需要办登记吗? 37
在正式开源发布或跨境合作前，一份两页纸的“发布合规护照”应当记录哪些内容? 38
六个真实世界实战场景 38

10. 原始文献、核验方法与通俗术语表 41
本书每一处事实是如何逐一核验的 41
写给普通读者的通俗术语表 41
全部 26 份经核验一手官方文献总表 42
本次审阅新增的研究与历史来源 43
作者、协助与再使用 44
可选阅读：核算博弈例子 44
可选阅读：独立审查不保证安全 44

知识可以分享而不被耗尽。杰斐逊 1813 年以蜡烛比喻： 借我的火点亮蜡烛，获得光而不使我变暗。 一个团队可以向另一个学习而不夺走其知识。 JEFFERSON



图 1 两支研究团队试图合作，边境障碍却阻滞了计算机部件和技术图纸的流动。

开放权重可能使小机构更有自主权。诊所、语言项目或大学可能在本地改进模型。这些是说明性用途，不是有记录的应用或临床安全证明；可下载权重也不同于完整开放 AI 定义。OSI R1 QWEN

共享模型只是开始。团队要把共享知识变成实用工具，还需要计算机，也需要持续向其他团队学习。

不止于软件与权重：托起开放心智的硬件底座

模型可以作为代码和学到的数字传播，训练和运行它的计算机却是实体机器。开放许可与机器的可获得性解决问题的不同部分。

模型依赖实体计算机。大型训练可能需要先进处理器、存储和网络，小模型可用较普通设备。不是所有使用者都需最新制程或万卡集群，但稀缺硬件仍可能影响谁能训练、检查和部署。

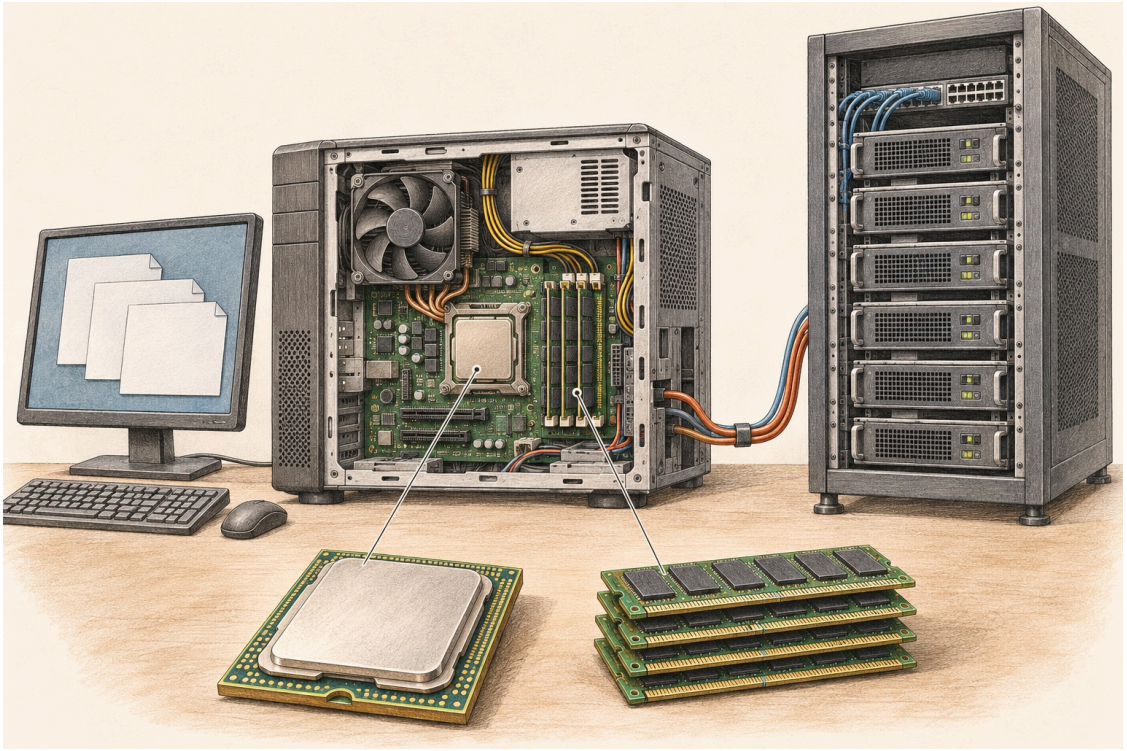


图 2 开放模型依赖芯片、存储与算力设施。限制一部分可能影响整体可用性。

- **硬件与设计知识：** 美国覆盖指定物项及符合条件的部分外国物项。中国提议覆盖指定设计和 **超过 1 万张** 加速卡集群的部分技术。设计知识、成品芯片和集群是不同管制对象。US26 EAR734 EAR742 CN-A1
- **模型与数据：** 中国于 **2026 年 10 月 16 日** 启动临时登记。目录拟以计算量、参数或合格前十评估作为替代条件。拟议类别、当前登记与美国权重规则须分开。 CN48 CN-A1 US25 GAO26

> **重要**
> 团队可能获准使用开放模型，却难以获得合适计算机。因此，我们同时追踪共享的知识及使用知识所需的硬件。

堡垒陷阱：双方如何一起受损

硬件问题引出政治问题。实用开放模型依赖许多团队的贡献，而各国政府又想保护本国能力。为争取国家优势作出的选择，为什么可能同时拖慢双方？我们用一张虚构的共享工作台来追踪这个问题。

两支团队，同一起点

设想 A 国与 B 国各有一支研究团队，都从同一公开 AI 模型出发，改进日常本地语言任务。A 队找到减少内存需求的方法，B 队开发发现错误的测试并协助修复。这些团队与贡献都是假设，不是实际部署记录。

如果交换下一轮改进，两队都能利用对方的成果。A 得到更好测试，B 得到资源需求更少的模型。双方仍需计算机、人员和时间。知识共享帮助利用资源，却不会让实体硬件免费。



图 3 两队共享部件和知识时能完成计算机，被墙隔开后却难以完成。这是书中假设博弈的示意，不是实测结果。

每个政府的两个选择

现在，政府为下一轮工作制定政策。各国都希望国内取得实用进展，也担心给予对方优势却得不到回报。我们把选择简化为两个：

- **共享：** 允许团队交换普通研究改进。
- **筑墙：** 广泛限制本国新贡献流向对方。

墙针对未来贡献，不能让已经公开的模型副本消失。团队保留起始文件，但下一轮改进可能无法互通。真实管制有更多选择，包括针对性限制与特定许可。我们先暂时放下这些复杂情况，看清一个激励问题。

先看四种结局，再看四个得分

我们给结局设定虚构的偏好得分。分数越高，表示政府在故事中越偏好这个结果。它综合了假设中的实用进展、保护与相对优势考量。这不是 AI 测试分、百分比或实测国家收益，公告也没有提供这些数字。

双方共享：各 17 分。 A 的内存优化到达 B，B 的测试与修复到达 A。双方无需独立重复每项发现，就能改进成果。我们用各 17 分表示相互合作的良好结果。

A 共享，B 筑墙：A 得 3 分，B 得 20 分。 B 利用 A 新公开的改进，却保留自己的新贡献。我们假设 B 最偏好这种单边优势，因此给 20 分。A 得 3 分，因为我们假设 A 政府不喜欢自己独自共享，而对方保护贡献。A 队仍能开展有用工作；3 分表示其政府在本例中最不偏好的结局。

A 筑墙，B 共享：A 得 20 分，B 得 3 分。 角色对调，A 获得单边优势，B 成为唯一共享的一方。我们赋予两国相同的假设优先次序，以展示战略问题，而不是把今天的美国或中国代入其中一方。

双方筑墙：各 5 分。 双方都得不到对方下一轮贡献，仍从公开起点继续工作，但需要更多重复劳动，或失去有用改进。我们假设政府宁愿保护自身贡献，也不愿独自共享，因此 5 高于 3；又假设双方都偏好相互合作胜过彼此隔离，因此 17 高于 5。

最关键的假设是 **20 优于 17**：政府在这一轮更重视单边优势，而非共同进展。这种偏好带来限制的诱惑。如果政府最看重共同进展，这个特定陷阱可能不会出现。数字只是表达假设的排序，不能证明真实政府具有这种偏好。 GAME

如何阅读博弈图

A 的选择决定一行，B 的选择决定一列。交点方格中，字母 A 旁是 A 的得分，B 旁是 B 的得分。例如右上格表示 A 共享、B 筑墙：A 得 3、B 得 20。绿色格表示相互共享，红色格表示相互限制。

假设偏好 / 分数越高越偏好

双方如何一起受损



双方都更愿意共享，而非共同筑墙。

只有在这些假设下，筑墙才是各自的最优回应。

分数说明故事中的偏好，不是实测影响。

图 4 两队的四种结局。分数是虚构偏好，本例中越高表示越偏好。

为什么筑墙开始显得更稳妥

A 政府考虑 B 可能怎么做。**如果 B 共享**，A 比较共享得 17 与保留自身贡献得 20。按我们的假设，A 选择筑墙以取得单边优势。图中对应左列两个格子的比较。

如果 B 筑墙，A 比较独自共享得 3 与也实行限制得 5。A 再次选择墙，这次是为了避免独自共享。图中对应右列两个格子的比较。

B 也作同样推理。无论对方如何，各国都能认为筑墙合乎自身利益。结果双方筑墙，各得 5 分，尽管双方都更愿意通过合作各得 17 分。即使没人希望共同结果变差，这种结果仍可能出现。

这就是 **囚徒困境**。结局也是 **纳什均衡**：只要另一道墙仍在，任何政府单独改变选择都无法提高得分。A 单独开放会从 5 降到 3。相互共享需要双方改变，或改变使合作值得的激励条件。 GAME

这如何帮助理解出口管制

故事为后续技术条目提出政策问题。政府可能把广泛限制视为保护或谈判筹码；从两国共同看，同样的限制也可能打断互补改进、增加重复劳动，让小团队更难工作。这些是待研究的机制，不是虚构得分测出的成本。

中美实际管制不是这个对称的二选一游戏。两国能力与法律工具不同。申报、禁止、普通许可、公开信息排除与便利发布路径，对合作的影响也不同。后续章节逐一分辨。我们不把所有申报要求都称为墙，也不把任何排除视为完全自由转移。

能防止严重伤害的针对性管制也可能改变结局排序。公开模型既有益处，也有滥用风险。政策任务是识别所控制的具体风险与所损失的合作，而非自动认定完全开放或广泛封闭就是答案。 NTIA OPENRISK

团队能否继续合作？

回到工作台。团队预计下月还会改进，之后继续改进。政府今天取得短期优势，可能失去它重视的未来合作。可信且持续的安排因此可能改变选择。是否有效取决于可观察的行动、未来交换价值和出错可能；承诺本身不能解决问题。

我们带着一个问题阅读全书： **哪些规则既应对具体危险，又为下一项有用贡献留下可行路径？** 从模型文件到硬件、医疗平台和光伏设备，共享对象不断变化，但合作损失的问题仍在。可选计算见 可选阅读：核算博弈例子，不看公式也能理解故事。

本书的核心实证发现：一扇微启的通道，而非封死的高墙

虚构的墙掩盖了真实规则中的重要区别。技术是否已经公开？新转移是禁止、限制，还是能走便利路径？48 号公告与美国规则回答不同问题。现在从想象中的工作台转向原始文本：

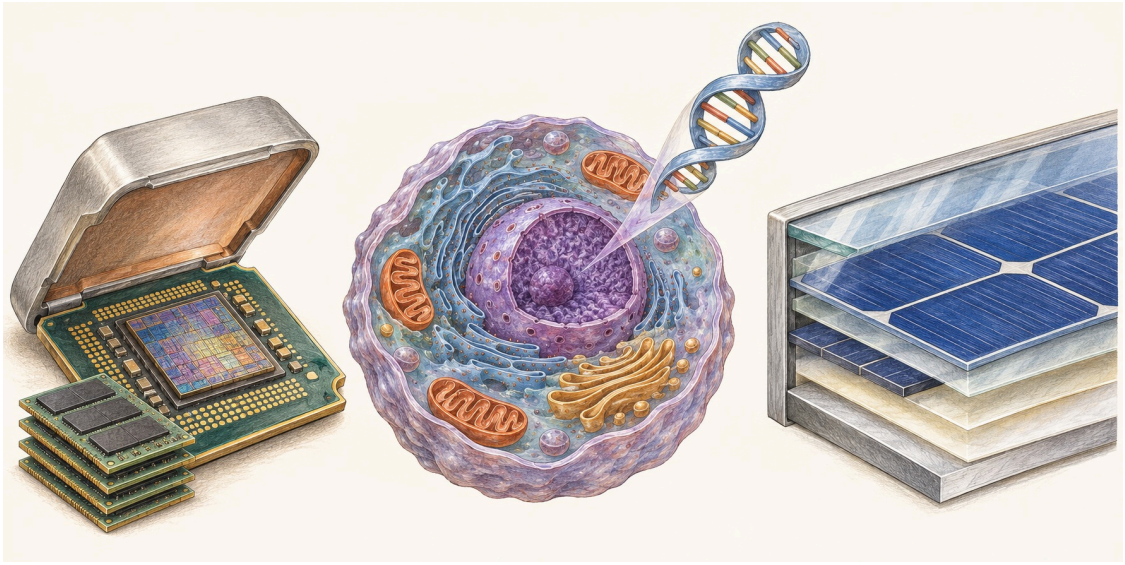


图 5 处理器、细胞和太阳能板的分层结构，分别展示计算、生物医药和光伏制造。

表 1 拟新增的 40 项技术

领域	拟禁止	拟限制
AI 及计算硬件	6	17

领域	拟禁止	拟限制
生物医药	3	2
光伏制造	5	7

- **已有公开与新发布不同**。中国排除及美国公开规则各有范围。论文未必公开私有权重，衍生版本需单独检查，也不解决其他所有法律。 CN-A1, note 1 EAR734 EAR774
- **新增开源 AI 发布与芯片流片享有专属快车道**。 中国并未禁止限制类人工智能技术的开源发布，而是在注释 2 中为通过开源方式出口、赴境外代工厂开展芯片流片（ `芯片流片` ）以及中资企业自建自营境外算力中心提供 **自动许可等便利化措施**（商务部官方政策解读称之为“即报即出”） CN-A1, note 2 CNQA 。
- **登记已实施，新增禁令仍拟议**。 覆盖的权属、境外许可和控制变化现在需要关注。核心数据新禁止项仍在草案中，并非公告已正式实施的新禁令。 CN48 CN-A1

