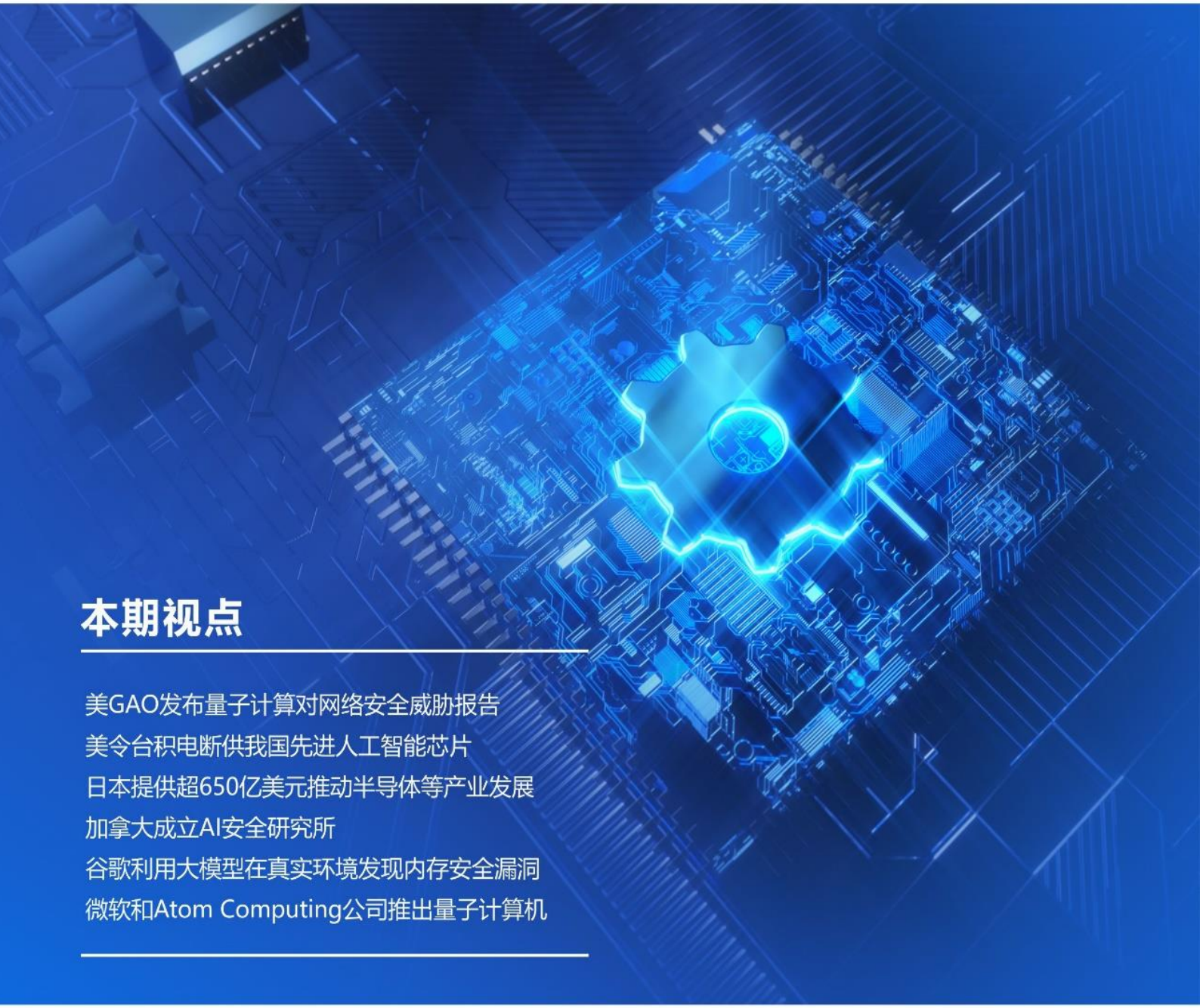
科学研究动态监测快报

信息科技专辑

INFORMATION TECHNOLOGY MONTHLY EXPRESS

2024
第12期
总第252期



本期视点

美GAO发布量子计算对网络安全威胁报告
美令台积电断供我国先进人工智能芯片
日本提供超650亿美元推动半导体等产业发展
加拿大成立AI安全研究所
谷歌利用大模型在真实环境发现内存安全漏洞
微软和Atom Computing公司推出量子计算机

