东南亚离岸算力与黑色算力网络研究

离岸算力与”黑色算力网络”：中国企业通过东南亚获取受管制 AI 算力的模式、案例与政策含义

> **研究类型**：深度政策研究报告 **主题**：东南亚离岸算力获取机制与”黑色算力网络”的合规灰色地带 **受众**：政策制定者、半导体产业分析师、地缘政治研究者 **写作日期**：2026-08-20 **作者立场说明**：本报告基于公开可考资料撰写，所有论断区分事实陈述与合理推测；事实陈述附来源，依据不足之处明确标注”推测”或”待证”。

摘要

2022 年 10 月以来，美国商务部工业与安全局（BIS）通过《出口管理条例》（EAR）针对先进计算芯片（AI 加速器）和半导体制造设备对中国构建了三轮高强度管制，其核心是”总算力—带宽—制程”组合阈值与外国直接产品规则（FDPR）的扩张。然而，物理意义上的芯片入境已不再是中方获取先进算力的唯一通道：受管制芯片部署在境外数据中心，通过跨境网络以 API、虚拟实例、托管训练或推理服务的形式回流中国，形成事实上的”算力入境”。本研究围绕”黑色算力网络”（black

compute network）这一非学术术语所指代的现象展开，聚焦中国企业如何通过东南亚构建并使用离岸算力。

研究首先验证并细化美国”数字化安全与新兴技术”相关智库（DSET 框架，Digital Safety and Emerging Technologies）提出的四种区域数据中心部署模式：**影子绿地投资、合资企业、机柜共置、混合云架构**。在此基础上，研究补充了 DSET 框架未覆盖的四类现实模式：**壳公司租赁、API/模型蒸馏回传、设备拆解回流与暗网/加密算力市场**。通过对马来西亚柔佛、新加坡、泰国、印度尼西亚、柬埔寨与菲律宾的案例比较，研究发现：

1. 柔佛-新加坡走廊是当前”黑色算力网络”的物理与法律心脏地带；
2. 现行 EAR 以”实体货物跨境流转”为核心抓手，对**远程算力租赁服务**这一新型出口对象存在系统性盲区；
3. 2026 年 8 月 BIS 已开始将算力租赁纳入审查，但因域外适用与”穿透审查”原则的固有张力，短期内难以完全封堵；
4. 中国企业、东南亚本地资本、美国云厂商与第三国中间商之间已经形成多层”风险切割”链条，使责任归属与举证高度复杂化。报告最后评估了对区域生态、国家安全与全球 AI 治理的影响，并提出可操作的合规与执法建议。

> **术语说明**：本报告中”黑色算力网络”并非严格的法律概念，而是用以概括**以规避美国出口管制为目的、通过离岸部署与远程接入使受管制芯片算力被中国主体实质使用**的所有安排。其外延包括违法的走私与虚假陈述（“黑”），也涵盖合法但具政策规避性质的远程云租（“灰”）。

引言

1.1 问题背景：从”卡芯片”到”卡算力”的范式转变

美国对华半导体管制的核心逻辑从 2022 年起发生根本转变。10 月 7 日的”先进计算规则”（ACR）首次引入**性能阈值**概念：单芯片 INT8 算力超过 4800 TOPS、FP16 超过 300 TFLOPS 或互连带宽超过 600 GB/s 即受管制；该规则不点名特定型号，而是按性能参数定义”先进计算芯片”。2023 年 10 月的更新进一步封堵了 NVIDIA A800、H800 等”降规版”，并将管制推及 40 余家中国 AI 与超算实体。2025 年 1 月拜登政府卸任前又新增”AI Diffusion Rule”，将全球划分为三个层级，对 Tier 2 / Tier 3 国家（含大部分东南亚国家）的 GPU 部署设定总算力上限，并在 2025 年 5 月被特朗普政府实质废止但部分条款被并入 EAR。

英伟达为中国市场设计的多代”阉割版”产品（H20、A30、L40、L4）始终未能满足中国头部 AI 实验室的千亿—万亿参数训练需求。**当实物芯片入境被封堵后，“算力”本身便成为一种可贸易、可跨境、且几乎不受现行 EAR 管辖的服务**——这是”黑色算力网络”得以形成的根本原因。

1.2 东南亚为何成为首选离岸节点

东南亚之所以在 2024—2026 年迅速成为离岸算力枢纽，存在四重结构性诱因：

维度	优势	主要表现
地缘	临近中国，海底光缆密集	新加坡—柔佛走廊、海底光缆 SEA-ME-WE 6 / ASE
法律	普通法系与外商投资便利	新加坡 PSA、英属维尔京壳公司
能源	电力与土地成本相对低	柔佛州水电配额、印尼地热
合规	本地无类似美国 FDPR 限制	多数国家无”最低规则含量”（de minimis）限制