如何阅读本书

我们为每一位怀抱好奇心的普通读者写下此书（无论你是工程师、科研人员、临床医生、创业者、青年学子、记者还是关心未来的公民），只要你渴望在严谨的一手证据之上读懂清晰生动的真相，都能按图索骥：

- 01. 知识设卡之日：当思想遇上海关岗亭 与 02. 四十道技术关隘：全景管制图谱 为您拆解北京第 48 号公告并行跳动的两套时钟，以及全部 **40 项受控技术指标** 的通俗地图。
- 03. 心智与硅基：模型、芯片与万卡集群 带您深入大模型软件配方与硅基芯片、存储及万卡集群底座（ `266504X` 、 `266506X` 、 `266507X` ）。
- 04. 开放模型：公开发布与私有转移 区分公开发布与私有转移，并把当前义务与提议路径分开。
- 05. 生命的代码：基因平台与共享良方 与 06. 将阳光装进机器：光伏工艺与核心装备 探访鲜活的基因制药平台与光伏制造车间，看核心工艺如何寄身于物理装备之中远渡重洋。
- 07. 华盛顿的守门人：算力芯片与模型权重 厘清华盛顿的算力芯片（ `3A090` ）与模型权重（ `4E091` ）规则，包括 2026 年 5 月美国政府问责局（GAO）裁决引发的制度交锋 USNE GAO26 。
- 08. 两套边界体系与官方审批实操指南 将中美两套管制体系并置对照，并附上办理官方审批所需的 **主管部门、在线申报平台、法定工作日时限，以及逐一核实的电话、传真、邮箱与办公地址名录** 。
- 09. 日常情境与实战：读者田野指南 与 10. 原始文献、核验方法与通俗术语表 以六个鲜活日常案例、一份平实易懂的术语表，以及截至 **2026 年 11 月 2 日** 核验无误的全部 **26 份一手官方文献** 收束全书。

> **备注**
> **关于官方附件格式的说明：** 商务部发布的附件 1 与附件 2 原件为 WPS 格式；我们在 10. 原始文献、核验方法与通俗术语表 中原封不动保存了原始字节文件，并同步提供转换后的 PDF 阅读版。此前本地误存为 `china_export_control.pdf` 的一份无关类器官学术演示文稿已从本书证据库中严格剔除。

01. 知识设卡之日：当思想遇上海关岗亭

一个周五午后，两套截然不同的时钟

不妨想象这样一幅情景：某个周五午后，市政厅贴出一纸通告，宣布计划在明年入冬前下调四十段高速公路的限速标准，并诚邀市民在三十天内来信建言献策。紧接着再往下读通告的后半截：就在同一个周五下午，高速公路上的实体岗亭已经亮灯运行，开始逐辆登记每一台驶过的受控货车，就连昨天已经驶出仓库、此刻尚未跨过江桥的货车也概莫能外。

这几乎正是 **商务部与科技部 2026 年第 48 号公告** 真实的运作方式。**2026 年 10 月 16 日**，中国商务部（由商务部安全与管制局牵头承办）会同科学技术部，依据《中华人民共和国对外贸易法》与《中华人民共和国技术进出口管理条例》联合印发这份文件，在同一时刻拨响了两套截然不同的时钟 CN48, sections I and III CNTIER：



图 6 2026 年 10 月 16 日发布的第 48 号公告分出两条并行轨道：针对 40 项拟新增目录技术为期 30 天的公开征求意见，以及在 ecomp.mofcom.gov.cn 即日执行的出口前信息登记义务。

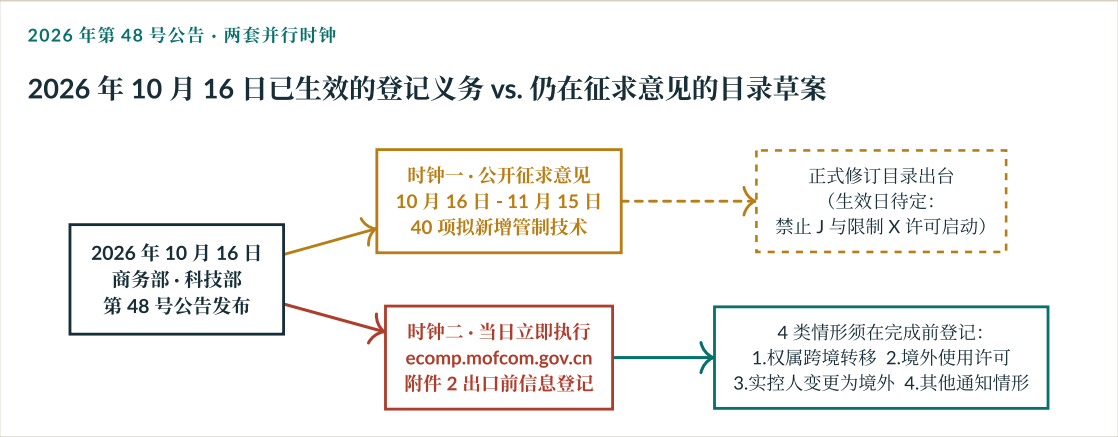


图 7 2026 年 10 月 16 日发布的第 48 号公告分出两条并行轨道：针对 40 项拟新增目录技术为期 30 天的公开征求意见，以及在 ecomp.mofcom.gov.cn 即日执行的出口前信息登记义务。

1. **征求意见时钟（2026 年 10 月 16 日至 11 月 15 日）：** 北京拟在《中国禁止出口限制出口技术目录》中新增 **40 项技术管制点**，包括 14 项禁止出口技术与 26 项限制出口技术，横跨人工智能与芯片（23 项）、生物医药（5 项）以及光伏新能源（12 项）。在公开征求意见期结束、正式修订目录依法公布实施之前，这些新增的禁止与许可条款仍属 **征求意见草案，而非已生效的正式禁令** CN48, sections I and II 。
2. **信息登记时钟（此刻正在运行）：** 自 2026 年 10 月 16 日第 48 号公告发布之时起，直至修订后的《中国禁止出口限制出口技术目录》最终正式公布实施之日止（具体实施日期官方尚未设定），凡拟出口附件 1 所列技术的经营主体，均须提前登录商务部业务系统统一平台（`https://ecomp.mofcom.gov.cn`）在线完成 **出口前信息登记** CN48, section III(1) CNPLAT 。

将这两套时钟混为一谈，是外界解读中国新规时最常犯的头号误区。出口前信息登记今天确已生效，但它是一道信息报备闸门，而非出口禁令；反过来，倘若一家初创企业或高校实验室误以为一切都要等到十一月中旬以后才算数，而眼下恰在签署境外技术授权协议、发运受控装备或推进境外融资交割，就极易在毫不知情中踩线失措 CN48 CNQA 。

不装一个木箱，知识如何跨越国境

在我们祖辈的耳中，“出口”二字意味着上海或鹿特丹港口的巨型龙门吊，正将钢铁集装箱稳稳吊上远洋货轮；而在现代技术出口管制立法者的字典里，完成一次“出口”，甚至不需要一只木箱碰到码头的地面。

根据第 48 号公告第三条第（二）款，四类交易情形必须在行为完成前履行强制性的出口前信息登记，**即便相关跨境转移在 10 月 16 日之前已经启动、但尚未最终交割完成，亦须补办登记** CN48, section III(2)：

- **将核心技术权属卖往境外：** 向境外买方转移境内技术所有权，例如转让专利权，或出售专有大模型、芯片设计等知识产权。
- **授予境外使用许可：** 技术所有权仍留在境内，但许可境外合作伙伴、客户或海外子公司在境外使用受控的境内技术。
- **更换手握方向盘的实际控制人：** 通过股权并购、架构重组或股东变更，使境内技术的所有权人或 实际控制人 变更为境外主体。哪怕每一位工程师和每一台服务器都纹丝不动地留在杭州或北京，只要最终公司控制权跨过了国境，登记义务便随之触发。
- **商务部通知规定的其他情形：** 一项法定兜底条款，使主管部门可通过正式通知将新型跨境技术转移架构纳入管理。

当出口经营者登录 `ecomp.mofcom.gov.cn` 进入“商务部业务系统统一平台 - 技术贸易管理信息应用”填报 **附件 2**（《技术出口信息登记表》）时，系统要求提供扎实可核验的要素：出口经营者主体信息并加盖单位公章（`公章`）、技术所有权人、境外接收方的中英文名称、所在国别/

地区、详细地址及与出口方的关联关系、准确的七位目录编号与控制要点技术指标、最终用户与最终用途、知识产权是否属于自主研发，以及折算为美元的合同金额 CN-A2 。同一项目中向同一境外主体出口多项技术的，可合并填报一张登记表；涉及不同境外接收主体的，则须分别单独填报 CN48, section III(3) 。

决定命运的四个法律档位

法律管制目录之所以常令外行望而生畏，是因为匆匆浏览的读者容易把每一行字都当成“一刀切禁令”。事实上，以下四种监管定位对技术流动与人类进步意味着天壤之别 CN-A1, notes 1 to 4 CNQA CNTIER：

禁止出口（ `禁止出口` ，编号以 `J` 结尾）
一堵密不透风的红墙。一旦修订目录正式生效，落入控制要点范围内的受控技术依法不得以任何方式出口 CNTIER, Art. 32 。

限制出口（ `限制出口` ，编号以 `X` 结尾）
一道配有锁孔与钥匙的守卫闸门。技术并非不可出海，只要出口经营者在跨境转移前依法取得商务与科技主管部门签发的许可文件，出口即完全合法 CNTIER, Art. 33 。

自动许可（ `自动许可` ）
指定限制出口拟享便利。官方意图加快办理，但不等于排除，也未给出最终流程或保证审批时间。 CN-A1, notes 2 and 3 CNQA

不纳入管理范围（ `不纳入管理范围` ）
完全处于本目录管辖之外。根据注释 1，已通过开源或公开发表论文进入公共领域的人工智能技术即归于此类（数据安全、著作权等一般性法律法规仍照常适用）CN-A1, note 1 。不妨把它想象成一座国际机场： 禁止出口 物品严禁登机； 限制出口 物品须凭申报批件放行； 自动许可 如同刷证秒过的自助快捷通道；而 不纳入管理范围 的物品则安稳留在你的随身背包里，连海关申报台都无需驻足。

这对两支团队意味着什么

对两队而言，转移前申报信息与禁止转移是不同障碍。故事关注每条规则下还剩下哪些合作。在判断影响前，本章先明确当前实行的义务与仍在提议中的目录变化。
两队的起点见 堡垒陷阱：双方如何一起受损。

02. 四十道技术关隘：全景管制图谱

监管者如何用尺规丈量一种思想

立法者该如何落笔，才能把一名大学生周末练手的编程作业，同一项关乎国家战略命脉的核心资产清晰分开？倘若只在法条里笼统写一句“先进人工智能与高端硬件一律受控”，世上每一个计算器小程序和每一块普通电路板都会被淹没在申报文书的汪洋里；可倘若指名道姓只写某家公司或某款模型的名字，明天只需换个代号便能大摇大摆绕过关闸。

现代监管者的破题之道，是划定精确的 **量化性能标尺与专门用途边界** 。在第 48 号公告附件 1 中，北京在七位目录编号之下精细标绘出 **40 个具体技术控制点** ： **人工智能与 AI 硬件领域 23 项** （6 项拟禁止出口、17 项拟限制出口）、 **生物医药领域 5 项** （3 项拟禁止、2 项拟限制），以及 **光伏制造领域 12 项** （5 项拟禁止、7 项拟限制），与官方通报的 **14 项禁止出口技术** 和 **26 项限制出口技术** 总数严丝合缝 CN48 CN-A1 CNQA 。

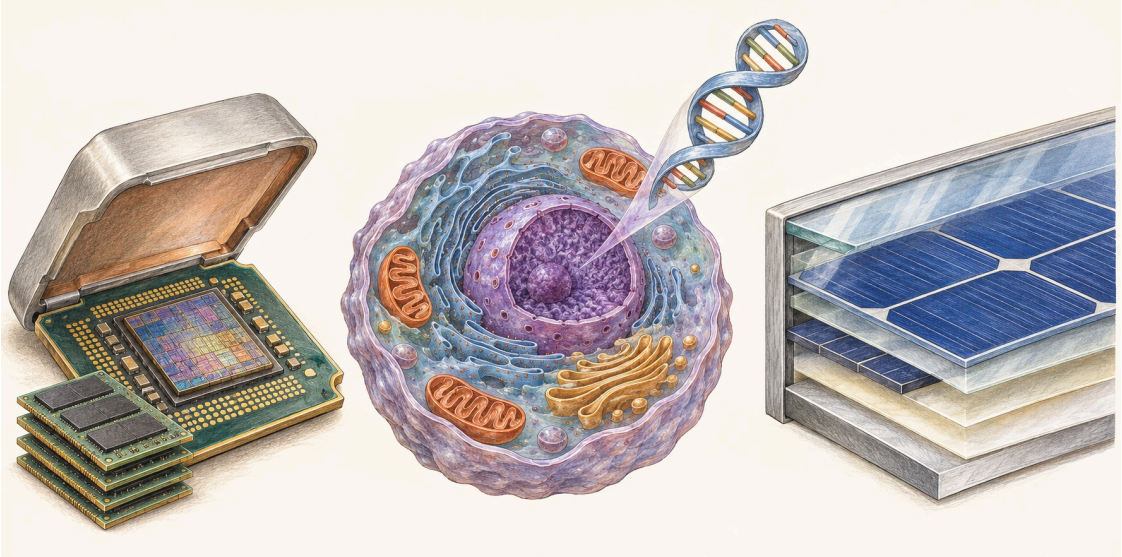


图 8 处理器、细胞和太阳能板的分层结构，分别展示计算、生物医药和光伏制造。

一个编号可含多个控制点：266504X 有 2 项，266505X 有 4 项，266506X 有 **2 个主项** ，266507X 有 4 项。编辑索引分成 40 点并保留原编号，不替代法律清单。 CN-A1

