

看世界

当 AI“吞噬”内存

新买的笔记本电脑变贵了，手机厂商的旗舰机型也涨价了——这背后的主要推手，是由人工智能（AI）驱动的存储芯片资源争夺战，而你我感受到的价格变化，不过是这场“电子设备战争”最末端的代价。

全球存储芯片市场正在上演“冰火两重天”：一方面，韩国半导体芯片制造企业 SK 海力士通过美国存托股份（ADS）发行募资 265 亿美元，成为外国企业在美国规模最大的首次公开募股（IPO）；三星电子单季营业利润暴增 18 倍，科技巨头们正加紧筹资扩大存储芯片生产。另一方面，苹果公司却因缺“芯”被迫将多个产品价格调涨，联想、戴尔也跟进涨价。生产端热火朝天，消费端却无“芯”可用——供应明明在扩大，为什么还是填不上需求的窟窿？

要解开这个谜团，我们需要先认识一下幕后主角，搞清楚存储芯片的 3 种基本类型：动态随机存取存储器（DRAM）、闪存（NAND），以及高带宽内存（HBM）。

打一个通俗的比方：DRAM 好比设备的“工作台”，负责临时处理手头的数据；NAND 则是“文件柜”，手机里的照片、电脑里的文档都靠它长期保存。这两类芯片，主要服务我们常用的手机、电脑和平板。

HBM 可以看作是 DRAM 的超级加强版。它把多个 DRAM 芯片垂直堆叠在一起，数据吞吐速度极快。所以，大多数情况下，它不会直接服务普通消费者，而是服务 AI 芯片。如果说图形处理器（GPU）是 AI 的大脑，那么 HBM 就是给大脑输送数据的高速公路——路不够宽、不够快，再聪明的大脑也只能闲着。

那么，AI 究竟是怎样搅动这场生产巨变的？生产 AI 专用内存所消耗的晶圆产能，正在以不可逆的方式吞噬手机和电脑所需通用内存的产能。

引爆点来自近年来生成式 AI 的爆发。训练一个千亿参数的大模型，需要成千上万颗 GPU 昼夜不停地运转，而每一颗先进 GPU，都必须搭配数颗 HBM 作为“近身数据仓库”。这一需求爆发有多猛烈？到 2026 年，全球 HBM 市场规模预计突破 600 亿美元。SK 海力士和美光已公开宣布 2026 年 HBM 产能全部售罄，客户甚至提前锁定了 2027 年乃至 2028 年的供应量。

在极度紧缺的卖方市场下，HBM 价格持续飙升。据互联网数据资讯网 DigiTimes 报告，下一代 HBM4 在 2026 年下半年的市场单价约为 2 美元/GB（千兆字节），到 2027 年有望涨至 4 美元/GB 至 5 美元/GB，甚至更高。摩根大通日前发布研报预计，2027 年全球 HBM 综合平均售价将同比上涨 54%，2028 年进一步上涨 25%。正是这巨大的利润，促使三星、SK 海力士和美光等主要存储原厂不约而同地紧急“换轨”——将原本用于生产手机和电脑内存的先进产能，大批量切换给了 HBM。

更要命的是，HBM 还天生“吃”产能：它的芯片面积是同等容量普通内存的 2 倍到 3 倍，这意味着，在有限的晶圆产能下，每为 AI 生产 1GB 的 HBM，就必须放弃大约 3GB 通用内存的产出。这不是简单的产能腾挪，而是一场由超额利润驱动的、不可逆的产能挤出。

换言之，对于当下的全球产能而言，AI 算力每往前迈一步，你我手里的笔记本、手机就可能贵上一分。

眼下，全球约七成的先进存储产能已被 AI 数据中心吞噬，手机、电脑等消费电子，只能争抢剩下的三成。供需极不平衡，正沿着产业链层层传导：仅今年上半年，通用内存合约价就几近翻倍，闪存涨幅也超过五成。多家投行测算，今年各类存储芯片的供需缺口普遍超过 4%，齐刷刷创下 10 余年来的新高。

消费电子终端是涨价大潮真正的受害者。存储芯片占一部智能手机整机物料成本的比例，已从以往的 10% 至 15% 区间飙升到 30% 以上，部分大存储旗舰机型甚至逼近 50%。单颗 12GB 的手机内存采购价从 200 元涨至近 600 元，1TB 的闪存芯片也从 200 元出头飙升至 600 元。难怪苹果公司会将眼下的供需紧张形容为“百年一遇的洪灾”。

存储芯片行业向来有很强的周期性。它是半导体行业中周期性最强的品类，产品高度标准化、可替代性强，带有类似大宗商品的属性，价格对供需变化极为敏感。过去 10 多年间，行业每三四年便要经历一轮价格起落，几乎每次暴涨都源于短期错配，每次暴跌都源于厂商同步扩产。然而，这轮周期与以往截然不同，其特殊性深深植根于 AI 带来的结构性撕裂。