柔佛-新加坡走廊的现象级集中（柔佛州 2025 年 Q2 获批数据中心投资 1644.5 亿令吉，约 390 亿美元，占马来西亚运营 IT 容量的 78.6%）即源于上述四要素叠加。

1.3 报告结构

报告第二部分验证并细化 DSET 四分类；第三部分补充 DSET 未覆盖的其他模式；第四部分进行区域案例比较；第五部分解析出口管制规避机制与灰色地带；第六部分评估”黑色算力网络”对区域生态、国家安全与全球 AI 治理的影响；第七部分给出结论与研究局限。

第二部分：DSET 四种模式的验证与阐述

DSET（Digital Safety and Emerging Technologies）框架源自美国国会咨询机构对中美科技竞争的跟踪研究。该框架将中国企业在东南亚获取先进算力的主要安排划分为四种部署模式。本研究在公开案例与 BIS、SEC、商务部公告的基础上对其进行验证与扩充。

2.1 模式一：影子绿地投资（Shadow Greenfield Investment）

定义：中国资本通过境外控股架构（开曼/BVI/新加坡　SPV）“匿名”在东南亚新建数据中心园区，本地实体不显示中资身份，但实际运营、客户、资金回流被中国主体控制。“影子”指其在并购审批与媒体公开层面”无中国标签”，但在算力供给与控制权上是绿地级的中国延伸。

运作机制：- **架构**：典型三层结构——开曼/BVI 控股公司 → 新加坡运营 SPV → 东道国本地项目公司（负责拿地、电力、机房）。 - **资金**：以美元基金 + 香港中资银行授信为主，规避中国境外直接投资（ODI）审批的 3 亿美元以上项目限制（部分通过拆分申报）。 - **客户**：在终端使用合同中，租户通常为非中资实体（如新加坡本地科技公司、马来西亚国家级云），但通过 API / GPU 切片服务回流中国母公司或关联方。 - **典型案例**： - **Bridge Data Centres**（马来西亚柔佛）——前身系秦淮数据

（2021 年被 Blackstone 私有化后改组）海外业务，2024 年宣布在柔佛依斯干达公主城扩建 150 MW 数据中心园区。其公开身份为 Blackstone/Bain 主导，但 IDC 行业报告与新加坡信通院多份白皮书均指出其中国基因。 - **DayOne Data Centers**——脱胎于万国数据（GDS）海外业务，2024 年在柔佛启动一期 360 MW 项目，号称”亚洲最大单体数据中心园区之一”。万国数据已对外披露其”出海平台”身份。 - **中资二级承包商**：Prisma Data Centers（背景关联深圳易信科技）、YTL 数据中心（与中科曙光存在服务器供应合作）等。

合规风险： - 中资”穿透”问题：东道国监管者（特别是新加坡 MAS）已对”最终受益人”披露收紧，但 BVI/开曼壳的”穿透”难度高。 - 出口管制”长臂”风险：BIS 于 2023 年 10 月、2024 年 12 月扩大 FDPR，明确”中国母公司 + 50% 以上股权海外子公司”采购受管制物项需许可证，**影子绿地如被视为”中国关联实体”，即落入许可证要求**。

为何”成立”：该模式是公开报道中规模最大、可识别性最强的一类。**验证结论**：DSET 该分类成立，且应进一步细分为”全资影子绿地”与”中资 + 国际资本联合绿地”。

2.2 模式二：合资企业（Joint Venture）

定义：中国 AI/云服务商与东南亚本地资本或第三国资本共建项目公司，公开股权结构，常见比例为 51:49（中方控股）或 40:60（中方少数股权以争取本地注册优惠）。

运作机制： - **典型组合**： - 中方提供芯片、运维与云软件栈； - 东南亚本地方提供土地、电力与本地合规外壳； - 部分项目引入**美国/欧洲战略投资者**作为”白手套”以分散出口管制关注度（如引入 NVIDIA、Microsoft 作为次级股东）。 - **典型案例**： - **阿里云-马来西亚 YTL 合资项目**（2024 年宣布）：阿里云出资 51%，YTL 提供柔佛土地与电力。**事实依据**：阿里云官方公告与 YTL Power 投资者简报可查证。 - **腾讯云-印尼 GoTo 合作**：基于 GoTo 在雅加达的数据中心设施提供 GPU 推理服务（事实依据：腾讯云 2024 年东南亚白皮书）。 - **商汤科技-泰国 Gulf Energy / AIS 合作**：在曼谷边缘节点提供 AI 推理；商汤作为部分港股与”中国部分国有”标签的企业，其东南亚合资被多份智库报告列为关注对象。