看懂技术红线而不被红线绊倒

在翻阅这份技术图谱时，请牢记三个极其实用的读法窍门：

1. **分清“满足其一即触发”与“全部同时满足才触发”**。例如 `266504X` 第 2 点（前沿大模型核心技术）只要触及三项标准中的 任意一项 即落入范围：训练算力 $\geq 10^{26}$ FLOPs，或 参数规模 ≥ 2 trillion parameters（2 万亿），或 出口时位居全球前十公开榜单。相反，`266505X` 第 1 点（自主任务规划智能体）则唯有在拆解子任务 ≥ 20 steps、且 拆解准确率 $\geq 80\%$、且 子任务平均完成率 $\geq 90\%$ 三者同时达标时方才触发 CN-A1 。
2. **特定用途往往构成半道藩篱**。 若干看似严厉的禁止类条目，例如准确率 $\geq 95\%$ 的深度伪造检测（ `266401J` ）或高性能敏感场景智能体（ `266502J` ）， 仅在 专门或主要面向国家网络数据跨境安全防护、关键信息基础设施、国防军事或党政核心机关场景研发时才适用；普通的影视工作室工具与消费级日常助手并不在此用途之列 CN-A1 。
3. **看清藏在软件清单里的硬核芯片与物理母机**。请留意下文人工智能板块中的最后 6 个控制点（ `266506X` 与 `266507X` ）根本不是聊天机器人，它们是实打实的 **AI 处理器芯片架构、3D NAND 与 DRAM/HBM 存储设计，以及超万卡超算集群高速互联技术** ；与此同时，注释 4 更将 **所列实体光伏核心制造装备** 直接拉入了技术出口管制范围 CN-A1 。

人工智能、算力芯片与超万卡集群（23 项管制点）

266401J · 第 1 点：跨境数据安全防护深度伪造检测技术 （拟禁止出口）
主要用于维护国家网络数据跨境安全、针对深度伪造视频、音频、图像或多模态内容同时达到准确率 >=95% 且召回率 >=95% 的高阶检测系统及专用装备制造技术。不具此项国家安全专门用途的普通民用媒体鉴伪工具不在打击之列。

266402J · 第 1 点：恶意代码自主生成与变异技术 （拟禁止出口）
能够针对关键信息基础设施、国防系统或党政核心网络自主编写或变异生成恶意代码，并达到所列免杀绕过指标（对多引擎查杀绕过率 >=60%、对主流杀毒软件绕过率 >=85%，或对机器学习检测模型绕过率 >=90%）的网络攻击型人工智能。日常编程辅助工具不受影响。

266402J · 第 2 点：自适应环境感知与动态免杀对抗技术 （拟禁止出口）
面向国家安全敏感目标构建的攻击型人工智能技术：可自动感知沙箱、调试器或模拟器分析环境并实施逃逸，或在保持攻击载荷功能不变的前提下，每次运行时自动重构 >=50% 的代码结构或控制流逻辑。

266402J · 第 3 点：规模化自动免杀变种生成与投放技术 （拟禁止出口）
面向敏感网络行动、可批量生产并自动化部署免杀恶意代码变种的技术：单次生成 >=20 个结构显著不同的变种（或全流程自动化率 >=80%）、日均生成 >=10 个语法树差异度 >=30% 的变种，或在沙箱内保持 >=90% 的正常伪装行为一致性。

266501J · 第 1 点：利用国家核心数据训练的大模型技术 （拟禁止出口）
利用中国依法认定的 国家核心数据（《数据安全法》下最高国家安全级别数据）训练并对外提供服务的人工智能大模型技术。触发这道红线的唯一依据是训练语料的法定密级属性，与研发机构或模型的商业品牌无关。

266502J · 第 1 点：面向关键基础设施或国防场景的高性能智能体 （拟禁止出口）
专门或主要面向关键信息基础设施、国防军事或党政核心机关业务研制，且同时达到 `266505X` 所列高性能技术指标的人工智能智能体。通用型办公效率智能体与日常编程智能体不落入此项。

266402X · 第 8 点：超高精度深度伪造检测技术（98%+） （拟限制出口）
针对视频、音频、图像或多模态合成伪造内容，检测准确率与召回率同时达到 >=98% 的顶尖鉴伪系统及专用设备制造技术（不论是否用于数据跨境安全防线）。

266402X · 第 9 点：高鲁棒近无损图像与视频隐写技术 （拟限制出口）
在图像或视频载体中隐藏与提取秘密信息的技术，须三项严苛指标同时达标方才受控：经受压缩失真后仍具极高鲁棒性（误码率 <=0.5% 或提取完整率 >=99.9%）、误检率 <=0.1%，且肉眼几乎完全不可察觉（SSIM >=0.999、PSNR >=41 dB 或 LPIPS <=0.005）。

266404X · 第 6 点：AI 驱动的高阶零日漏洞挖掘与利用链生成技术 （拟限制出口）

满足以下六项高门槛标准之一的网络安全人工智能技术：在顶级漏洞基准测试中得分 >=75%；能自动构建完整漏洞利用链（对主流操作系统/浏览器成功率 >=50% 或任意代码执行率 >=40%）；挖掘效率达资深人类安全专家的 10 倍以上；能将 >=2 个中低危漏洞自动串联组合为可执行的 PoC 攻击；单轮扫描即可在主流操作系统或大型开源项目中独立发现 >=5 个高危漏洞或 >=50 个未知新漏洞；或达到主流漏洞自动化利用能力分级的最高等级。

266501X · 第 19 点：高并发、抗伪造及民族语/方言声纹识别技术 （拟限制出口）

达到以下四项标准之一的说话人声纹识别算法与系统：短语音片段在误识率 <=0.01% 下正确识别率 >=99.1%；在 >=100 次/秒高并发下响应延迟 <=300 毫秒；对录音重放及 AI 合成语音具备 >=98% 防伪检出率（或误受率 <=1%）；或针对中国少数民族语言及地方方言定制且识别准确率 >=90%。

266501X · 第 20 点：汉语与中国少数民族语言高质量机器翻译技术 （拟限制出口）

主要面向汉语与中国少数民族语言互译研发，且达到人工主观评价得分（MOS） >=4.8，或在语义保真度 >=95% 的同时通用领域 BLEU >=35（专业垂直领域 BLEU >=30）的机器翻译核心技术。

266504X · 第 1 点：利用法定重要数据训练的大模型技术 （拟限制出口）

利用国家依法界定的 重要数据 训练并对外提供服务的大模型技术。尤为关键的是，说明 1 明确豁免了两类情形：一是重要数据经脱敏清洗后仅占训练语料微量比例（ <=0.1% ），既未实质增强特定领域核心研发能力、亦无法在输出中被复现；二是数据本身源自合法公开渠道。

266504X · 第 2 点：前沿大模型核心技术 （拟限制出口）

整份 AI 模型管制规则的核心枢纽：涵盖模型权重、关键检查点、底层源代码、模型架构、训练优化及推理加速技术，只要触及以下三项指标中的 **任意一项** 即纳入范围：累计训练算力 >=10^26 FLOPs、总参数量 >=2 万亿，或在出口行为发生时位居境内外权威公开评测全球前十。通过开源方式出口的，享受注释 2 自动许可（“即报即出”）便利。

266505X · 第 1 点：长序列自主任务规划智能体技术 （拟限制出口）

能够将复杂自然语言指令自主拆解为 >=20 个可执行子任务序列，同时实现任务拆解准确率 >=80% 且子任务平均执行完成率 >=90% 的智能体规划技术（三项数值须同时满足）。

266505X · 第 2 点：60 智能体大规模协同编排技术 （拟限制出口）

支持 >=60 个人工智能智能体并发协同运行的多智能体编排框架：在同等产出质量下总耗时不超过最优单智能体基准耗时的 2 倍，且最终结果与标准真值的一致率达到 >=85%。

266505X · 第 3 点：200+ 外部工具调用与系统操控智能体 （拟限制出口）

支持集成调用 >=200 种第三方软件工具的系统操作型智能体技术：工具选择准确率 >=90%，且在需串联调用 >=3 种不同工具的复杂组合任务中端到端执行成功率 >=90%。

266505X · 第 4 点：毫秒级实时博弈与多单元动态决策智能体 （拟限制出口）

同时满足三项标准的实时策略决策智能体：具备 >=20 步前瞻规划深度（或 >=10 个并发协同智能体）；在动态对抗环境中可对 >=10 个控制单元在 <=200 毫秒内作出自适应决策；且在主流标准策略博弈评测中表现超越 >=90% 的人类选手。

266506X · 第 1 点：AI 处理器架构、定制指令集与计算 IP 核设计 （拟限制出口）

满足所列任一特征的人工智能处理器芯片设计技术（涵盖自定义处理器架构、指令集、核心计算 IP 核、基础软件栈及专用设计工具），包括需采用 <=14 纳米制程、具备浮点或整型张量算力、采用 2.5D/3D 芯粒（Chiplet）封装、高速片间互联、非冯·诺依曼/存算一体架构，或面向智能视觉、语音、自动驾驶等指定应用。注释 2 对赴境外晶圆代工厂开展芯片流片给予自动许可便利。

266506X · 第 2 点：高密度 3D NAND 闪存与堆叠式 DRAM / HBM 存储芯片设计 （拟限制出口）

存储密度 >=8 Gb/mm2、I/O 接口速率 >=1.5 Gbps 或采用晶圆键合工艺的 3D NAND 闪存芯片设计技术；以及采用 <=18 纳米光刻制程、垂直沟道晶体管（VCT）、晶圆键合或类似 HBM 多层晶圆/裸片三维堆叠架构的先进 DRAM 存储芯片设计技术。

266507X · 第 1 点：超万卡智算集群超高速互联技术 （拟限制出口）

应用于超过 10,000 张加速卡的超大规模人工智能算力集群内部、芯片间或节点间双向通信带宽达到 >=800 GB/s 的高速互联核心技术。

266507X · 第 2 点：超万卡集群分布式训练秒级容错恢复技术 （拟限制出口）
在超万卡智算集群中满足任一高可用指标的分布式训练容错自愈技术：检查点故障平均恢复时间（MTTR）<=120 秒、任务无缝迁移业务感知中断 <=30 秒，或因网络故障导致的有效算力折损率 <=5%。

266507X · 第 3 点：超万卡集群微秒级通信调度优化技术 （拟限制出口）
面向超万卡 AI 集群、达到以下任一性能高度的集合通信调度技术：线性加速比 >=98%、支持 <=1 微秒端到端延迟的动态拓扑感知路由，或计算与通信掩盖重叠率 >=90%。

266507X · 第 4 点：多厂商异构芯片混训与跨地域算力协同技术 （拟限制出口）
在超万卡集群中将两家及以上不同厂商异构算力芯片统一池化混训与调度的软件及运维核心技术：达到所列高带宽互联、系统吞吐提升（+30%）、算力卡综合利用率（>=65%）、单位训练成本下降（-20%）、99.9% 可用性或跨数据中心跨域协同训练效率 >=80% 等指标。

生物医药与基因治疗平台（5 项管制点）

262704J · 第 1 点：通用型细胞与基因治疗（CGT）底层研发平台 （拟禁止出口）
中国自主拥有知识产权、可支撑多款细胞与基因治疗药物衍生开发的通用底层平台技术。关键边界在于：仅禁止将平台技术“所有权”转让至境外；对外授权许可（Out-licensing）、境内保留所有权的 CRO/CDMO 委托研发生产，以及单款具体候选药物临床试验、注册审批与商业化上市所需的技术资料均不在禁止之列。

262705J · 第 1 点：通用型小干扰核酸（siRNA）成药研发平台 （拟禁止出口）
中国自主拥有知识产权的小干扰核酸（siRNA）通用底层成药平台，适用完全一致的精准切分边界：禁止向境外转移可复用底层引擎的技术所有权，而正常对外授权许可、委托研发生产及围绕具体单药品种的国际商务合作全面保持开放。

267302J · 第 1 点：病原体毒力增强与受控定向进化技术 （拟禁止出口）
严守生物安全底线的禁止类条目：涵盖通过人工基因改造或受控连续传代手段增强病原体致病功能、实现规模化毒力维持或加速病原体适应性进化的技术。常规临床病原检测与合规疫苗医疗不受影响。

262705X · 第 1 点：全球未公开全新细胞与基因治疗靶点发现技术 （拟限制出口）
中国自主研发、用于发现并确证此前从未在全球任何专利、学术期刊、公共数据库或会议上披露过的全新 CGT 治疗靶点的技术。注释 3 对对外授权许可、国际科研合作及突发公共卫生事件应急提供自动许可便利。

262706X · 第 1 点：全球未公开全新 siRNA 药物靶点发现技术 （拟限制出口）
中国自主研发、用于筛选与锁定全球范围内尚未公开披露的全新 siRNA 药物分子靶点的技术，同样享有注释 3 针对跨国授权合作、联合科研及人道主义卫生应急设立的自动许可快车道。

光伏晶硅材料、超薄硅片与产线装备（12 项管制点）

263003J · 第 1 点：超大规模冷氢化法多晶硅生产工艺与装备技术 （拟禁止出口）
单线三氯氢硅年产能达到 >=25 万吨的超大型冷氢化流化床工艺配方及核心反应器制造技术。

263003J · 第 2 点：万吨级硅烷流化床法颗粒硅工艺与装备技术 （拟禁止出口）
单线年产能达到 >=2 万吨的硅烷流化床法多晶硅化学制备工艺与核心成套设备制造技术。

263004J · 第 1 点：70 微米及以下超薄光伏硅片切割工艺与装备 （拟禁止出口）
厚度 <=70 微米（约相当于一根人类头发丝直径）超薄太阳能硅片的精密切割工艺与多线切割机制造技术，条文明确将底层控制软件、核心算法与全套工程机械图纸一并纳入禁止出口范围。

