英伟达：我们的芯片不存监控软件

2025年8月6日凌晨，英伟达通过其官方网站和微信公众号发布长文，标题为NVIDIA芯片不存在后门、终止开关和监控软件，明确否认其芯片存在任何形式的监控软件或后门机制。此声明由英伟达首席安全官大卫雷伯撰写，针对近期关于其H20芯片可能存在安全隐患的争议作出回应。据悉，国家互联网信息办公室于7月31日约谈英伟达，要求其就对华销售的H20算力芯片可能存在的漏洞和后门风险进行说明并提交证明材料。英伟达此次声明不仅是对中国监管机构的回应，也是在全球范围内对其产品安全性的公开澄清。

英伟达在声明中指出，NVIDIA GPU是现代计算的核心，广泛应用于医疗健康、金融、科学研究、自动驾驶和人工智能基础设施等领域。为了降低潜在的误用风险，一些专家和政策制定者曾提出在硬件中设置“终止开关”或内置控件，以便在用户不知情或未经同意的情况下远程禁用芯片。英伟达明确表示，其GPU不存在此类机制，也不支持在芯片中植入任何形式的后门或监控软件。公司认为，硬编码的单点控制会为黑客和敌对势力提供可乘之机，严重威胁全球数字基础设施的稳定性和用户对技术的信任。

英伟达还援引了历史案例美国国家安全局于1993年推出的Clipper芯片项目，以说明后门设计的风险。该项目旨在通过密钥托管系统提供加密功能，同时允许政府访问数据。然而，安全研究人员发现其存在根本性缺陷，可能被恶意方利用，导致系统漏洞。英伟达强调，政府后门的存在会削弱用户对系统安全性的信心，违背网络安全的基本原则。此外，英伟达驳斥了将智能手机的“查找我的手机”或“远程擦除”功能与芯片后门类比的观点，指出这些软件功能由用户控制，而硬件后门是用户无法掌控的永久性缺陷，可能引发严重后果。

英伟达在声明中进一步阐述，其产品安全性通过严格的内部测试、独立验证和全球网络安全标准的遵循来实现。公司遵循“深度防御”原则，通过多重保障措施确保单一漏洞不会导致系统瘫痪。英伟达表示，其三十多年的处理器设计经验表明，故意在芯片中植入后门或终止开关不仅违反法律规定，还会增加安全风险。许多国家和地区的法律明确要求企业修复漏洞，而非制造漏洞。英伟达还提到，当CPU的“Spectre”和“Meltdown”漏洞被发现时，全球业界迅速采取措施消除风险，证明了这一原则的有效性。

此次声明的背景是，英伟达H20芯片作为专为中国市场设计的AI加速器，近期因安全争议备受关注。据报道，美国政府曾于2025年4月将H20芯片列入对华禁售清单，但7月14日，英伟达首席执行官黄仁勋访华期间表示，已获得重新出口H20芯片的许可。黄仁勋强调，中国市场的重要性及其创新活力。然而，安全疑虑并未完全消散，部分美国议员提出要求在出口芯片中加入“追踪定位”功能，而有消息称英伟达的“追踪定位”和“远程关闭”技术已成熟，这加剧了外界对芯片安全的担忧。

英伟达的声明不仅针对监管机构的质询，也意在安抚全球客户和开发者生态。英伟达的CUDA生态系统是其核心竞争力，依赖于全球开发者的信任。一旦安全疑虑动摇这一信任，可能导致开发者转向竞争对手如AMD的ROCm平台，对英伟达的市场地位构成威胁。因此，英伟达在声明中反复强调其对透明、开放软件的支持，以及通过用户同意的诊断和性能监测功能来维护系统安全，而非依赖硬件后门。尽管英伟达多次否认芯片存在后门，但仅靠声明难以完全消除市场疑虑。

未来，英伟达可能需要提供更透明的供应链安全审计报告和可验证的驱动程序，以满足大客户和监管机构的需求。业内人士指出，芯片安全问题不仅是技术挑战，也是商业信任和地缘政治博弈的交汇点。英伟达需在技术、法律和市场信任之间找到平衡，以维持其在全球AI芯片市场的领先地位。嘿，兄弟们，这事儿得好好唠唠！英伟达这波声明够硬气，直接拍胸脯说芯片没后门、没监控，摆明了要怼那些质疑的声音。文章里拿Clipper芯片翻车的事儿当例子，逻辑挺清楚：后门就是给自己挖坑，迟早被黑客玩儿坏。

但说实话，光喊口号没啥说服力，市场和监管那边可不是听你说两句就信了。H20这芯片本来就敏感，夹在中美博弈中间，英伟达想稳住中国市场还得拿出硬核证据，比如公开点审计数据啥的，不然这信任危机可不好破。总的来说，这报道中规中矩，信息量够，但要真想让人买账，还得看英伟达后续咋整。

原文链接：https://hz.one/baijia/英伟达-芯片-监控软件-2508.html