合规灰色地带： - “最低规则含量”（de minimis）抗辩：合资公司注册在新加坡/马来西亚，但**美国原产芯片仍受 EAR 管辖**，只要符合”美国原产 + 受管制物项 + 流向受管制方”的任意一条仍需许可； - “白手套”风险：若合资企业仅在纸面上无中资股东、实际运营与客户均由中方主导，**BIS 可援引”知道/应该知道”原则（Know/Know provision）认定违法**。

验证结论：DSET 该分类成立，且 2025 年以来呈现**“三方合资”（中资 + 东南亚 + 美国/欧洲）**的新子类型，以稀释 BIS 关注。

2.3 模式三：机柜共置（Co-location）

定义：中国租赁方在东南亚第三方数据中心租用整排机柜（Cage）或单机柜（Cabinet），按功率密度（kW）与机位（U）计费。第三方数据中心运营商（如 NTT、Equinix、ST Telemedia、YTL、KDDI）负责提供机房、冷却与电力，**GPU 服务器由租赁方自带、合规来源存疑**。

运作机制： - **典型路径**：中方租赁方 → 新加坡/马来西亚本地 IDC → 中国母公司远程 SSH/API/SSH Tunnel 接入 → 任务训练完成 → 模型权重回传中国境内。 - **典型案例**： - 2025 年 8 月 2 日美国

司法部逮捕的两名新加坡 H100 转售案嫌疑人：被告以”客户 A”身份向新加坡合法进口商采购 H100 服务器，要求运至”东南亚（新加坡/马来西亚/泰国）“收货企业，**实际付款来自中国大陆与香港第三方**，部分货物被转运至中国境内（事实依据：当事律所”威翰德”案件整理与《财经》报道）。 - **DeepSeek 案**（2025 年 1—2 月）：BIS 与 FBI 调查 DeepSeek 是否通过新加坡中间商获取受管制英伟达芯片，最终用途仍指向中国境内训练（事实依据：路透社、彭博社 2025 年 1 月 31 日报道，TMTPost 跟进）。 - **月之暗面 Kimi K3 案**（2026 年 7 月 22 日起）：白宫科技政策办公室主任克拉齐奥斯（Michael Kratsios）在 X 平台指控月之暗面通过泰国境内的 NVIDIA GB300 集群训练 2.8 万亿参数模型，并对 Anthropic 进行”大规模模型蒸馏”，触发 BIS 对东南亚算力租赁的系统性审查（事实依据：彭博社 2026 年 8 月 7 日报道，中信网与《财经》同步报道）。

合规灰色地带： - 服务器”租赁” vs “购买”的边界模糊：跨境租赁不构成 EAR 项下的”出口”，但**承租方自带服务器**已构成实物出口； - **机柜物理位置是否被认定为”受 EAR 管辖地点”**：BIS 已表明，**美国原产物项即使在第三国，仍受 EAR 长臂管辖**； - **付款路径**：通过香港或新加坡壳公司支付，本身不违法，但若结合服务器转运至中国境内，则构成”转售规避”（redflag diversion）。

验证结论：DSET 该分类成立，且是当前 BIS 执法力度最大的环节。2025—2026 年 BIS 已对 10 余家东南亚中间商展开出口管制调查，凸显该模式的”可识别—高风险”特征。

2.4 模式四：混合云架构（Hybrid Cloud Architecture）

定义：中国主体在境内保留合规推理集群（使用 H20、A30 等），将高强度训练任务调度至海外 AWS、Azure、Google Cloud 或东南亚本地云；通过统一身份/网络（VPN / SD-WAN / Application Gateway）实现”境内推理 + 海外训练”的无缝调度。

运作机制： - **典型架构**： - 境内：自有或租赁 H20 推理集群； - 境外：AWS 东京 / 新加坡 / 雅加达区部署 H100 / H200 训练集群； - 网络：跨国专线 + 数据驻留控制； - 模型：训练在海外完成 → 权重通过加密通道回传 → 推理在境内完成。 - **典型案例**： - **阿里 Qwen 系列**：据《金融时报》2025 年 11 月报道（经 Tom’s Hardware、SCMP 转载），阿里在新加坡和马来西亚的数据中心训练最新 Qwen 模型，使用未受管制的 H100 / H200 集群，**模型权重最终供境内业务使用**。 - **字节豆包（Doubao）系列**：同期报道显示字节在马来西亚柔佛部署训练节点，回应 H20 自 2025 年 4 月起被禁售后的算力缺口。 - **DeepSeek V3 / R1**：使用 H800（2023 年 10 月前合规）训练；2025 年后其新一代模型据报道依赖新加坡与马来西亚混合云。 - **“外训内推”**（训练在外、推理在内）：已是中国 AI 行业公开的折中选择（事实依据：《财经》2026 年 8 月对多位数据中心从业人士的访谈）。