263801J · 第 1 点：大尺寸超薄晶硅电池边缘钝化技术 （拟禁止出口）
应用于尺寸 182 至 230 毫米、且硅片厚度 <=140 微米的大尺寸薄片晶硅光伏电池专用边缘钝化工艺及核心装备制造技术。
263801J · 第 2 点：30% 转换效率钙钛矿及晶硅叠层光伏技术 （拟禁止出口）
触及四项量产标尺之一的下一代钙钛矿光伏制造技术：转换效率 >=30% 的大尺寸（ >=182 毫米）晶硅-钙钛矿叠层电池工艺；幅宽 >=1.1 米的钙钛矿狭缝涂布技术；面积 >=1 平方米且效率 >=18% 的单结钙钛矿组件；或面积 >=1 平方米且效率 >=28% 的叠层光伏组件。
263004X · 第 1 点：3 万吨级多晶硅整线工程成套设计技术 （拟限制出口）
单线年产能 >=3 万吨的多晶硅工厂整线工程工艺包、厂房系统蓝图及成套核心设备设计技术。
263004X · 第 2 点：单炉年产 800 吨大型多晶硅还原炉技术 （拟限制出口）
单台还原炉年产量达到 >=800 吨的高产多晶硅化学气相沉积还原工艺及大型还原炉装备制造技术。
263005X · 第 1 点：大炉膛低功耗光伏单晶硅生长炉技术 （拟限制出口）
满足任一先进指标的光伏直拉单晶生长炉设计制造技术：主炉膛内径 >=1,600 毫米、热场尺寸 >=35 英寸、平均拉晶速率 >=1.2 毫米/分钟，或等径生长阶段运行功耗 <=40 千瓦。
263005X · 第 2 点：720 毫米以上超长单晶硅棒开方与磨削技术 （拟限制出口）
半棒截断磨削工艺，或针对长度 >=720 毫米超长光伏单晶硅棒的高精度一体开方磨削加工工艺与专用机床制造技术。
263005X · 第 3 点：矩形硅片与 130 微米薄片钨丝金刚线切割技术 （拟限制出口）
矩形光伏硅片（任一边长 >=182 毫米）或薄型硅片（厚度 <=130 微米）的精密制造与切割技术，涵盖采用母线直径 <=28 微米细钨丝金刚线、高速主轴（ >=6,500 转/分）或紧凑轴距罗拉结构的切片工艺及装备。
263802X · 第 1 点：高效 TOPCon 与背接触（XBC）晶硅电池工艺 （拟限制出口）
在尺寸 182 至 230 毫米、厚度 <=140 微米硅片上实现量产电池效率 >=25% 或组件效率 >=22.3% 的六大工业核心工艺簇：LPCVD/PECVD 隧穿氧化层制备、高速 ALD 原子层沉积钝化、激光选择性硼扩散、无栅铜电镀、微晶硅薄膜沉积以及背接触（XBC）金属化工艺。
263802X · 第 2 点：高效异质结（HJT）低铟低银电池制造工艺 （拟限制出口）
涵盖四大异质结（HJT）电池核心降本增效工艺簇：低铟（铟占比 <=50%）或超高速透明导电氧化物（TCO）镀膜、在 <=110 微米超薄硅片上沉积晶硅薄膜、低银含量（银占比 <=30%）银包铜导电浆料应用，以及异质结铜电镀栅线电极工艺。

这对两支团队意味着什么

索引统计的是拟议技术点。博弈分数表达虚构偏好，不是技术数量。对团队更有用的问题是下一项贡献具体符合哪个条目与条件，而非把所有 AI 放在同一道墙后面。
两队的起点见 堡垒陷阱：双方如何一起受损。

03. 心智与硅基：模型、芯片与万卡集群

老面酵种、面包店窗口与铸铁烤炉

在对着手机屏幕敲下一行提问的普通用户眼中，人工智能宛如一场浑然天成的魔术：一个会思考、会答话的对话框。但在系统工程师，以及如今北京与华盛顿的出口管制立法者，眼中，一套人工智能系统却清晰地分为 三**层截然不同的数字与物理结构**：

1. **面包店的售卖窗口（远程 API 与终端应用）：** 隔着橱窗递给顾客一片温热的面包，并不会把烤炉的布线图纸或明早自己烤出一万只面包的秘方交到对方手中。
2. **老面酵种与母本秘方（权重、检查点与训练代码）：** 由数十亿乃至数万亿个经训练习得的数值参数（ `模型权重` ）、训练中途保存的快照（ `关键检查点` ）、模型架构设计，以及底层源码与性能调优代码（ `训练优化、推理加速` ）共同构成。复制了这些文件，就等于完整复刻了那颗训练成型的大脑本身。
3. **铸铁烤炉与发电厂（AI 芯片、堆叠存储与超算集群）：** 由物理硅基处理器、高带宽存储器、芯片架构蓝图与高速光互联集群网络组成，离开了这层底座，无论是前沿模型的预训练，还是医院与高校的本地私有化部署，都将成为无源之水。

商务部问答区分远程 API、应用、网页、SaaS 及轻量本地服务与草案中的受限大模型技术转移。这只说明该范围，不是所有技术或数据规则的豁免。附件 1 分别列出模型技术（`266504X`）、处理器及存储设计（`266506X`）、超过 10,000 张加速卡集群的特定技术（`266507X`）。CNQA CN-A1

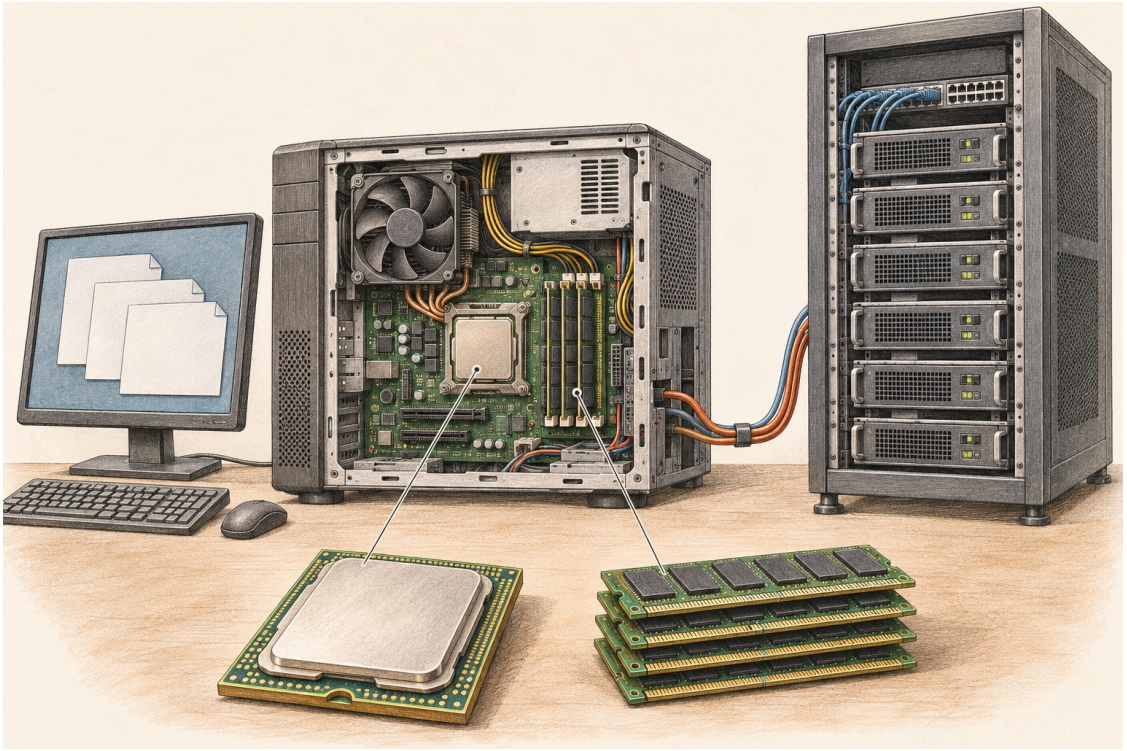


图 9 开放模型依赖芯片、存储与算力设施。限制一部分可能影响整体可用性。

前沿大模型核心技术的三条触发红线（ 266504X ）

并非高校实验室或创业车库里训练出的每一个神经网络都会落入拟限制出口的 **266504X 第 2 点**。只有当某款大模型的核心技术（涵盖模型权重、关键检查点、底层源代码、模型架构、训练优化与推理加速技术）触及以下三条量化指标中的 **任意一条** 时，才会被纳入管制范围 CN-A1, 266504X(2), note 3：

1. **训练算力规模：** 模型累计训练计算量达到或超过 10^{26} **次浮点运算（FLOPs）**，这一超大规模算力门槛与美国 4E091 闭源模型权重管制条款所采用的算力标准完全一致 US25。
2. **参数规模：** 模型总参数量达到或超过 **2 万亿（20,000 亿）**。
3. **出口行为发生时位居全球前十：** 即便是一款精悍紧凑的中小参数模型，如果在 **出口行为发生时**，境内外主流权威评测机构或大型行业平台的公开评测结果将其列为 **全球前十名**，无论是综合能力、特定业务场景能力、全球调用规模、安全对齐表现还是训练效率指标，同样会触发管制 CN-A1, 266504X, note 3。

第三条指标具有鲜明的动态生命力。由于开源研究者不断发明精巧的蒸馏与强化学习方法，将顶尖推理能力浓缩进 300 亿或 700 亿参数的轻量模型之中，一款惊艳问世、首周空降全球第六的“小钢炮”模型在发布当周会 跨入 限制类门槛；而八个月后，当新一代模型纷纷超越其排名时，它又会自然 退回 门槛之外。因此，合规判定永远绑定于“特定模型版本在特定出口时点”的客观状态，而绝不会给“DeepSeek”或“Qwen”之类品牌贴上终身固定的标签 CN-A1。

数据安全红线（ 266501J 与 266504X(1) ）及自主智能体（ 266505X 与 266502J ）

哪怕模型体量再小，一旦喂入了关乎国家主权机密的训练语料，也会撞上不可逾越的红墙。附件 1 直接引入《中华人民共和国数据安全法》的分级概念：利用国家依法认定的 **核心数据** 训练并对外提供服务的大模型被列入 **拟禁止出口**（ 266501J，连远程提供服务亦在禁止之列）；而利用法定 **重要数据** 训练的大模型则归入 **拟限制出口**（ 266504X(1) ），但附有两条极其实

用的豁免说明，若相关重要数据源自 **合法公开渠道**，或经脱敏清洗后占比 **不超过 0.1% 的微量比例**（既未实质提升特定领域核心研发能力，亦无法在模型输出中被还原泄露），则不纳入该项管制 CN-A1 。

围绕基座大模型外围，**266505X** 下设四个限制点，精准覆盖高阶 **人工智能智能体（Agent）** 技术：长程任务规划引擎（拆解 ≥ 20 个子步骤，且拆解准确率 ≥ 80% 、子任务平均完成率 ≥ 90% ）、多智能体协同编排系统（支持 ≥ 60 个并发智能体）、大规模工具调用引擎（集成 ≥ 200 种外部软件工具，且多工具串联任务端到端成功率 ≥ 90% ），以及响应延迟低于 200 毫秒且超越 90% 人类选手的实时博弈决策系统。唯有当此类高性能智能体 专门或主要 面向国防军事、关键信息基础设施或党政核心机关场景打造时，才会跨入禁止出口红线（ `266502J` ） CN-A1 。

中国 AI 清单深处的硬件底座：算力芯片、先进存储与万卡集群

AI 部分还包括处理器设计、存储设计及大型集群工程：

- **AI 处理器设计蓝图（266506X 第 1 点）：** 草案拟限制出口满足所列 任一 技术特征的 AI 处理器架构、定制指令集、核心计算 IP 核、基础软件栈及专用设计工具，不仅涵盖需采用 ≤ 14 nm 制程工艺的设计、2.5D/3D 芯粒（Chiplet）先进封装或非冯·诺依曼/存算一体等新型架构，甚至囊括了具备浮点/整型张量运算能力或面向智能语音、计算机视觉、自动驾驶等广泛应用场景的功能特征 CN-A1, 266506X 。不妨想一想这会触及多广的面：开源硬件社区（如基于 RISC-V 的开源 AI 加速器项目）、定制 NPU 初创公司，以及跨国协同研发的芯片设计团队！正因无晶圆厂（Fabless）芯片设计企业必须将完成版图交付境外半导体代工厂才能造出实体晶圆，**注释 2** 才专门开辟了一道至关重要的减压阀：对 **赴境外开展芯片流片制造**（ `赴境外开展芯片流片制造` ）给予自动许可等便利化安排 CN-A1, note 2 CNQA 。
- **存储设计（266506X 第 2 项）：** 分为 3D 闪存和内存两个子项。闪存看密度、速度或键合，内存看 18 纳米及以下、垂直沟道、键合或多层堆叠。这些是替代条件，不是所有存储统一适用 18 纳米门槛。 CN-A1, 266506X(2)
- **超万卡集群的系统工程底座（266507X 第 1 至 4 点）：** 在 **超过 10,000 张算力加速卡** 上训练前沿开源大模型，不亚于一场精密工业魔法，稍有不慎，单卡故障就会令整座集群每隔一小时停摆一次。四个限制点严密把守着双向带宽 ≥ 800 GB/s 的芯片/节点高速互联、恢复时间 ≤ 120 -second 的自动容错自愈、端到端延迟 ≤ 1 -microsecond 的动态集合通信调度，以及 **将两家及以上不同硬件厂商算力芯片统一池化混训的异构集群软件栈** CN-A1, 266507X 。当华盛顿严控英伟达高端 GPU（ `3A090` ），而北京拟限制多厂商异构集群混训缝合技术（ `266507X` ）时，全球开源分布式训练框架正不偏不倚地站在两大管制体系交汇的断层线上！

这对两支团队意味着什么

A 的内存改进与 B 的测试是可以交换的知识，计算机则是另一项依赖。开放模型许可无法补上缺失芯片，硬件限制也不能独自说明所有模型文件的法律状态。我们同时追踪工作台的这两个部分。

两队的起点见 堡垒陷阱：双方如何一起受损。

04. 开放模型：公开发布与私有转移

开放许可只是发布的一部分

团队可以公开代码和权重供研究、改进及运行。宽松著作权许可只是发布的一部分，还需评估适用的出口、数据和安全规则。DeepSeek-R1 和 Qwen3 是有记录的公开发布例子，不能证明所有相关活动都获豁免。 R1 QWEN