中国科学院成都文献情报中心
CHENGDU LIBRARY AND INFORMATION CENTER, CHINESE ACADEMY OF SCIENCES

目 录

执行主编：唐川 E-mail：tangc@clas.ac.cn
执行编辑：黄茹 E-mail：huangr@clas.ac.cn
出版日期：2024 年 12 月 1 日

重点关注

[量子技术]美 GAO 发布量子计算对网络安全威胁报告

2024年11月21日，美国政府问责局（GAO）发布了一份关于量子计算对网络安全威胁的报告——《网络安全的未来：全面定义量子威胁缓解策略》，指出联邦机构和关键基础设施依赖于加密技术来保护敏感数据和系统。然而，量子计算机的出现可能使现有的加密方法失效，从而威胁到数据的安全性。

联邦机构和国家的关键基础设施，如能源、交通系统、通信和金融服务，都依赖于计算机系统和电子数据来提供基本服务，并处理、维护和报告重要信息。机构和关键基础设施所有者和运营商依靠密码学来保护敏感系统和数据。然而，量子计算机的出现可能会破坏广泛使用的加密方法的安全性。一些专家预测，在未来10到20年内，可能会开发出一种能够破解传统密码学的量子计算机，称为密码学相关量子计算机（CRQC），将使依赖传统密码学的机构和关键基础设施面临严重风险。

量子计算机可比经典计算机更快地解决选定的问题。当前的公钥加密方法依赖于传统计算机，在执行某些计算时需要很长的时间。然而，足够强大的量子计算机可能会将当前公钥加密方法的破解时间缩短到只有几个小时或几天。

量子计算机的能力对密码学构成了重大威胁。具体而言，它们对依赖密码学进行保护的系统和数据的机密性、完整性和可用性构成威胁：对手可以使用量子计算机破解加密方法，并访问联邦机构系统上存储或通信的敏感政府信息；对手可以针对验证信息或数据来源的加密方法，允许他们创建和分发看似合法的虚假通信；对手可以使用量子计算机来破坏关键基础设施。

美国国家量子计算网络安全战略包含三个核心目标：

1、标准化后量子加密方法

制定和推广能够抵抗量子计算机攻击的后量子加密标准，通过严格的评估和选择过程来确定最有效的后量子加密算法，确保这些算法被广泛接受和使用。

2、将联邦系统迁移到后量子加密

将依赖传统加密算法的联邦机构的系统和数据迁移到新的后量子加密算法，以保护其免受量子计算机的威胁。这包括制定详细的迁移计划和时间表，以确保所有联邦系统能够在预定的时间内完成迁移。

3、鼓励所有经济部门为量子威胁做好准备

推动所有经济部门，采用后量子加密算法。这需要联邦机构与私营部门积极合作，并提供指导和支持，以确保所有部门都能够有效地应对量子计算带来的威胁。

联邦机构和关键基础设施所有者和运营商迫切需要过渡到后量子加密。鉴于对手有可能复制敏感数据，并在CRQC可用后访问这些数据，这种转变尤为重要。

联邦机构认识到量子计算的威胁，并采取了一些行动来部分解决这一问题，指定负责全面实施量子国家战略的领导层是战略成功的关键。美国国家网络安全办公室（ONCD）应负责协调和领导美国的量子计算网络安全战略，确保所有相关机构和部门的协调和合作，明确各机构的角色和责任，确保战略的全面实施。此外，美国国家量子计算网络安全战略文档应涵盖明确的战略目标、活动、里程碑和绩效指标。为确保策略的有效实施，还应提供一个明确的资源分配和管理路线图。