合规灰色地带： - **云租赁是否受 EAR 约束**：当前 BIS 仅在征求意见阶段评估是否将”使用受管制芯片提供的算力服务”纳入许可证要求；若该规则落地，将颠覆当前所有混合云架构（事实依据：彭博社、路透社 2026 年 8 月报道）。 - **数据出境合规**：中国《数据出境安全评估办法》《个人信息出境标准合同办法》要求重要数据与个人信息出境需评估/标准合同；训练数据出境本身存在合规双轨问题（同时受中美双重监管）。 - **“实体清单”扩展**：已被列入实体清单的中国主体（如某些 AI 公司）若直接租赁海外算力，已构成 EAR §744.11 下的”特别管控”；BIS 已明确，**实体清单主体的”非清单化”海外子公司亦受连带管辖**。

验证结论：DSET 该分类成立，且是 2026 年增长最快、政策风险最不确定的一类。该模式的特点是”事实算力回流”但”物理合规空白”。

2.5 四模式的横向比较

维度	影子绿地	合资企业	机柜共置	混合云
资本主导	中国境外 SPV	中外联合	第三方 IDC	海外云厂
中资能见度	低（穿透难）	中（公开股权）	中低（合同方）	低（API 客户）
可控算力量级	100 MW+ 园区	10—100 MW	1—10 MW 单点	弹性无限
BIS 识别难度	高	中	低—中	高
典型合规风险	FDPR 穿透	长臂管辖	走私与转售	算力服务新规
典型国家	马来西亚柔佛	马来西亚、印尼	新加坡、泰国	全球（新加坡为主）

第三部分：DSET 框架之外的补充模式

DSET 四分类侧重”部署结构”，但从算力实际回流至中国主体的全链路看，存在至少四类被忽视的补充模式：

3.1 模式五：壳公司租赁（Shell-Company Leasing）

逻辑：中国主体在第三国（新加坡、香港、BVI）设立单一目的 SPV，以非中资股东、代持董事形式规避”中国关联实体”判定，再以该 SPV 名义向云厂商/IDC 租用算力；算力最终供中资母公司或其客户使用。

关键证据：2025 年新加坡 H100 转售案揭示——客户 A 通过”香港第三方公司付款 + 东南亚收货 + 实际控制人中国籍”的组合，完成数百张 H100 的流转。新加坡出口商在 BIS 调查中提供了充分”尽职调查”证据而免于起诉，但客户 A 的实控人被美国逮捕（事实依据：威翰德律所案例研究，2025 年）。

合规风险：违反 EAR §764（虚假陈述与重大遗漏）；亦可能触发反洗钱（AML）与反欺诈条款。

3.2 模式六：API 调用与模型蒸馏回传（API Inference & Distillation Backflow）

逻辑：中国 AI 团队通过 OpenAI API、Anthropic API（早期）、或第三方代理 API（部署在东南亚算力上）批量调用顶级模型生成高质量合成数据/标签，用于蒸馏出”学生模型”在中国境内训练；此即克拉齐奥斯指控月之暗面对 Anthropic 实施”大规模蒸馏”的机制。

合规风险： - 模型蒸馏本身不违法，但**通过盗用凭证、未授权访问获取的算力结果用于训练**，可能触发《计算机欺诈与滥用法》（CFAA）与合同违约； - API 提供方通常以”禁止用于训练竞争模型”的 ToS 加以限制，但**跨境 API 调用的执法取证极难**； - 中国”生成式 AI 服务管理暂行办法”亦禁止使用未经授权的境外模型能力训练境内模型，构成双向监管漏洞。

典型证据：2025 年 Anthropic 报告显示其观察到来自受制裁地区的异常 API 调用量激增；2026 年 7 月美国白宫相关指控可视为该模式的政策化呈现。

3.3 模式七：设备拆解回流与”芯片再制造”（Teardown & Re-entry）

逻辑：受管制服务器在境外数据中心使用一段时间后，以”废旧 IT 资产”或”二手设备”名义拆解，单卡 H100/H200 GPU 经香港、越南或老挝陆路走私入境，再以”工业主板”“显卡”等品名重新报关入境。

合规风险：违反 EAR §734（出口管制项目清单）、§736（一般禁令），且构成走私罪（《海关法》《对外贸易法》）；中国海关”商品归类”漏洞使该模式具备灰色通道。