首先，需求性质变了。过去周期的驱动力是消费电子换机潮和容量升级，比如智能手机爆发式增长、安卓手机内存容量提升等，触及需求天花板后价格自会回落。这次的核心引擎却是 AI 训练与推理，科技巨头将其视为未来 10 年最重要的战略竞赛，宁愿压缩短期利润也要保住算力投入。HBM 订单由此呈现出“类基础设施”的刚性——只要大模型还在变大、AI 应用还在扩张，对它的强烈需求就难以消退。

其次，产能弹性消失了。传统内存扩产后能较快转化为供给，产线还能在不同品类间灵活调配。但 HBM 的生产极度依赖先进封装，良品率爬坡艰难。一座新建的专用晶圆厂从动工到量产至少需要两年，投产后的产线几乎被不可逆地锁定，哪怕需求有变，也无法轻易转回生产手机或电脑内存。换言之，供给正在变得“又硬又慢”，基本丧失了调节周期波动的能力。

再次，定价机制扭曲了。目前，全球主要存储原厂未来一两年的 HBM 产能，均被云厂商和终端品牌以多年长期协议的形式提前全额锁定，现货市场几乎无货可放。这意味着，合约价格失去了短期调节的余地，整个市场的价格发现功能遭到破坏。市场由此分裂成“两个平行世界”：AI 专用的高性能内存价格高悬，持续赚取超额利润；消费级内存则因供给塌陷而被迫跟涨，涨价的压力几乎单向传导到普通消费者的肩上。

目前来看，这种结构性撕裂还在加剧——一场史无前例的扩产竞赛已然打响，但新

增产能几乎全部指向 HBM 和服务器 DRAM，而非手机、电脑所需的消费级内存。三星、SK 海力士和美光三大存储原厂 2026 年合计资本支出超过 500 亿美元，其中三星一家就投入超 110 万亿韩元。然而，由于 HBM 对晶圆产能的挤占效应，消费级 DRAM 和 NAND 的供给非但未获缓解，反而可能进一步收紧。

如今，存储行业正站在一个新的十字路口。当所有原厂都在全力扩产，当一座座新建的晶圆厂在 2027 年后陆续投产，这场由 AI 驱动的“超级周期”，究竟会成为存储行业有史以来最长的一次繁荣，还是再次沦为“周期从未消失”的残酷注脚？又或者，出现“第三种剧本”——HBM 和消费级内存从此分道扬镳，一个在 AI 的推动下持续沸腾，另一个在产能的长期压抑下彻底告别廉价时代？关于这些问题，业界至今也没讨论出一个明确的结论。未来已来，变数依旧。

在《生物多样性公约》第十七次缔约方大会（COP17）密集的议程间隙，记者来到位于举办地亚美尼亚首都埃里温以西约 17 公里处的埃奇米阿津主教座堂。耳畔激烈的讨论声渐远，取而代之的是清脆婉转的鸟鸣与风吹落叶的轻响。

作为亚美尼亚世界文化遗产的核心区域，埃奇米阿津主教座堂经历了漫长的时代变迁。本地红褐色凝灰岩构筑的庄严古建，以及历经千年风雨仍静默伫立的石刻，承载着亚美尼亚乃至整个南高加索地区的历史人文脉络，诉说着人与自然和谐共生的古老智慧。

秋日浸染的大教堂院落内层次丰盈，枝叶金黄与绯红的渐变，花木在这里错落舒展。教堂穹顶上，鸽子时而盘旋飞翔；斑驳古墙的青苔上，蜗牛在慢慢爬行；回廊转角处，小猫倏然穿梭；阳光铺洒的草坪上，小狗酣然入睡……一幅古韵生动的画卷经年累月仍不改其色。

同样的院落，这世上还有很多。它们不仅是建筑所在地，还是微缩但并不简单的生物圈。墙角野草之间、层层落叶之下，蚯蚓翻动土层；昆虫在枯枝间觅食繁育，麻雀啄食虫卵草籽……这些串联起的细碎生态链让建筑空间有了呼吸，庭院减少水土流失，并调节着局部的微气候。

也许不少人会以为，生态保护是针对濒危动植物的专项守护，是偏远自然保护区的专属课题。但埃奇米阿津主教座堂里的美好景象很容易让人明白，人与自然和谐共生的答案，往往藏在日常生活的细微处。生态保护的核心，不止于守护稀缺的濒危物种，还在于珍视身边触手可及的自然生灵与生境。平凡的草木鱼虫皆是蓝色星球的奇迹，共同构筑地球完整的生态链与系统。