图 10 获得文件和知识后独立工作，与使用把底层模型保留在别处的服务不同。

从具体文件开始

公开论文、可下载权重、私有训练代码和后续微调是不同对象。开放 AI 定义要求自由、代码、参数及足够数据信息；自称开放的产品可能只提供部分内容。著作权标签也不能决定出口状态。 OSI

中国：当前登记与目录提案分开

第 48 号公告要求覆盖的转移先临时登记，含未完成出口。情形包括所有权、境外许可、外国控制及其他通知。目录禁令和许可是另一条轨道。拟禁止不等于已生效的新禁令，也须检查现有法律。 CN48 CN-A1

我们结合适用于整个 AI 部分的注释阅读草案，不把每次发布都当成必须经过四个关口：

1. **已有公开 AI：** 注 1 排除已通过开源或论文公开的技术。须识别公开了什么；论文不等于公开私有权重，私有衍生版本也不自动继承所有排除。 CN-A1, note 1
2. **未公开的数据敏感技术：** 指定核心数据模型拟禁止，重要数据模型拟限制。微量数据排除不只有 0.1% 这一条件，需要事实与法律解释。 CN-A1, 266501J and 266504X
3. **其他未公开技术：** 检查替代模型条件及一起交付的智能体、芯片或集群技术。低于一个门槛不等于所有条目、现有法律或捆绑内容均已通过。 CN-A1
4. **便利路径：** 注 2 对指定限制 AI 的开源、境外制造及部分自营计算中心提出自动许可等便利。排除与简化许可不同，仍要看最终程序和适用条件。 CN-A1, note 2 CNQA

表 2 转移前的三个独立问题

问题	核查内容
中国当前登记	所覆盖的技术和转移，包括尚未完成的出口。
中国目录草案	准确条目、注释、排除规定及拟议便利路径。
独立的美国规则	先判断具体对象是否受 EAR 管辖，再核查分类及适用条件。

美国：单独判断管辖

先判断文件是否受 EAR 管辖。公开条款及 4E091 注释可能排除合格的公开技术或权重。衍生模型有额外训练条件，私有改进不自动等同公共原版。不执行政策、GAO 意见和正式文本亦须分开。 EAR734 EAR774, 4E091 notes GAO26

商务部对 API、应用、网页、SaaS 及轻量部署的答复针对拟议措施下的限制类大模型。不能变成美国通用豁免或中国其他措施的批准。交付私有权重与远程服务不同。 CNQA

对开放模型的可能影响

继续发布 符合明确便利政策。 **更多记录或延误** 、 **公开小模型加私有服务** 、 **训练更集中** 是可能机制。需要调查，不能当成公告已证明的结果或量化预测。 CN-A1 CNQA NTIA

没有识别因果的证据，就不能说某模型效率提升由芯片管制造成。参数少不保证排除。本地使用可能减少远程依赖，但不自动保证隐私、安全或临床可靠性。

独立审查及其局限

开放让原开发者之外的团队检查模型并建议修复。更多审查者可能有帮助，但也可能共享盲点或缺乏测试资源。发现缺陷也不同于修复缺陷。可选阅读：独立审查不保证安全 中的可选概率例子解释这些局限。

公开权重也可能方便恶意修改或删除防护。NTIA 在 2024 年权衡收益与风险，建议监测当时的开放权重。研究强调比较相对现有替代品的新增风险；两者均未确立普遍的安全倍数。 NTIA OPENRISK

实用的发布记录

我们建议记录版本、文件哈希、许可、公开与私有内容、数据类别、指标、接收方、目的地和交付方式，并保存公开及手续证据。这是记录建议，不是新强制表格，也不替代官方登记。 CN-A2

这对两支团队意味着什么

团队保留公开起始模型。下一项贡献可能是论文、新代码、私有权重或服务，各需单独评估。公开信息排除与拟议便利路径的重要之处，在于可能保留故事中广泛墙体会阻断的特定交换。两队的起点见 堡垒陷阱：双方如何一起受损。

05. 生命的代码：基因平台与共享良方

留住活字印刷机，让良方典籍传遍天下

如果说人工智能是用浮点数谱写思想，现代生物医药便是用生命的四字母密码（`A, C, G, U/T`）编写疗法。过去十年间，中国生物科技团队已从早年的专利到期仿制药车间，跨越式成长为原创底层平台的发明者，构建起可反复复用的 **细胞与基因治疗（CGT）** 研发引擎，以及能够在致病蛋白合成之前精准沉默致病基因的 **小干扰核酸（siRNA）** 技术平台。

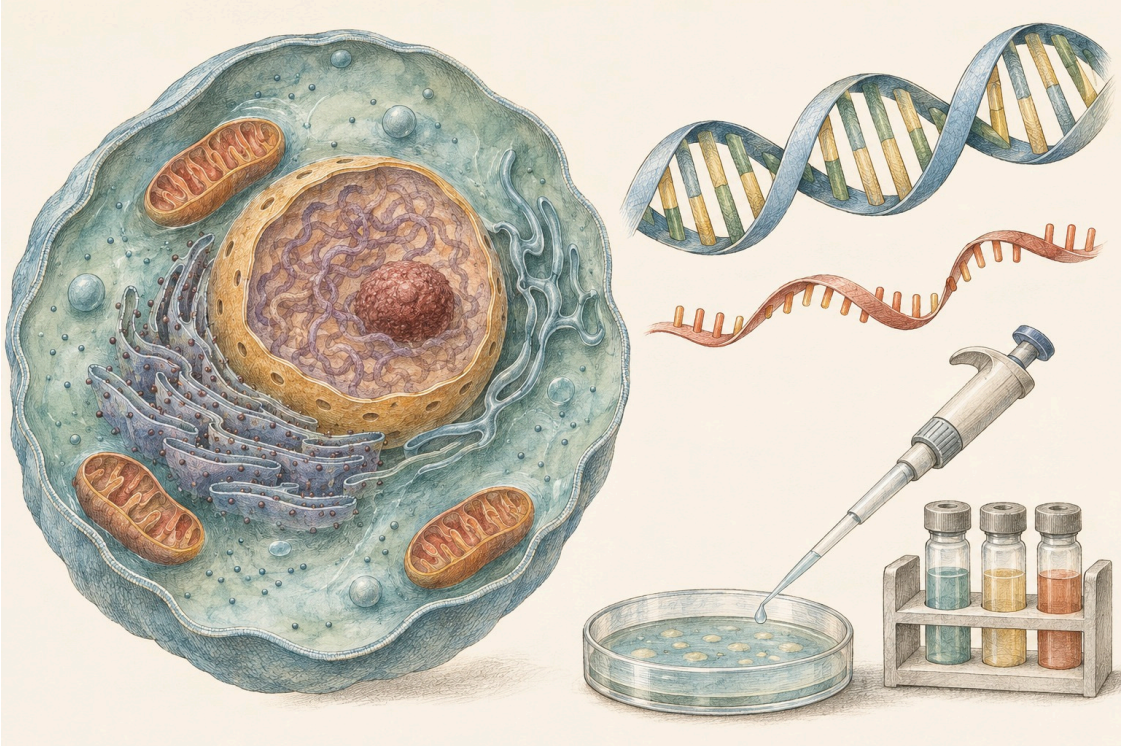


图 11 细胞、DNA、RNA 和实验工具让主题更具体。可复用的药物研发平台与某一种治疗不同。

草案区分可复用药物研发平台的所有权与具体药物项目，拟限制所列平台的所有权转移，并明确排除许可等活动。这些排除只针对相关条目，药品及临床试验仍可能受其他规则约束。CN-A1, 262704J and 262705J CNQA

不妨将一套十年磨一剑的 CGT 或 siRNA 底层技术平台想象成一台定制的 **活字印刷机**，其中凝聚着递送载体、化学修饰稳定配方与模块化序列设计规则，足以在未来源源不断印制出二十种新疗法；而某一款进入临床管线的具体候选新药，则是这台印刷机印出的 **一本书**：

- **平台所有权转移拟禁止（262704J、262705J）**。草案针对指定可复用平台的境外所有权转移并设排除。它不是第 48 号公告已经正式实施的新禁令。 CN-A1
- **对外授权许可、委托研发生产与单药出海合作全面放行：**两项条目下设的三条明确说明，特意豁免了技术所有权留在境内的 **对外授权许可**（ `对外授权许可` ）、**委托研发与生产（CRO/CDMO）**，以及跨国医药商务拓展（BD）合作中围绕 **特定候选药物开展临床前研究、临床试验、生产制造、质量控制、注册申报及商业化上市** 所需的全部管线技术资料 CN-A1 CNQA 。唯有那种名义上叫“许可”、实质上永久买断并掏空境内所有权的变相转让，才会触碰红线。

全球未公开全新靶点与生物安全红线

另有两项 **拟限制出口** 条目（ `262705X` 与 `262706X` ）聚焦于中国自主研发的 CGT 与 siRNA **全新治疗靶点发现与确证技术**，其范围被严格界定为 **此前从未在全世界任何专利、学术期刊、公共数据库、行业披露或学术会议上公开过的全新分子靶点** CN-A1 。即便在这一领域， **注释 3** 也专门为突发公共卫生事件应急、人道主义救援、利用境外资源开展国际科研合作以及对外授权许可提供了 **自动许可便利化通道** CN-A1, note 3 CNQA 。
第五项生物医药条目（ `267302J` ，拟禁止出口）则是一道纯粹的 **生物安全防火墙**，严禁出口通过人工基因改造或受控连续传代等方式增强病原体毒力、实现规模化毒力维持或加速病原体定向进化的技术 CN-A1, 267302J，这与美国《出口管理条例》第一类病原体管制及 `EAR 744.4` 生物武器最终用途禁令遥相对应 EAR774 EAR744 。 （与此同时，大批量人类基因组数据在中美两国均另受专门的数据安全法规约束，例如美国司法部实施的“数据安全计划”DOJ 。）

这对两支团队意味着什么

医学中的共享工作台涉及平台、研究与特定治疗。上述区别帮助判断规则触及哪些合作、保留哪些可能。我们不把 AI 游戏得分套用到医学，也不认为开放本身就能证明患者安全。
两队的起点见 堡垒陷阱：双方如何一起受损。

06. 将阳光装进机器：光伏工艺与核心装备

光伏组件畅行全球，“秘密厨房”设闸留存

官方解释区分制造技术及其产品。第 48 号公告没有全面禁止成品光伏板。这不代表其他海关规定或措施不会影响具体运输。 CNQA



图 12 晶体生长炉、薄硅片和涂层设备展示成品太阳能板背后的设备与知识。机器为示意结构。

那么，为何 **40 项技术管制点中有整整 12 项** （5 项拟禁止出口、7 项拟限制出口）精准指向光伏制造? 因为从把普通石英砂提纯为电子级多晶硅、拉制巨型单晶硅棒、切出比办公打印纸更薄的硅片，到涂布下一代钙钛矿叠层电池，中国掌握着全球最精尖的量产工艺体系。当海外多国纷纷祭出高额补贴与进口关税、试图在本土复制整座光伏工厂时，北京决定围绕 **核心工业配方与承载这些配方的物理产线装备** 同步划定边界 CN-A1 CNQA：

1. **高纯晶硅制备（263003J 与 263004X）：** 拟禁止出口条目涵盖超大规模冷氢化流化床工艺（单线年产三氯氢硅 $\geq 250,000$ tonnes/year ）与硅烷流化床法多晶硅工艺（单线年产能 $\geq 20,000$ tonnes/year ）；拟限制出口条目涵盖单线年产能 $\geq 30,000$ -tonne 的多晶硅整线工程成套设计包与单炉年产量 ≥ 800 -tonne-per-furnace 的大型还原炉工艺 CN-A1 。
2. **单晶拉棒与薄如蝉翼的硅片切割（263004J 与 263005X）：** 厚度 ≤ 70 micrometers 的超薄光伏硅片切割技术，明确包含底层控制软件、核心算法与机械工程图纸，被列为 **拟禁止出口** （ `263004J` ）。拟限制出口条目则覆盖大型单晶生长炉（炉膛内径 $\geq 1,600$ mm 或

等径功耗 ≤ 40 kW）、长度 ≥ 720 mm 长硅棒的开方磨削加工、矩形硅片（任一边长 ≥ 182 mm），以及采用直径 ≤ 28 -micrometer 钨丝金刚线切割厚度 ≤ 130 -micrometer 薄硅片的工艺与装备技术 CN-A1 。

3. **钙钛矿叠层与高效晶硅电池（263801J 与 263802X）：** 拟禁止出口条目锁住了量产级 **钙钛矿及晶硅-钙钛矿叠层电池** 核心工艺（叠层电池转换效率 ≥ 30% 、幅宽 ≥ 1.1 -meter 狭缝涂布装备、大面积叠层组件效率 ≥ 28% ）以及超薄大尺寸硅片边缘钝化工艺；拟限制出口条目则涵盖量产效率达标（电池 ≥ 25% 或组件 ≥ 22.3% ）的高通量 **TOPCon、背接触（XBC）与异质结（HJT）** 电池制造工艺 CN-A1 。

注释 4：当物理装备 本身 就是核心配方

正如人工智能软件无法脱离算力芯片而独存，光伏制造诀窍也无法与车间里的炉台装备剥离。当一家装备供应商将薄膜沉积反应腔发往海外、刷入嵌入式控制代码，并派工程师驻厂六个月手把手调试带教时，冰冷的机器内部早已承载着整套工艺心智。

草案注 4 覆盖体现所列技术指标的特定光伏核心设备，包括反应器、晶体炉、晶圆锯及涂层设备。当前受覆盖出口需要临时事前登记。如获采纳，最终目录将区分禁止技术与需要许可的限制技术。许可不能使禁止转移合法，须核对最终文本和程序。CN-A1, note 4 CNQA CNMEAS