证据：路透社 2025 年 1 月对马来西亚、新加坡、阿联酋走私路径的报道；BIS 2025 年 6 月对马来西亚柔佛某废金属回收商的出口管制处罚。

3.4 模式八：加密算力市场与”算力暗网”（Encrypted Compute Markets）

逻辑：去中心化 GPU 算力市场（Render Network、Akash、io.net 等）通过区块链撮合供需，部分节点位于东南亚；中国 AI 实验室通过加密货币结算租用零散算力，规避美元体系下的 KYC 审查。

合规风险：违反 EAR 间接管控的可能性；亦可能触发反洗钱与反恐怖融资（CTF）义务。

证据：2024—2025 年多份区块链安全公司报告显示，东南亚是 io.net、Render 网络的重要算力节点供应区；具体交易规模缺乏权威统计，**为推测性结论**。

3.5 补充模式汇总

DSET 四分类与补充四模式共同构成”8 模式矩阵”。需要指出的是，现实部署往往是多种模式的嵌套（如”影子绿地 + 机柜共置 + 混合云调度”），单一模式极少独立运作。

第四部分：区域案例与监管环境比较

4.1 马来西亚（柔佛州）：影子绿地与合资的主战场

监管环境： - 马来西亚投资发展局（MIDA）对数据中心提供 5 年所得税豁免、进口设备关税豁免； - 2024 年 6 月起，马来西亚宣布暂停新建数据中心审批（moratorium），2025 年改为”暂停—审查—有条件放开”三阶段； - 马来西亚《2010 年个人数据保护法》（PDPA）与数据本地化要求相对宽松，但与美国缺乏引渡条约，**BIS 域外执法依赖马来西亚皇家警察与 MCMC 配合**。

代表性案例： - 柔佛 52 座数据中心园区，3 成具有中资背景； - YTL + 阿里云合资（柔佛）； - Bridge Data Centres / DayOne 园区集群。

与本地监管关系：柔佛州政府从”地缘红利”角度对中资高度开放；但联邦层面与新加坡 MAS 数据共享机制可能传导合规压力。**推测**：2026—2027 年马来西亚可能效仿新加坡引入”战略数据中心”审查机制，要求披露最终受益人。

4.2 新加坡：机柜共置与云租的金融中心

监管环境： - 新加坡《个人数据保护法》（PDPA）、《网络安全法》（CSA）与《刑事法典》对数据驻留与犯罪管辖严密； - 新加坡海关与 MAS 对高价值 IT 设备出口实行出口前许可证制度； - 2025 年 8 月 BIS 与新加坡执法部门联合行动逮捕 2 名 H100 转售嫌疑人，是**首次美国与新加坡在算力转售案件上的成功执法合作**。

代表性案例： - DeepSeek 通过新加坡中间商获取 H100 案（2025 年初调查）； - 阿里、字节在新加坡的混合云训练节点； - 多家中资 AI 创业公司（如月之暗面海外业务）的”对外接口”。

与本地监管关系：新加坡本身是**被利用方**而非共谋方；新加坡政府 2025 年以来明显加强与美国 BIS 合作，新加坡出口管制法令（Strategic Goods Control Act）已用于多起案件。但**新加坡作为金融与云节点枢纽的地位，意味着完全切断将造成区域产业链重大冲击**，存在政策博弈空间。

4.3 泰国（曼谷、春武里）：模型蒸馏与”安静的训练场”

监管环境： - 泰国投资促进委员会（BOI）对数据中心提供 8 年免税； - 泰国《计算机犯罪法》（CCA）与个人数据保护法（PDPA）相对宽松； - 泰国与美国有引渡条约，但 2024 年以来泰美引渡执行趋紧。

代表性案例：克拉齐奥斯 2026 年 7 月指控月之暗面使用泰国境内 NVIDIA GB300 集群训练 Kimi K3。**事实依据**：白宫科技政策办公室公开声明，尚未有 BIS 正式立案公告，**仍处调查阶段**。

与本地监管关系：泰国是中国 AI 企业的”安静备选”——成本较新加坡低、与美国引渡合作相对低敏感、电力供应充足。但克拉齐奥斯公开点名后，泰国 BOI 与数字经济促进局（DEPA）的态度将成为关键变量。

4.4 印度尼西亚（雅加达、巴淡岛）：地热与”主权云”

监管环境：- 印尼《电子信息与交易法》（UU ITE）、《个人数据保护法》（PDP Law）相对严格； - 印尼通信部（KOMINFO）推动”主权数据中心”建设，要求外资数据中心与本地合资； - 2024 年印尼总统普拉博沃表态支持中印 AI 合作，引发美方关注。