黄茹 供稿自

https://www.gao.gov/products/gao-25-107703

原文标题：Future of Cybersecurity:Leadership Needed to Fully Define Quantum Threat Mitigation Strategy

科技政策与科研计划

[信息技术]美国防部发布《5G 专网部署战略》

据美国国防部官网2024年11月12日报道，2024年10月16日，美国国防部发布了《5G专网部署战略》，为美国国防部私有5G网络的部署提供了战略性指导。

任何工作领域内5G网络的部署和管理都需要有效的治理机制，以确保成功实施。为促进和管理私有5G网络在军事设施中的实施和运行，美国国防部不仅须防范部署5G可能会带来的威胁，还应改造未来网络，使其具有弹性。

在军事任务应用中采用私有5G网络需要考虑任务安全性和性能/覆盖范围要求以及采购方式。美国国防部关于军事设施的私有5G网络战略主要包括以下三个目标。

1、确保在军事设施上部署私有5G网络时，充分考虑任务安全性、操作环境、性能要求和采购可行性

逐个点位进行技术和业务案例分析（BCA），以确定是否只能通过私有5G网络才能满足特定的任务、安全性、覆盖范围和性能要求。确保网络基础设施可维护、可扩展，并能够满足特定军事点位不断变化的需求。

2、加速5G的采购、开发和安全部署

（1）缩短交付周期。参阅《5G采购手册》，以便采用新的商业5G功能或将其集成到国防部的任务和系统中。

（2）国防部各部门将利用即将推出的美国国防部5G参考架构（5G Reference Architecture）来部署5G系统。

（3）增加通用基础设施、风险框架和标准的使用。应在可行且适当的情况下利用通用基础设施。例如，应考虑利用已规划的国防部企业级5G网，而不是建立单独的专用5G核心网。美国国防部各部门应把国防部企业级5G网的可用性纳入其业务案

例分析中。

（4）私有5G网络必须遵守网络安全要求和供应链风险管理要求。与美国国防部使用的大多数产品一样，5G设备、产品和服务必须符合国防部的供应链要求，应满足适当的合规性要求。此外，国防部各部门必须符合2019年5月15日颁布的《确保信息通信技术和服务供应链安全》行政令。

（5）针对私有网络，国防部各部门及合作伙伴应采用国防信息系统局（DISA）的持续监控功能，或由国防部首席信息官批准的类似的网络安全服务供应商（CSSP）提供的监控功能服务。

黄茹 供稿自

https://www.defense.gov/News/Releases/Release/Article/3962808/dod-releases-private-5g-deployment-strategy/

原文标题：DOD Releases Private 5G Deployment Strategy

[半导体]美令台积电断供我国先进人工智能芯片

2024年11月10日，据路透社报道，美国商务部已经发函给台积电，要求对采用7纳米或更尖端技术制造的AI加速器和GPU实施出口管制。

据2024年10月报道，全球半导体逆向工程和信息提供商TechInsights公司拆机发现，华为最先进人工智能芯片昇腾910B使用了台积电生产的芯片，违反了美国出口管制法规。基于此，美国商务部向台积电发送“知会函”，绕过冗长的出口管制规则制定程序，快速对台积电先进人工智能芯片生产实施新的管制要求。

消息称，在收到美国商务部函文后，台积电已于2024年10月暂停向我国芯片设计公司算能（Sophgo）发货，因其芯片与华为昇腾910B使用的台积电芯片相匹配。台积电已通知受影响客户，自2024年11月11日起暂停供应7纳米及以下工艺制程的先进人工智能芯片。这次美国商务部发出的通知函，能让该部门对收到信函的特定公司迅速实施管制。