这对两支团队意味着什么

成品面板、制造机器和操作知识是不同事物。对合作建厂团队而言，获得其中一项并不能得到其余全部。工作台问题变成哪些设备与知识仍能按适用规则共同流动。

两队的起点见 堡垒陷阱：双方如何一起受损。

07. 华盛顿的守门人：算力芯片与模型权重

扼守全球算力的物理引擎

越过太平洋来到华盛顿特区，映入眼帘的便是全球技术边界体系中历史更久、也更以物理硬件为先导的另一半版图。这套由美国商务部 **工业与安全局（BIS）** 依据 《**出口管理条例**》**（EAR，美国联邦法规汇编 15 CFR 第 730 至 774 部分）**执掌的监管制度，牢牢把控着全球获取 **前沿算力硬件、芯片电子设计自动化（EDA）软件与半导体制造核心装备** 的阀门 EAR734 EAR742 EAR774 。

任何一个可能触及美国出口管制体系的项目，都需要按顺序回答以下四个核心问题：

1. **是否受 EAR 管辖？** 美国境内、原产及指定外国物项有相应条件与排除。公开和基础研究条款有例外，包括加密。使用过某美国软件并不足以认定所有外国芯片受管辖。EAR734
2. **第二问：对应的出口管制分类编码（ECCN，第 774 部分）是什么？** 受控物项在《商业管制清单》（CCL）中均配有专属代码，其中最核心的两个便是代表先进 AI 算力加速卡的 **3A090** ，以及针对特定闭源前沿大模型权重的 **4E091** EAR774 。
3. **第三问：运往哪个目的地（第 742 部分）？** 是否需要申请许可证及适用何种审查标准，直接取决于目的地所属的国家组别。
4. **第四问：最终用户是谁、最终用途是什么（第 744 部分）？** 凡向被列入 **实体清单（744.11）** 的机构供货，或用于受限超级计算机、先进制程半导体制造及大规模杀伤性武器等最终用途（ `744.23` 、 `744.4` ），即便物项本身原本不受限，依然必须申领出口许可证 EAR744 。

2026 年 1 月半导体新规：只是“允许敲门”，绝非敞开大门

在此前整整三年里，输往中国的高端数据中心 AI 芯片一律面临“推定拒绝”的铁门。 **2026 年 1 月 15 日** ，BIS 发布了一项精准校准硬件审查口径的最终规则（联邦公报 `91 FR 1684` ，修订 `15 CFR 742.6(b)(10)` ）：对于从美国直接出口至中国内地或澳门地区最终用户的特定芯片，只要其 **总处理性能（TPP）低于 21,000** 且 **总 DRAM 显存带宽低于 6,500 GB/s** ，规则正文中直接点名英伟达 **H200** 与 AMD **MI325X** 作为处于这一性能窗口的代表型号，便可申请适用 **逐案审查（case-by-case review）** ，而不再直接推定拒绝 US26 EAR742 。

然而只要细读附加条件便会明白，“逐案审查”仅仅意味着允许上前敲门递交申请，绝非免签通行证。申请人必须逐项立据证明：美国本土客户未面临任何供应短缺、全球晶圆代工产能未因此从美国买家处被挤占转移、累计对华出货量严格控制在对美交付量的限定比例之内、已部署严密的物理安防与网络安全“了解你的客户”（KYC）机制以杜绝未经授权的远程调用或实体清单主体使用，并且在芯片装运出口前须经由一家 **总部位于美国的独立第三方检测实验室** 对实际算力与带宽指标完成抽检核验 US26, sections I and IV 。此外，经由第三国转口的再出口交易并不自动适用这一审查通道。

美国 AI 模型权重规则（ `4E091` ）一波三折的奇特法律命运

当华盛顿试图将管制边界从物理芯片向上延伸至虚拟的 **人工智能模型权重** 时，却上演了一出耐人寻味的“三幕法律剧”：

- **第一幕（2025 年 1 月 15 日）：** BIS 公布《**人工智能扩散框架**》临时最终规则（ `90 FR 4544` ），正式增设 ECCN **4E091** 编码，对训练运算量达到 10^{26} 次及以上的闭源前沿模型权重实施出口许可管制，同时在注释中 **明确豁免公开发布的开放权重模型**（以及性能低于当前领先开源模型基准的闭源模型） US25 EAR774, 4E091 。
- **第二幕（2025 年 5 月 13 日）：** BIS 发表官方新闻公报，宣布在正式出台替代法规之前，**指示执法部门暂停执行** 《人工智能扩散框架》规则 USNE 。
- **第三幕（2026 年 5 月 12 日）：** GAO 决定 `B-337935` 认为，不执法政策属于须依《国会审查法》提交的规则。GAO 另记载商务部称撤销已启动但未完成。这是国会审查问题的决定，不是废除或执行 `4E091` 的法院判决。我们另行确认，2026 年 11 月 2 日 BIS 公布的第 774 部分仍列有该条目。 GAO26 EAR774

公开权重条款重要，但 4E091 对私有衍生版本有专门注释。硬件、数据、软件、正式条文与不执行政策须分开。 EAR734 EAR774 GAO26

华盛顿身旁另外两道闸门：跨境美元资本与大批量敏感数据

在商务部 BIS 身旁，还并排站立着另外两位独立的联邦守门人：

- **美国财政部“对外投资安全计划”（Outbound Investment Security Program）：** 自 **2025 年 1 月 2 日** 起，美国主体对中国半导体与微电子、量子信息技术及特定人工智能系统开展股权或特定投资，须面临禁止交易或强制申报审查；**2026 年 10 月 22 日** ，美国财政部又就拟议细化技术门槛的修订规则启动公开征求意见（截止期至 **2026 年 12 月 7 日** ） TREAS 。
- **美国司法部“数据安全计划”（Data Security Program）：** 严格限制向受关注国家跨境批量传输或开放访问美国敏感个人数据（涵盖人类基因组、生物识别、健康医疗、个人金融及精准地理定位数据）与美国政府相关数据 DOJ 。

这对两支团队意味着什么

博弈中的 A 国与 B 国都是虚构的。中美管制在范围、机构及算力供应链位置上不同。本章解释这些差异，不给任何真实国家赋予 3、5、17 或 20 分。
两队的起点见 堡垒陷阱：双方如何一起受损。

08. 两套边界体系与官方审批实操指南

同一座项目桥梁两端相遇的两种监管哲学

将中国 2026 年第 48 号公告与美国《出口管理条例》（EAR）并排铺开，你会看见两个超级大国正分别把守着同一座技术长桥的两端。北京守护的重点是 **本土原创技术成果与企业控制权的向外流失**，追问中国研发的大模型核心、芯片设计蓝图、基因底层平台或光伏产线母机是否正在跨境外移，或变更至境外实际控制人名下；华盛顿把守的重点则是 **全球获取物理算力瓶颈物项与受限最终用户的通道**，在世界范围内严密追踪算力芯片、半导体设备以及“实体清单”机构的每一笔流向 CN48 EAR734 EAR742 EAR744 。

表 3 中国商务部与科技部第 48 号公告同美国商务部 BIS《出口管理条例》横向对比表

对比维度	中国（商务部、科技部 2026 年第 48 号公告体系）	美国（商务部 BIS《出口管理条例》体系）
核心管辖连接点	境内技术所有权向境外转移、授予境外使用许可，或境内技术所有权人/实际控制人变更为境外主体 CN48 CNTIER 。	美国原产物项、位于美国境内的物项，以及依据“外国直接产品规则”采用美国芯片设计软件或设备在境外制造的特定物项 EAR734 。
算力芯片与物理硬件	拟议 `266506X` （<=14nm AI 芯片架构、芯粒封装、<=18nm DRAM/HBM、3D NAND 设计）、 `266507X` （超万卡集群技术）及 所列核心光伏装备 CN-A1 。	ECCN `3A090` 算力芯片、晶圆厂设备与 EDA 软件；2026 年 1 月 `742.6(b)(10)` 对输往中国内地/澳门且 TPP <21,000、带宽 <6,500 GB/s 的芯片改设附条件逐案审查 US26 EAR742 。
前沿大模型权重	拟议 266504X(2)：至少 10^26 次计算、2 万亿参数或合格全球前十。266501J 拟禁止，服务解释有特定适用范围。 CN-A1 CNQA	法典在册 `4E091` （>=10^26 次运算闭源模型权重）；2025 年 5 月 BIS 宣布暂停执行，但 2026 年 5 月美国政府问责局 `B-337935` 号裁决认定新闻稿不能废止成文法典 US25 USNE GAO26 。
开源人工智能待遇	**注释 1** 将已公开开源 AI 与论文排除在目录之外； **注释 2** 对新增开源发布、自建境外算力中心及境外芯片流片给予自动许可（“即报即出”）便利 CN-A1 。	**15 CFR 734.7** （已公开信息豁免）与 **4E091 注释** 明确将无限制公开发布的开源代码与开放模型权重排除在出口许可范围之外 EAR734 EAR774 。
官方在线申报平台	`https://ecomp.mofcom.gov.cn` （商务部业务系统统一平台 - 技术贸易管理信息应用） CN48 CNPLAT 。	`https://snapr.bis.gov` （SNAP-R 电子申报门户）与 `https://snapr.bis.gov/public/stela`

对比维度	中国（商务部、科技部 2026 年第 48 号公告体系）	美国（商务部 BIS《出口管理条例》体系）
		（STELA 审批进度追踪系统）EAR734 SNAPR 。

假设一个跨中国、新加坡的实验室使用覆盖芯片后境外许可私有技术。硬件、人员和用途可能涉及美国规则，技术转移可能涉及中国登记；一项许可不解决两个制度。 CN48 EAR734 EAR744

分步实操指南：如何办理信息登记或申领官方出口许可

市面上绝大多数关于出口管制的文章总是止步于渲染凝重警告，却让真正干实事的创业者、开源项目维护者、高校学者与设备采购方一头雾水地追问一个最朴素的实操问题：“如果我们的模型发布、境外流片或国际合作真的落入了管制范围，究竟归哪个政府部门管？该打开哪个网站填报？法定审批需要多少个工作日？遇到疑问又该打哪个电话、发哪个邮箱？”图 13 展示申报涉及的文件。下文分别列出两国的步骤与联系方式。 CN48 CN-A2 CNTIER CNMEAS CNPLAT EAR734 EAR742 SNAPR



图 13 研究人员提交技术文件供审核。该图介绍文书工作，不是完整法律程序，也不保证获批。

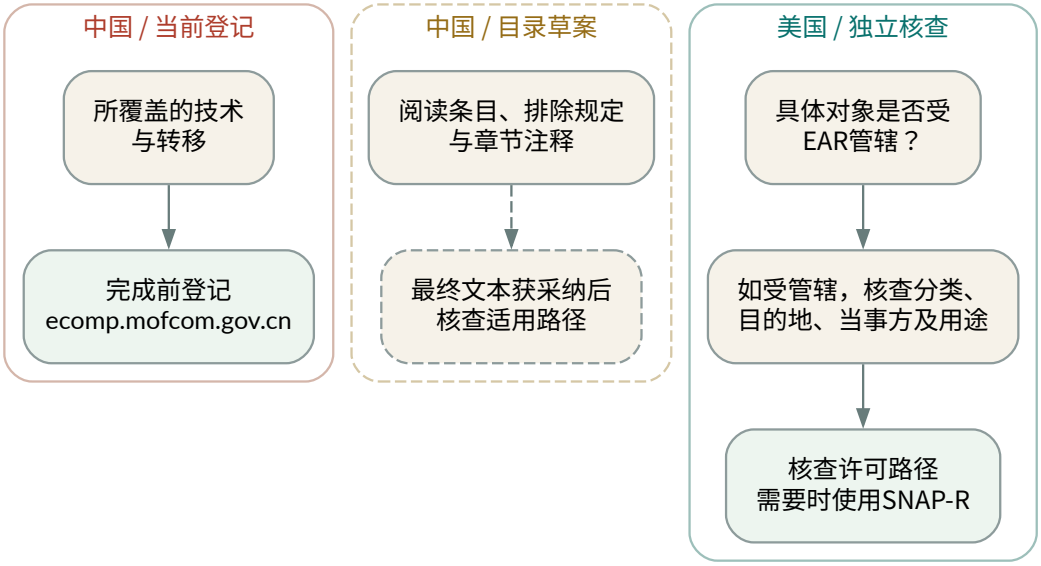


图 14 中国当前登记、目录草案和美国管辖是独立核查。虚线表示拟议路径。

中国篇：主管政府部门、法定审批时限与核验通讯录

在中国，技术出口管理依据《中华人民共和国技术进出口管理条例》（中华人民共和国技术进出口管理条例 第 30 至 39 条）与《禁止出口限制出口技术管理办法》（禁止出口限制出口技术管理办法，商务部、科技部 2009 年第 2 号令第 4 至 18 条），实行清晰的**“中央统筹制定目录与统一平台 + 省级属地实质审批发证”协同机制**：北京的**商务部**与**科学技术部**负责制定国家目录政策并运行全国统一的在线业务系统平台；而具体的限制出口技术许可证，则由出口经营者注册地所在的**省、自治区、直辖市商务主管部门**会同**同级科技行政主管部门**依法审查签发 CN48 CNTIER CNMEAS 。

> **重要**
> **期限范围：** 30 及 15 个工作日是现有标准限制技术流程，不保证总共 45 个自然日，也不是临时登记或未来自动许可期限。谈判、材料及其他审查可能增加时间。联系方式按来源刊载，使用前核对当前渠道。

中国境内的三条法定在线申报路径

1. **路径 A：强制性出口前信息登记（自 2026 年 10 月 16 日起即日执行）：**
   - **适用时点：** 凡涉及附件 1 所列 40 项技术控制点，拟向境外转移境内技术所有权、许可境外使用境内技术，或将境内技术所有权人/实际控制人变更为境外主体的（包括 10 月 16 日前已启动但尚未交割完成的进行中交易），均须在行为完成前办妥登记 CN48, section III 。
   - **办理方式：** 登录**商务部业务系统统一平台**（`https://ecomp.mofcom.gov.cn`），进入**商务部业务系统统一平台 - 技术贸易管理信息应用**（技术贸易管理信息应用），在线填报并提交加盖单位公章（公章）的**附件 2**《技术出口信息登记表》（须如实列明技术所有权人、境外接收方中英文名称/国别/地址/关联关系、七位目录编号、控制要点技术指标、最终用户与用途及折算美元合同金额） CN48 CN-A2 CNPLAT 。
2. **路径 B：开源发布、境外芯片流片与自营算力云快车道（注释 2、3 拟议“自动许可”）：**
   - **适用场景：** 待修订后的正式目录生效实施后，适用于通过开源方式出口限制类人工智能技术、在中资企业**自建自营的境外算力中心**部署大模型、赴境外晶圆代工厂开