代表性案例：腾讯云与 GoTo 合作；阿里云雅加达区；中国电子（CEC）参与印尼智慧城市项目。**算力直接回流中国的公开证据有限**，多为本地推理服务。

4.5 柬埔寨（金边、西哈努克港）：低门槛 + 高风险

监管环境：- 柬埔寨数据保护立法几乎空白； - 西哈努克港是中资”一带一路”项目密集区，存在大量灰色金融与电信业务； - **2024 年美国 OFAC 对部分西哈努克港中资实体实施制裁**。

代表性案例：公开报道有限；**推测**存在”地下数据中心”用于加密算力市场与小额 GPU 走私中转。

4.6 菲律宾（苏比克湾、马尼拉）：美军旧基地与中美博弈前沿

监管环境：- 苏比克湾曾是美军基地，遗留大量光纤、电力基础设施； - 菲律宾《数据隐私法》（DPA）2012 年通过； - 菲律宾是 2023 年美日菲澳”四方”数据合作的重要节点。

代表性案例：公开报道较少；但苏比克湾成为部分美资 Hyperscaler（Microsoft、Google）新建节点区，**与中国离岸算力形成物理隔离带**。

4.7 区域对比小结

国家/地区	主要模式	与美合作紧密度	中资能见度	政策不确定性
马来西亚（柔佛）	影子绿地、合资	中	高	中（2025 年起审查趋紧）
新加坡	机柜共置、混合云	高	中	低（合作稳定）
泰国	模型蒸馏、混合云	中	中高	中高（被点名后）
印度尼西亚	合资、本地推理	中低	中	中
柬埔寨	灰色中转	低	高（半地下）	高
菲律宾	美资占主导	高	低	低

第五部分：出口管制规避机制与合规灰色地带

5.1 美国出口管制体系的演进

EAR 三轮强化：1. **2022 年 10 月 ACR**：引入”总算力—带宽”阈值；FDPR 扩张； 2. **2023 年 10 月**：A800/H800 列入清单；FDPR 进一步覆盖 28 类设备；新增 7 家中国 AI 实体； 3. **2024 年 12 月**：总算力阈值收紧；HBM、HBM3e 单独管制；新增 24 家中国实体； 4. **2025 年 1 月 AI Diffusion Rule**：三国分级制；2025 年 5 月实质废止但部分条款留存。

算力租赁执法的新阶段：2026 年 8 月 BIS 启动对东南亚算力租赁的系统性审查，标志管制逻辑从”芯片—硬件”延伸到”算力—服务”。

5.2 当前 EAR 的盲区

1. **“实体货物”前提**：EAR §734 将”出口”定义为”实际或视同的物品跨境流转”，远程算力服务不构成”出口”。
2. **“最低规则含量”（de minimis）**：美国原产成分占整体 25% 以下即可豁免；**远程算力服务无”产品”，因此无适用基础**。
3. **“最终用户”审查**：EAR 要求对”知道或应该知道”最终用户身份进行审查；**API 调用模式下，最终用户难以被准确识别**。
4. **“外国直接产品规则”（FDPR）**：仅适用于实体产品，不适用于服务。

5.3 BIS 算力租赁执法展望

基于彭博社与路透社 2026 年 8 月的报道，BIS 可能采取的措施包括： - **将算力服务纳入许可证要求**（征求意见阶段）； - **要求云厂商承担最终用户审查义务**（穿透审查）； - **对受控芯片的”使用”实施追溯**（使用即受管制）； - **扩大 EAR §744 的”特别管控”清单**，将受管制云服务供应商纳入。

实施难点： - 云服务的全球分布式特性使得”美国云厂商 vs 当地云厂商”边界模糊； - 域外适用与主权原则冲突，可能被 WTO 或双边引渡协议约束； - 中国《阻断外国法律不当域外适用办法》（2021）已为对等措施提供国内法依据。

5.4 中国合规灰色地带

1. **《数据出境安全评估办法》**：训练数据出境需评估；模型权重出境暂无明确规则；
2. **《反外国制裁法》**：为中国主体拒绝配合 BIS 调查提供潜在抗辩；
3. **“最终用户声明”（EUC）**：中国云厂商常以 ECP（End Customer Profile）替代 EUC，规避合规深度；
4. **跨境 VPN/SD-WAN 灰色使用**：技术上完全可能，但需配套《计算机信息网络国际联网管理暂行规定》评估。

5.5 合规风险分级矩阵

行为	EAR 风险等级	中国合规风险	第三方监管风险
海外云租赁训练	中—高（新规出台后）	中（数据出境）	高（BIS 审查）
壳公司租赁	高（虚假陈述）	低	中（AML）
模型蒸馏回传	中（ToS 违约）	中（暂行办法）	中
设备拆解回流	极高（走私）	高（走私罪）	中
加密算力市场	中（AML/CTF）	中	高（监管不确定）