本次 COP17 的核心议程是全面盘点“昆明—蒙特利尔全球生物多样性框架”的落地成效，查漏补缺，推动全球生态治理从蓝图走向实景。除了聚焦珍稀物种保护、大型生态系统修复等议题，本次大会注重普惠性生态保护、城市生物多样性存续以及人居微生态守护，将保护视野从遥远的自然秘境延伸至城市街巷、庭院等每个角落。

COP17 明确，生物多样性的完整内涵包括地球所有层级、所有类型的生命个体，珍稀物种是生态瑰宝，平凡生灵同样是生态系统不可或缺的组成部分。看似微不足道的生命活动，串联起的是古迹与自然、人文与生态、城市与山野的共生纽带，保障了局部生态的稳定循环，最终汇聚成为全球生态保护的基底。

埃奇米阿津主教座堂庭院内的生物，早已与千年古建融为一体。在这里，生物多样性的课题与答案，变得质朴而清晰——始于看见，尊重和善待。

去看见一片落叶的荣枯，去聆听一声飞鸟的啼鸣，铭记那些消逝物种留下的警示与遗憾……保护生物多样性，不仅是联合国、各国政府、专业人员的任务，也是地球上每个人的责任。

陈俊锋

刘书辰

细微

本版编辑 韩叙 王伊美 编倪梦婷

脑洞

“冷柜变烤箱”的启示

在许多电影里，黑客的工作都与信息有关——要么窃取国家机密，要么窃取商业机密，整个过程体现在屏幕上，就是黑屏上倾泻而下的字符，看起来有如天书。

然而，最近一则真实发生的案件却打破了人们对黑客的刻板印象。10 月 11 日夜至 12 日，法国数家大型零售巨头遭遇空前的黑客网络攻击。数百家大型超市的冷链管理系统突然失去控制，部分设备的定温标准飙升至 50 摄氏度并持续数小时之久，导致冷柜内储存的冰鲜食品解冻乃至腐败，给相关超市造成了巨大损失。

“冷柜变烤箱”仅仅是数字物联时代安全风险的缩影。当前，随着物联网、操作技术与云计算的深度融合，网络与物理世界之间的界限日益模糊，网络威胁已不再局限于数据泄露，而是能够直接跨越虚拟空间，对实体产业造成破坏。

仅就食品产业而言，在数字物联网环境下，任何高度依赖数字监控与自动控制环节，都可能成为黑客攻击的目标。在作物种植阶段，现代化农场广泛应用自动灌溉、水肥一体化及智能喷药系统。一旦控制系统遭受入侵，攻击者可恶意篡改化

肥、农药的配比，导致农作物重金属或毒素超标，甚至直接污染水源。在食品加工阶段，加工工厂高度依赖监控与数据采集系统控制高温灭菌、成分添加配比和烘焙时间。攻击者一旦入侵，可悄无声息地降低灭菌温度，或故意篡改过敏原标注系统，引发严重的食品安全事故。早在 2021 年，全球知名肉类加工商 JBS 就曾遭遇勒索软件攻击，其位于北美和澳大利亚的多处大型屠宰场及加工厂被迫停产数天。在运输仓储阶段，冷链运输车队和智能自动化冷库普遍采用卫星导航与温湿度物联网感应器进行实时监控。若云端调度平台或车载物联终端遭到黑客阻断或数据篡改，货物可能高温下运输数小时却误报温度正常，导致腐败食品误流入市场。

目前，多国已经充分意识到风险，并加紧行动筑牢食品安全防线。

在法律法规层面，欧盟在 2022 年施行的《网络与信息安全指令》中，明确将“食品生产、加工与分销”整体列为重要实体，强制要求大型食品企业建立严密的供应链风险管理机制。美国国土安全部与网络安全和基础设施安全局也将食品与农业部门列

入 16 个国家关键基础设施之一，要求实施高密度的工控安全审计。

在应对机制层面，多国网络安全机构已针对本次事件中暴露出的脆弱性发布紧急指导，对办公网络与生产设备控制网络加强隔离，确保即使办公终端感染勒索病毒，也无法跨网段操控冷柜、消毒炉等关键物理设备。有关指导还强制要求物联网设备出厂禁用统一默认密码，远程管理也必须经过多因素身份验证。

在硬件管理层面，越来越多从事食品安全相关基础设施和关键设备制造的先进企业开始强调，在积极拥抱数字化的同时保留物理安全底线。例如在关键冷库与消毒设备上安装独立的物理温控断路器，一旦温度超过安全阈值，硬件将直接切断电源或启动备用制冷，防止软件指令单点失效导致严重灾难。

“冷柜变烤箱”事件，标志着网络安全威胁已全面渗透人类最基础的生活保障体系。数字物联时代赋予了各产业链供应链极高的效率，但也放大了系统性脆弱点。唯有将网络安全与物理安全深度结合，才能真正筑牢数字时代的安全防线。

梁桐