展 **芯片流片**（芯片流片）、参与国际联合研发或国际标准制定，以及生物医药领域受控新靶点的对外授权许可与人道主义应急救援 CN-A1, notes 2 and 3。
- **已说明的内容：** 草案提出自动许可等便利，并未确定完整最终程序或保证周转时间，应向主管部门核实。 CN-A1 CNQA

3. **路径 C：标准两阶段限制出口技术许可审批（技术出口许可证）：**
   - **第一阶段，开展实质性谈判或签约前预申请（合计不超过 30 个工作日）：** 向所在地**省级商务主管部门**（省、自治区、直辖市商务主管部门）提交《中国限制出口技术申请书》（中国限制出口技术申请书） CNMEAS, Arts. 4-5。省级商务部门在收到申请后 **5 个工作日内** 将技术审查材料转送 **省级科技行政主管部门**（省、自治区、直辖市科技行政主管部门），由后者组织专家在 **15 个工作日内** 完成技术审查 CNMEAS, Art. 7。自收到申请之日起 **总计 30 个工作日内**，主管部门作出是否准予许可的决定；获批的，签发有效期 **最长 3 年** 的 **《中华人民共和国技术出口许可意向书》**（中华人民共和国技术出口许可意向书） CNTIER, Arts. 35-36 CNMEAS, Arts. 6, 10。（法定铁律：未取得《技术出口许可意向书》之前，任何单位或个人不得对外进行实质性谈判，不得作出具有法律约束力的出口承诺 CNMEAS, Art. 11。）
   - **第二阶段，正式签订合同后申领许可证（不超过 15 个工作日）：** 取得意向书并正式签约后，出口经营者在统一平台登记合同信息，并向省级商务主管部门报送四项法定文件：**(i)**《技术出口许可意向书》、**(ii)** 已签署的技术出口合同副本、**(iii)**《技术资料出口清单》（技术资料出口清单），以及 **(iv)** 签约双方法律地位证明文件 CNTIER, Art. 37 CNMEAS, Arts. 13, 16。省级商务主管部门对合同真实性进行审查，并在 **15 个工作日内** 作出决定；准予许可的，颁发正式 **《中华人民共和国技术出口许可证》**（中华人民共和国技术出口许可证） CNTIER, Arts. 37-38 CNMEAS, Art. 14。**关键法定效力条款：** 限制出口技术合同 自《技术出口许可证》颁发之日起方才生效；申请人须凭该许可证办理 **海关报关、外汇收付、银行结算与税务核销** 等全部后续手续 CNTIER, Art. 38 CNMEAS, Arts. 15, 18 CNQA。

经核验的中国官方主管部门通讯录

- **中央牵头主管部门（目录政策制定、范围解释与公开征求意见）：** 中华人民共和国商务部产业安全与进出口管制局（中华人民共和国商务部安全与管制局），会同中华人民共和国科学技术部（科学技术部） CN48。
- **信函邮寄地址：** 中国北京市东长安街 2 号商务部安全与管制局，邮政编码：100731（北京市东长安街2号商务部安全与管制局，邮编：100731） CN48。
- **官方意见反馈与政策咨询邮箱：** jinxianmulu@mofcom.gov.cn（*2026* 年 *11* 月 *15* 日前提交公开征求意见的，请在邮件主题注明《中国禁止出口限制出口技术目录》公开征求意见，并附有效联系方式；以单位名义反馈的须加盖单位公章） CN48。
- **官方传真：** +86-10-6519-7565（010-65197565） CN48。
- **全国统一在线登记与许可申报平台：** https://ecomp.mofcom.gov.cn，商务部业务系统统一平台 - 技术贸易管理信息应用（商务部业务系统统一平台 - 技术贸易管理信息应用，已整合原 jsjckqy.fwmys.mofcom.gov.cn 系统） CN48 CNMEAS, Art. 16 CNPLAT。
- **统一平台技术支持热线：** +86-10-6787-0108（86-10-67870108） CNPLAT。
- **属地审批发证机关：** 出口经营者注册地所在的省、自治区、直辖市商务主管部门会同同级科技行政主管部门（所在地省、自治区、直辖市商务主管部门会同科技行政主管部门） CNMEAS, Art. 4。

美国篇：联邦监管机构、SNAP-R 电子申报流程与核验通讯录

在美国，两用物项硬件、软件及技术的出口许可由 **美国商务部** 下辖的 **工业与安全局（BIS）** 在联邦层面统一执掌，所有通过官方电子系统提交的分类与许可证申请均免收政府行政规费 EAR734 EAR742 SNAPR。

办理美国物项分类认定或申领出口许可的四个标准步骤

1. **先看管辖和公开状态：**按 734.3、734.7、734.8 及 4E091 核对文件。合格公开内容可在 EAR 之外；某目的地无需许可不等于不受 EAR 管辖。744 部分通常针对受 EAR 物项，其他制裁和美国人规则另行分析。 EAR734 EAR744 EAR774
2. **第二步，在 SNAP-R 系统注册企业识别号（CIN）：**拟出口受控算力硬件（ `3A090` ）、半导体设备或私有受控技术的经营主体，须前往 BIS **简化网络申请流程再设计系统（SNAP-R）**门户 `https://snapr.bis.gov` 在线免费注册企业识别号（美国境内主体可提交出口许可证申请；美国境外主体亦可注册提交再出口许可证或物项分类认定申请） EAR734 SNAPR 。
3. **第三步，拿不准编码时提交官方物项分类认定（CCATS）或政策咨询：**在 `snapr.bis.gov` 创建物项分类工作项（Commodity Classification Work Item）并上传详细技术参数表，即可获取具有官方效力的 ECCN 归类裁定书（系统生成专属 `ACN` 追踪号），亦可直接联系 BIS 法规政策处咨询条文适用解释 EAR734 SNAPR 。
4. **第四步，在线递交许可证申请并通过 STELA 追踪进度：**上传 PDF 证明附件、最终用户声明与产品规格书（针对适用 2026 年 1 月 `742.6(b)(10)` 规则输往中国内地或澳门的芯片逐案审查，须一并附上 `TPP < 21,000` 、 `DRAM bandwidth < 6,500 GB/s` 、美国本土供应充足、KYC 安防机制及美国本土独立第三方实验室检测核验等全套证明文件） US26 EAR742 SNAPR 。提交后可在 **STELA** 系统（ `https://snapr.bis.gov/public/stela` ）实时查询跨部门联审状态 EAR734 。

经核验的美国官方监管机构通讯录

- **电子申报与审批追踪门户：** SNAP-R 在线申报门户： `https://snapr.bis.gov` | STELA 审批进度追踪系统： `https://snapr.bis.gov/public/stela` EAR734 SNAPR 。
- **SNAP-R 技术服务台与账户支持：**系统技术支持邮箱： `snapr@bis.doc.gov` | 账户找回与授权官员证明函（Empowered Official）受理邮箱： `ECDOEXS@bis.doc.gov` SNAPR 。
- **BIS 外联与教育服务处（华盛顿特区总部）：** U.S. Department of Commerce, 14th and Pennsylvania Avenue, NW., Room H1099D, Washington, DC 20230 | 电话： `+1 (202) 482-4811` | 传真： `+1 (202) 482-2927` EAR734 。
- **BIS 西部地区办公室（南加州尔湾）：** 2302 Martin St., Suite 330, Irvine, CA 92612 | 电话： `+1 (949) 660-0144` | 传真： `+1 (949) 660-9347` EAR734 。
- **BIS 北加州分部（硅谷圣何塞）：** 160 W. Santa Clara Street, Suite 725, San Jose, CA 95113 | 电话： `+1 (408) 998-8806` | 传真： `+1 (408) 998-8677` EAR734 。
- **BIS 法规政策处（Regulatory Policy Division）：** Room 2099B, U.S. Department of Commerce, Washington, DC 20230 | 电话： `+1 (202) 482-2440` | 邮箱： `RPD2@bis.doc.gov` US25 US26 EAR742 。
- **BIS 半导体与人工智能技术规则负责人：** 第 3 类半导体（ `3A090` ）：Carlos Monroy， `+1 (202) 482-3246` ， `Carlos.Monroy@bis.doc.gov` US25 US26 | 第 4 类计算机与 AI 模型权重（ `4E091` ）：Aaron Amundson， `+1 (202) 482-0707` ， `Aaron.Amundson@bis.doc.gov` US25 。
- **美国财政部，对外投资安全计划（Outbound Investment Security Program）：** `https://home.treasury.gov/policy-issues/international/outbound-investment-program` | 业务咨询： `Outbound@treasury.gov` | 法规意见： `OIS.Outbound.Regulations@treasury.gov` | 申报系统支持： `Outbound.ITSupport@treasury.gov` TREAS 。
- **美国司法部国家安全司，数据安全计划（Data Security Program）：** `https://www.justice.gov/nsd/data-security` | 合规申报咨询： `NSD.FIRS.datasecurity@usdoj.gov` | 公共事务联系： `nsd.public@usdoj.gov` DOJ 。

这对两支团队意味着什么

工作台故事现在成为实际问题：转移什么、哪个体系管辖、还剩哪条路径？明确排除、可用程序与可信持续合作可能改变激励。效果需要证据，填好表格本身不能证明合作已改善。

两队的起点见 堡垒陷阱：双方如何一起受损。

09. 日常情境与实战：读者田野指南

我还能把 DeepSeek、Qwen 或其他开源模型下载到自己的电脑或服务器上运行吗?

公告没有全面禁止下载公开模型。排除均有条件。私有微调、受限数据或后续转移需另查，公共原版不是所有衍生物和用途的通用批准。 CN-A1, note 1 EAR734 EAR774

既然软件挂的是 MIT 或 Apache 2.0 宽松协议，物理硬件管制还会影响开源 AI 吗?

影响极为深远。一份 MIT 许可证赋予你的是运行模型的 法律权利 ，而物理 GPU、HBM 高带宽存储与高速集群互联网络赋予你的才是训练或运行它的 物理能力 。美国法规（ `3A090` 、`742.6(b)(10)` ）决定着谁能买到先进 AI 加速卡；中国拟议的 `266506X` 与 `266507X` 则规制着 AI 处理器架构、3D NAND/DRAM 存储设计以及超万卡集群系统工程技术的跨境转移（同时由注释 2 为赴境外晶圆厂流片提供便利）CN-A1 US26 EAR742 。因此，任何跨境项目都必须同时核查软件仓库与随同流动的定制芯片或集群工程技术栈。

如果海外用户通过网页对话使用我们的 AI 应用或调用云端 API，这算出口大模型吗?

商务部区分拟议措施下限制类大模型服务与技术转移。API、应用、网页、SaaS 和轻量部署并非对核心数据、其他物项、数据法律或当前登记的通用豁免。 CNQA

我们的实验室和服务器都留在国内，但境外投资方正在收购公司控制权，需要办登记吗?

请立即启动核查！第 48 号公告第三条第（二）款明确规定：凡涉及附件 1 所列境内技术的 **所有权人或实际控制人变更为境外主体** 的，哪怕每一台服务器与每一位工程师都留在国内原地不动，亦必须在变更完成前履行出口前信息登记 CN48, section III(2) 。此外，若交易中有美国投资人参与，还须同步核查美国财政部“对外投资安全计划”的合规义务（咨询邮箱 `Outbound@treasury.gov` ） TREAS 。

在正式开源发布或跨境合作前，一份两页纸的“发布合规护照”应当记录哪些内容?

在启动任何重磅开放权重发布、境外芯片流片或跨境技术授权之前，建议在团队内部留存一份整洁可查的合规备忘档案，如实记录六项要素：**(1)** 准确版本号与文件 SHA-256 哈希值；**(2)** 已逐条比对的目录编码（如 `266504X` 、`266506X` 、`266507X` 、`3A090` 、`4E091` ）；**(3)** 实测累计训练算力 FLOPs、总参数量及发布当日主流公开榜单排名截图；**(4)** 训练语料合规审计记录（确认零核心数据，并留存重要数据属合法公开渠道或不超过 0.1% 脱敏微量占比的证明）；**(5)** 既有公开发布凭证或首次发布状态说明；**(6)** `ecomp.mofcom.gov.cn` 信息登记回执或美国 `snapr.bis.gov` 申报追踪号（ACN）副本 CN-A1 CN-A2 SNAPR 。

六个真实世界实战场景

> **备注**
> **场景适用说明：** 以下六个案例旨在直观演示经核验的法规条文如何在现实业务中落地运行；在推进具体项目前，请务必结合实际案情核对官方原始法律文本。