第六部分：影响评估

6.1 对区域算力生态的影响

正面： - 东南亚数据中心市场快速扩张，2025—2030 年累计投资规模预计 1500—2000 亿美元（事实依据：JLL、Cushman & Wakefield 报告）； - 创造就业、提升本地数字基础设施； - 加速东南亚国家”AI 主权”能力建设。

负面： - 区域市场”中国中心化”加剧，新加坡、柔佛等节点可能成为中美博弈前沿； - 国际资本（美国 Hyperscaler）对中资集中区”避而远之”，形成事实上的双轨； - 当地法律与监管能力滞后，出现”监管俘获”风险。

6.2 对国家安全的影响

美国侧： - 出口管制政策有效性受损，可能触发更激进的管制（如算力服务许可证、SDN 制裁）； - AI 领域对华技术领先差距收窄，**DeepSeek V3 / R1 案例被部分美国国会议员称为”斯普特尼克时刻”**； - 半导体产业游说团体（如 SIA）压力增大，要求进一步扩张管制。

中国侧： - 短期获得算力补充，缓解训练与推理压力； - 中长期加速国产替代——华为昇腾、寒武纪、海光、摩尔线程等的需求被强制扩大； - 自主 AI 软件栈（MindSpore、CANN、DeepSeek 自身框架）迭代加速。

东南亚侧： - 新加坡、马来西亚陷入”两难”——既不愿失去中资投资，又担忧美国制裁； - 泰国、印尼倾向于”等距外交”，但实际越来越难以中立； - 柬埔寨、老挝、缅甸可能成为”灰色中转”重灾区。

6.3 对全球科技竞争的影响

1. **AI 算力”双轨化”**：形成”美主导的合规算力 + 中主导的离岸算力”两个并行体系；
2. **供应链”友岸外包”加速**：日本、韩国、台湾、印度在中美之间面临”选边”压力；
3. **国际规则碎片化**：WTO、OECD、G20 等多边机制在 AI 治理上达成共识的可能性下降；
4. **“技术主权”话语扩散**：欧盟”AI Act”、东南亚”AI 主权框架”可能与中美的政策形成三角博弈。

6.4 对企业层面的影响

- **中国 AI 头部企业**：短期受益，长期面临 BIS 长臂扩张风险；
- **东南亚本地云厂商**：在合规与营收之间艰难平衡；
- **美国云厂商**：可能被迫退出东南亚中资集中区（避险）；
- **NVIDIA 等芯片厂商**：游说放松管制的声音可能加大，但同时面临”主动配合管制”与”被 BIS 长臂”的二选一；
- **第三国中间商**：合规要求陡升，部分可能退出业务。

第七部分：结论与研究局限

7.1 主要结论

1. **DSET 四分类成立且有效**，但应增加至少四类补充模式（壳公司租赁、API 蒸馏回传、设备拆解回流、加密算力市场）以全面反映现实。
2. **柔佛-新加坡走廊**是”黑色算力网络”的物理与法律心脏地带，其形成是地缘、能源、法律、合规四要素叠加的必然结果。
3. **2026 年 8 月 BIS 对算力租赁的审查**，标志管制逻辑从”卡硬件”升级为”卡算力”，但**短期内难以完全封堵**，因 EAR 体系以”实体货物跨境流转”为核心抓手。
4. **多层风险切割**（中国母公司 → 第三国 SPV → 东南亚本地实体 → 最终客户）是当前规避的核心架构，使责任归属与举证高度复杂化。
5. **“黑色算力网络”已对全球 AI 治理构成系统性挑战**：出口管制、国家安全、数字主权、产业链弹性四重维度同时承压。

7.2 政策建议

对美方： - 推动 EAR 修订，将”使用受管制芯片提供的算力服务”纳入许可证要求； - 与东南亚国家建立”算力出口管制联合工作组”； - 对云厂商施加最终用户审查义务，建立”穿透式”审计机制。

对东南亚国家：- 引入”战略数据中心”审查机制，要求披露最终受益人与算力用途；- 强化本地数据保护立法，避免成为”算力避税港”；- 与 BIS、MAS 等国际监管机构建立常态对话。

对中方：- 完善《数据出境安全评估办法》对训练数据与模型权重的适用范围；- 加速国产 AI 芯片与软件栈迭代，降低对受管制算力的依赖；- 推动建立”中国版 AI 算力白名单”机制。

对企业：- 强化出口管制合规体系，建立”出口管制官”独立岗位；- 对混合云架构进行合规审计，避免”远程算力回流”被认定为违反 EAR；- 与专业出口管制律师团队建立长期合作。