黄茹 供稿自

https://www.reuters.com/technology/us-ordered-tsmc-halt-shipments-china-chips-used-ai-applications-source-says-2024-11-10/

https://www.reuters.com/technology/artificial-intelligence/tsmc-suspend-production-advanced-ai-chips-china-monday-ft-reports-2024-11-08/"

原文标题：Exclusive: US ordered TSMC to halt shipments to China of chips used in AI applications

[半导体]韩国拟投入 100 亿美元政策性融资支持芯片产业

2024年11月28日，据《韩国经济》报道，韩国政府将为国内半导体产业，投入超14万亿韩元（约合100亿美元）的政策性融资，以应对来自美国新政府的不确定性和芯片行业愈发激烈的竞争。这是继2024年6月公布26万亿韩元规模的《半导体生态界支援方案》后，韩国时隔5个月再次推出新的措施。

韩国财政部11月27日表示，为继续实施刺激政策，明年将提供包括国有银行贷款在内的财政支持，金额将达到14.3万亿韩元。此外，韩国政府在一份声明中表示，政府计划承担首尔南部的龙仁、平泽芯片产业集群地下铺设电缆所需的1.8万亿韩元中的大部分资金，以支持新芯片园区的企业。韩国正在建设号称全球最大的高科技芯片制造集群，以吸引相关企业。

韩国政府还计划到2030年，将半导体相关企业的税收抵免率提高10个百分点，并建设规模达4万亿韩元的国家“人工智能计算中心”。

韩财政部在声明中表示，特朗普新政府上台后，经济不确定性可能会增加。保护主义浪潮的兴起也可能削弱韩国依赖贸易的经济。技术出口约占韩国海外出口的1/3。与2023年相比，2024年韩国经济预计将至少增长2%，尤其是受半导体需求强劲的推动，包括用于人工智能开发的存储芯片。近几个月出口涨势减弱后，经济学家对明年的预测变得不那么乐观。

黄茹 供稿自

http://korea.people.com.cn/n1/2024/1129/c407882-40371832.html

原文标题：韩媒：韩国拟融资100亿美元支持芯片业

[半导体]日本提供超 650 亿美元推动半导体等产业发展

2024年11月12日，日本政府表示计划在2030财年前提供至少10万亿日元（约650亿美元），以支持半导体和人工智能产业发展。

美国及其盟友正竞相在人工智能驱动的半导体研究方面发力，日本政策制定者认为这一领域对经济安全至关重要。根据新的计划草案，该投资计划与之前的4万亿日元专项投资资金分开，将共同推动半导体和人工智能产业的发展。未来10年全球对芯片的需求预计将增加两倍，该计划旨在通过外包、财政支持和立法措施等方式向日本企业提供超过10万亿日元的资助，以提高私营企业的盈利。在日本前首相的支持下，日本已经拨出约4万亿日元的资金来振兴其芯片行业，其中包括向北海道的Rapidus公司提供9200亿日元补助。Rapidus公司提出的目标是到2027年，实现先进逻辑芯片的量产。

此外，据《日经新闻》2024年11月1日报道，日本政府正计划发行债券，为半导

体公司提供额外补贴。

黄茹 供稿自

https://www.bnnbloomberg.ca/business/technology/2024/11/11/japans-ishiba-pledges-over-65-billion-aid-for-chip-ai-sectors/

原文标题：Japan’s Ishiba Pledges Over $65 Billion Aid for Chip, AI Sectors

[人工智能]美 NIST 成立 AI 国家安全风险测试工作组

2024年11月21日，美国国家标准与技术研究院（NIST）下属的美国人工智能安全研究所宣布成立人工智能国家安全风险测试（TRAINS）工作组，致力于评估人工智能模型的安全。

该工作组成员由美国多个部门及研究机构的专家组成，包括美国国防部首席数字和人工智能办公室和国家安全局、能源部及其国家实验室、国土安全部、网络安全和基础设施安全局、美国国立卫生研究院（NIH）卫生与公众服务部。工作组将在关键的国家安全和公共安全领域，包括辐射和核安全、化学和生物安全、网络安全、关键基础设施、常规军事能力等，对先进的人工智能模型进行协调测试和评估。