1. 在本地微调已公开发布的开放权重模型
假设医院研究团队本地改进公开权重。公共原版与后续私有临床版本不同，须查公开条款、数据和后续交付。版权许可不证明临床安全，也不是政府批准。 CN-A1, note 1 EAR734 EAR774
2. 中国实验室首次向全球开源一款位列全球前十的新模型
一家中国人工智能实验室准备将刚刚训练完成的一款全新推理大模型首次面向全球开源上传，而当时主流权威评测榜单将其排在全球第 7 名（触及 `266504X(2)` 指标）。团队首先须确认训练数据不含国家核心数据（ `266501J` ）并符合重要数据公开或微量脱敏豁免规则；在 2026 年 10 月 16 日之后的过渡期内，通过 `ecomp.mofcom.gov.cn` 核实履行出口前信息登记；待正式修订目录生效后，则可直接走 **注释 2 设立的自动许可快车道** （“即报即出”）合规开源 CN48 CN-A1, note 2 CNQA 。
3. 向外国商业伙伴私下授权未公开前沿权重或定制芯片 IP
一家北京技术团队签署闭源商业合同，拟向某境外企业交付尚未公开的 2.4 万亿参数模型权重（ `266504X` ）或一套定制 7 纳米 NPU 指令集计算 IP 核（ `266506X` ）。由于这属于一对一私密商业技术出口而非公开开源，现阶段必须立即在 `ecomp.mofcom.gov.cn` 填报 **附件 2 出口前信息登记表** ；待修订目录正式实施后，则须履行 **省级商务主管部门会同省级科技部门的两阶段审批** （30 个工作日内审发《技术出口许可意向书》 + 签约后 15 个工作日内审发正式《技术出口许可证》） CN48 CNTIER CNMEAS 。（注：若仅将芯片版图发往境外晶圆代工厂开展流片制造，则适用注释 *2* 的自动许可便利。）
4. 面向海外用户提供网页端对话或按量计费的远程 API 服务
一家上海初创企业将旗舰前沿大模型部署在境内服务器上，通过网页端交互界面与 HTTPS API 接口为海外客户提供智能问答与推理服务。商务部官方答记者问明确确认：在不转移底层模型权重与核心源代码的前提下，此类远程 API 调用及应用层服务 **不纳入大模型技术出口管理范围** （前提是模型未采用拟禁止出口的国家核心数据 `266501J` 训练） CN-A1 CNQA 。
5. 境外风险投资架构重组或跨国控制权并购
一家握有未公开 `266505X` 六十智能体协同编排系统或 `262705X` 全新未公开基因治疗靶点发现引擎的深圳初创企业开展跨境股权重组，使一家境外离岸控股主体成为其新的实际控制人。哪怕没有任何一个字节的文件离开深圳机房，根据第 48 号公告第三条第（二）款，企业仍须 **在控制权变更交割完成前办妥出口前信息登记** ，且若有美国美元基金参与本轮交易，还须并行核查美国财政部的对外投资安全审查规则 CN48, section III(2) TREAS 。
6. 向海外整线出口光伏硅片切割或钙钛矿涂布装备

一家中国光伏装备制造商签约向海外新建光伏工厂发运单晶生长炉与 PECVD 镀膜机，并随附工艺配方包及驻厂工程师调试服务。根据目录草案 **注释 4**，只要这些物理机器承载了 `263004X` 至 `263802X` 所列受控技术指标，装备本身即直接纳入技术出口管制（而若涉及 `<=70 微米` 超薄硅片切割 `263004J` 或 `>=30%` 转换效率钙钛矿叠层工艺 `263801J`，则面临拟禁止出口红线）。企业必须在合同履行完成前通过 `ecomp.mofcom.gov.cn` 办妥出口前信息登记 CN48 CN-A1, note 4 CNQA 。

10. 原始文献、核验方法与通俗术语表

本书每一处事实是如何逐一核验的

截至 2026 年 11 月 2 日，我们对照 26 项法律、技术和研究来源检查论述。新增研究帮助分析合作与风险，但不会使假设变为实测结果。联系方式来自所引记录，可能变化。
我们对官方原始 WPS 字节流及其 SHA-256 加密哈希值均原封不动予以归档，并同步附上转换后的 PDF 便捷阅读版。针对美国政府问责局（GAO）服务器拦截自动化脚本抓取（返回 `HTTP 403` ）的情形，我们在文献表中如实透明注明。纵观全书，所有一手法律事实均标有方括号文献代号；而书中的博弈论收益矩阵与未来演进情境，则均坦诚标明属于数理分析模型与示例推演，不构成针对任何具体商业交易的正式法律意见。

原封不动保存的官方原始文件副本

- 商务部与科技部 2026 年第 48 号公告官方页面归档（PDF 阅读版）
- 附件 1：40 项拟新增管制技术目录（WPS 原始原件） | 转换后 PDF 阅读版
- 附件 2：《技术出口信息登记表》（WPS 原始原件） | 转换后 PDF 阅读版
- 商务部、科技部 2009 年第 2 号令：《禁止出口限制出口技术管理办法》（官方 PDF 原件）
- 美国 BIS 2026 年 1 月半导体许可证审查最终规则 91 FR 1684（官方 PDF 原件）
- 美国 BIS 2025 年 1 月《人工智能扩散框架》规则 90 FR 4544（官方 PDF 原件）
- 美国 BIS 官方 SNAP-R 电子申报操作指南与常见问题解答（官方 PDF 原件）
- 机器可读文献溯源与 SHA-256 哈希核验清单（sources.json）

写给普通读者的通俗术语表

模型权重（Model weights / 参数）
训练中学到、影响模型输出的数值。权重本身不包含可复现或安全系统的所有组成部分。

检查点（Checkpoint）
在模型训练中途或收敛完成时保存下来的参数快照，可用于断点续训、蒸馏轻量化小模型，或针对医疗、法律等垂直任务开展微调。

浮点运算次数（FLOPs）
模型训练全过程累计执行的每一次基础数学浮点运算。10^{26} **FLOPs**（即 1 后面跟着 26 个零）是中国拟议 `266504X` 条款与美国 `4E091` 条款共同采用的前沿大模型算力门槛。

总处理性能与高带宽存储（TPP 与 HBM 硬件瓶颈）
总处理性能（TPP）衡量一颗 AI 芯片的综合算力吞吐量，而 **高带宽存储器（HBM / DRAM 带宽）**则决定数据喂入计算核心的速度（美国 2026 年 1 月对华逐案审查条款 `742.6(b)(10)` 将两道上限分别卡在 `TPP < 21,000` 与显存带宽 `< 6,500 GB/s` ）。

芯片流片（ 芯片流片 ）
芯片设计团队完成全部电路与版图设计后，将最终设计文件交付半导体晶圆代工厂试产或量产实体硅晶圆的关键环节，第 48 号公告附件 1 注释 2 明确对赴境外开展芯片流片给予自动许可便利。

远程 API / SaaS 服务（“面包店窗口”）
允许境外或远程用户向你的云端服务器发送提问并接收模型生成的回答，但全程不向对方交付底层模型权重、核心源代码或芯片设计图纸。

纳什均衡
任何一方都不能仅改变自己的选择而提高收益的状态。均衡不一定僵持、安全、公平或对社会最好。相互筑墙只在本例假设下构成均衡。 GAME

开源软件许可证 vs. 政府技术出口许可证
MIT 或 *Apache 2.0* 许可证是创作者授予公众自由使用、修改与再分发代码或权重的民事著作权授权；而《技术出口许可证》（ 技术出口许可证 或美国 BIS 许可证）则是主权国家政府签发、准许受控技术或硬件跨越国境的行政许可批件。

自动许可（ 自动许可 ）
第 48 号公告附件 1 注释中针对开源人工智能出口、中资自建自营境外算力中心、境外芯片流片及人道主义生物医药合作提出的便捷许可机制，商务部政策解读将其概括为基本实现“即报即出”（ 即报即出 ）。

ECCN、CCATS 与 SNAP-R
在美国出口管制体系中， **ECCN** （如 AI 芯片的 `3A090` 、模型权重的 `4E091` ）是受控物项的分类编码； **SNAP-R** （ `snapr.bis.gov` ）则是出口商免费在线提交出口许可证申请与 **CCATS** 官方物项分类认定申请的电子政务门户。

全部 26 份经核验一手官方文献总表

表 4 截至 2026 年 11 月 2 日逐一核验的一手法律、行政法规与技术原始文献名录

文献代号	官方文献名称与核验范围	发布/核验日期	原始网址与 SHA-256 哈希前缀
`CN48`	中国商务部、科技部 2026 年第 48 号公告正文（第一、二、三条）	2026-10-16	mofcom.gov.cn (`a5261a74...`)
`CN-A1`	第 48 号公告附件 1:《中国禁止出口限制出口技术目录》40 项拟新增技术与 4 条注释（WPS）	2026-10-16	WPS 原始原件 (`213158bb...`)
`CN-A2`	第 48 号公告附件 2:《技术出口信息登记表》（WPS）	2026-10-16	WPS 原始原件 (`d65818c2...`)
`CNQA`	商务部新闻发言人就 2026 年第 48 号公告《目录》调整公开征求意见答记者问	2026-10-16	mofcom.gov.cn (`37fc685a...`)
`CNTIER`	国务院《中华人民共和国技术进出口管理条例》（第 30 至 39 条）	2020-11-29	xzfg.moj.gov.cn (`39f4b9bb...`)
`CNMEAS`	商务部、科技部 2009 年第 2 号令《禁止出口限制出口技术管理办法》	2009-04-20	mofcom.gov.cn PDF (`d14e5230...`)
`CNPLAT`	商务部业务系统统一平台 - 技术贸易管理信息应用通知与支持热线（ `+86-10-6787-0108` ）	2026-11-02	mofcom.gov.cn (`5bc9740f...`)

文献代号	官方文献名称与核验范围	发布/核验日期	原始网址与 SHA-256 哈希前缀
US26	美国 BIS 半导体许可证审查政策修订最终规则（ 91 FR 1684 ；742.6(b)(10) ）	2026-01-15	govinfo.gov (d3b27863...)
US25	美国 BIS《人工智能扩散框架》临时最终规则（ 90 FR 4544 ； 4E091 ）	2025-01-15	govinfo.gov (6e202458...)
USNE	美国商务部 BIS 指示暂停执行《人工智能扩散框架》规则的官方新闻公报	2025-05-13	bis.gov (14a05e6e...)
GAO26	美国政府问责局（GAO）关于 AI 扩散规则与《国会审查法》的 B-337935 号裁决	2026-05-12	gao.gov （*HTTP 403*；经网页实地核验）
EAR734	15 CFR 第 734 部分，EAR 管辖范围、公开开源豁免（ 734.7 ）与官方联系名录	2026-11-01	bis.gov/ear/734 (eeb76281...)
EAR742	15 CFR 第 742 部分，基于商业管制清单（CCL）的审查政策（ 742.6(b)(10) ）	2026-11-01	bis.gov/ear/742 (3eccf859...)
EAR744	15 CFR 第 744 部分，基于最终用户与最终用途的管制（ 744.11 、 744.23 ）	2026-11-01	bis.gov/ear/744 (ab19c823...)
EAR774	15 CFR 第 774 部分，《商业管制清单》（ECCN 3A090 与 4E091 ）	2026-11-01	bis.gov/ear/774 (01d3beba...)
SNAPR	美国 BIS SNAP-R 电子申报常见问题与联系指南（ snapr.bis.gov ）	2026-11-02	snapr.bis.gov PDF (e0c3bdee...)
TREAS	美国财政部“对外投资安全计划”及 2026 年 10 月拟议细化规则	2026-10-22	home.treasury.gov (75f52eee...)
DOJ	美国司法部国家安全司，“数据安全计划”（Data Security Program）	2026-11-02	justice.gov/nsd (1bf01adb...)
OSI	国际开源促进会（OSI），《开源人工智能定义 1.0》（OSAID 1.0）	2024-10-28	opensource.org (a5442179...)
R1	DeepSeek-R1 官方开源仓库与 MIT 许可证记录	2025-01-20	github.com/deepseek-ai (875b282c...)
QWEN	通义千问 Qwen3 官方开源仓库与 Apache 2.0 许可证记录	2025-04-29	github.com/QwenLM (2b7cdab9...)
GD	GuideDog 文档与多语种图书出版引擎（ v1.0.0-beta.10 ）	2026-11-02	github.com/insanai/guidedog (6fe7704f...)

本次审阅新增的研究与历史来源

- NTIA：2024 年 7 月的开放权重报告，评估当时模型的收益、风险和监测建议，不能证明所有未来模型的情况。 Dual-Use Foundation Models with Widely Available Model Weights (July 2024)
- OPENRISK：讨论开放基础模型社会影响的研究。有关边际风险的论证不是出口管制因果影响的实测。 On the Societal Impact of Open Foundation Models
- GAME：网络与市场教材第 1 章，定义博弈、最优回应与均衡。具体分数及重复博弈计算是本书示例。 A Course in Networks and Markets, Chapter 1
- JEFFERSON：1813 年 8 月 13 日致 Isaac McPherson 的信，是蜡烛比喻的原始出处；比喻本身不证明经济影响。 Thomas Jefferson to Isaac McPherson, 13 August 1813

作者、协助与再使用

作者为 **Vikrant Rathore**，由 **Jennifer Yuan、Vicky Ni、Ronak Rathore 和 Kanak Rathore** 协助。

原创文字、编辑工作及新插图插图采用 **CC BY-SA 4.0**。使用时须署名，改编须沿用同一许可。官方文件、引文、字体、软件和其他第三方材料保留自身版权及许可，范围见仓库 LICENSE 和 NOTICE。

七种语言均为编辑译文，未经独立法律或母语专业审核。原法律文本优先。例子和博弈分数不是官方分类或实测预测。

可选阅读：核算博弈例子

不看这些计算也能理解开篇故事。这里为希望核算的读者明确额外假设。

为什么结局稳定

20 > 17 > 5 > 3 的排序使每国无论对方如何，都有理由限制。两道墙存在时，单独共享会从 5 降到 3。相互共享在这个小游戏中是帕累托有效的：其他所列结局都不能在不损害一方的情况下改善另一方。但这不代表各国都获得其个人最高分。 GAME

未来合作的重要性

下一项计算额外把虚构分数视为每轮可比较的收益。数字门槛取决于该尺度，而不只是偏好排序。

国家会反复互动。例中双方共享就继续合作，一次偏离可得 20，此后永远得 5。δ 表示下一轮相对当下的价值。合作至少同样有利的条件是：

$$\frac{17}{1-\delta} \geq 20 + \frac{5\delta}{1-\delta} \quad \Longleftrightarrow \quad \delta \geq \frac{1}{5}$$

这是假设博弈内的计算，不是外交预测。它假定无限期关系、可观察选择和可信回应；错误、隐藏行动或已知最后一轮可能破坏策略。关键在如何使持续合作可信。 GAME

可选阅读：独立审查不保证安全

开放可方便独立测试与修复。若缺陷存在概率为 p_0，每个独立团队发现概率为 q，共有 n 个团队，则：

$$P(\text{flaw remains undetected}) = p_0(1-q)^n$$

已知存在缺陷且每队发现概率假定一半时，1 队漏检 50%，4 队 6.25%，10 队约 0.098%。这是条件计算。现实团队可能盲点相同、资源不足，或发现后未修复。漏检概率不是总体网络、生物或社会风险。

公开权重也可能方便恶意修改或删除防护。NTIA 在 2024 年权衡收益与风险，建议监测当时的开放权重。研究强调比较相对现有替代品的新增风险；两者均未确立普遍的安全倍数。 NTIA OPENRISK