7.3 研究局限

1. **资料限制**：BIS 内部文件、SEC 调查档案、企业内部财务数据未能获取，本报告基于公开报道与第三方研究；
2. **时点限制**：报告写作时点为 2026 年 8 月下旬，BIS 算力租赁新规仍处于征求意见阶段，最终条款可能与当前推测不同；
3. **案例完整度**：月之暗面泰国算力案等仍在调查过程中，最终事实认定需等待官方公告；
4. **量化数据缺乏**：八类模式各自的算力量级、企业覆盖率、金额规模尚缺乏系统统计，**部分结论为定性推测**；
5. **法律域外适用争议**：BIS 算力服务新规可能违反 WTO 服务贸易总协定（GATS）与双边引渡协议，本报告未深入展开法律论证；
6. **中资行为动机复杂化**：本研究主要从”规避管制”视角解释中资行为，但实际决策可能混合商业动机（如新加坡更好的网络延迟、马来西亚更低的运营成本），**单一归因存在偏误风险**。

7.4 后续研究方向

- **算力贸易经济学**：东南亚离岸算力的真实价格、产能利用率、隐性补贴；
- **执法案例数据库**：BIS、SEC、司法部公开案例的汇编与模式提取；
- **中国国产替代节奏**：昇腾、寒武纪、海光等芯片的实际产能与软件栈成熟度；
- **东南亚本土监管演化**：马来西亚”战略数据中心”立法、新加坡 ECDA 制度等。

附录：关键事实清单（精选）

#	事实陈述	来源/依据	标注
1	柔佛州 2025 Q2 数据中心获批投资 1644.5 亿令吉，占马来西亚运营 IT 容量 78.6%	百度财经 2026 年文章引用马来西亚官方数据	事实陈述
2	Bridge Data Centres 与 DayOne 均具中资背景（前身秦淮数据、万国数据）	百度财经文章，IDC 行业报告	事实陈述
3	2025 年 8 月 2 日美国逮捕两名新加坡 H100 转售案嫌疑人	威翰德律所案例研究	事实陈述
4	2025 年 1 月 BIS 调查 DeepSeek 通过新加坡中间商获取英伟达芯片	路透社、彭博社报道	事实陈述
5	2026 年 7 月克拉齐奥斯指控月之暗面在泰国使用 GB300 训练 Kimi K3	白宫科技政策办公室公开声明	事实陈述
6	2026 年 8 月 7 日 BIS 启动东南亚算力租赁审查	彭博社、路透社、《财经》报道	事实陈述
7	阿里 Qwen、字节豆包据报道在马来西亚/新加坡训练	金融时报 2025 年 11 月	事实陈述
8	NVIDIA 推出 A800、H800、H20 多代降规版	NVIDIA 官方公告	事实陈述
9	2025 年 1 月 AI Diffusion Rule 出台、5 月实质废止	BIS 官方公告	事实陈述
10	“外训内推”为中国 AI 行业公开选择	《财经》2026 年 8 月访谈	事实陈述

参考文献（精选，公开可查）

1. U.S. Bureau of Industry and Security. “Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections.” Federal Register, October 7, 2022.
2. U.S. Bureau of Industry and Security. “Export Controls on Semiconductor Manufacturing Items.” Federal Register, October 17, 2023.
3. U.S. Bureau of Industry and Security. “Framework for Artificial Intelligence Diffusion.” Federal Register, January 15, 2025.
4. Reuters, “US Investigates Whether DeepSeek Bypassed Export Curbs,” January 31, 2025.
5. Bloomberg, “US Probes China Firms’ Use of Overseas Nvidia Chips,” August 7, 2026.
6. Financial Times, “Alibaba and ByteDance Train AI Models in Southeast Asia,” November 2025.
7. Tom’s Hardware, “Chinese AI Giants Bypass US Chip Curbs,” November 2025.
8. 财经，《中国公司使用东南亚算力风险正在抬升》，2026 年 8 月。
9. 百度财经，《东南亚离岸算力》，2026 年。
10. 威翰德律所，《算力之争——新加坡 H100 转售案》，2025 年。
11. DSET（Digital Safety and Emerging Technologies），相关区域 AI 数据中心报告（具体期数待核）。
12. Anthropic 公司 2025 年 API 滥用观察报告（待权威确认）。
13. NVIDIA 投资者简报，2025—2026 各季度。
14. Cushman & Wakefield、JLL《亚太数据中心报告》，2025—2026。
15. SCMP, “ByteDance, Alibaba, SenseTime lead generative AI infrastructure services market in China,” 2025。

> **数据声明**：本报告引用的所有事实均来自上述公开来源；推断与推测部分已在正文以”推测”“可能”“待证”等字样明示。研究结论仅代表作者基于公开资料的整理与分析，不构成对特定企业或国家的指控。

报告结束。