美国商务部部长表示，实现安全、可靠和值得信赖的人工智能不仅是一项经济优先事项，更是公共安全和国家安全的当务之急。美国人工智能安全研究所将继续发挥领导作用，集中政府各部门的顶尖国家安全和人工智能专业知识，利用人工智能的优势造福美国人民和美国企业。

黄茹 供稿自

https://www.nextgov.com/artificial-intelligence/2024/11/nist-sets-new-task-force-ai-and-national-security/401214/

原文标题：NIST sets up new task force on AI and national security

[人工智能]加拿大成立 AI 安全研究所

2024 年 11 月 12 日，加拿大创新、科学和经济发展部宣布成立加拿大人工智能安全研究所（CAISI），以提升加拿大应对人工智能安全风险的能力，巩固加拿大在全球人工智能技术安全开发与应用方面的领导地位。

人工智能的快速发展凸显了这项变革性技术的前景和风险，确保人工智能系统安全和负责任使用是加拿大政府的首要任务。CAISI 将利用加拿大世界领先的人工智能研究生态系统和人才基础，促进对与先进人工智能系统相关风险的理解，并推动制定应对这些风险的措施。基于加拿大通过《布莱切利宣言》对国际合作的承诺，

CAISI 还将与其他司法管辖区的安全机构合作。

CAISI 初始启动资金为 5000 万美元，隶属于加拿大创新、科学和经济发展部，并设有专门的办公室负责监督研究进程并与国际合作伙伴交流。

CAISI 将依托加拿大国家研究委员会、加拿大高级研究所（CIFAR）以及加拿大三大国家人工智能研究所（埃德蒙顿的艾米研究所、蒙特利尔的米拉研究所、多伦多的矢量研究所）的现有资源，并让更广泛的加拿大研究和商业界参与开展项目，以评估风险、测试系统和制定应对风险的指南，重点聚焦以下两个方面：

（1）应用研究和科研主导的项目：与 CIFAR 合作，促使国际专家共同解决人工智能安全领域的关键问题。

（2）政府主导的项目：由加拿大国家研究委员会实施，重点关注与国家优先事项相关的人工智能技术，特别是与网络安全等相关的项目，或涉及全球人工智能安全机构的合作项目。

黄茹 供稿自

https://www.canada.ca/en/innovation-science-economic-development/news/2024/11/canada-launches-canadian-artificial-intelligence-safety-institute.html

原文标题：Canada launches Canadian Artificial Intelligence Safety Institute

[人工智能]美发布《关键基础设施中 AI 的角色和职责框架》指南

2024年11月14日，美国国土安全部发布了一份关于在关键基础设施中负责任地使用AI的新指南——《关键基础设施中人工智能的角色和职责框架》。该框架由AI供应链各层实体共同开发，旨在为云和计算提供商、AI开发者、关键基础设施所有者和运营商，以及民间社会和公共部门实体提供指导，确保AI在美国关键基础设施中的安全和可靠部署，同时保护公民权利和自由，并推进AI安全研究。

电力、水处理、交通和数字网络等对国家安全至关重要的关键基础设施，越来越多地依赖AI来提升服务、建立弹性和应对威胁。然而，AI漏洞让这些关键基础设施面临着被恶意操纵的风险。因此，该框架针对美国关键基础设施中AI开发和部署的每类关键利益相关者提出了以下建议：

（1）云和计算基础设施服务提供商在保护关键基础设施中的AI开发环境方面发挥着重要作用，涉及审查硬件和软件供应商、建立强大的访问管理、保护为AI系统提供支持的数据中心的物理安全等。该框架鼓励云和计算基础设施服务提供商通过监控异常活动并建立明确的途径来报告可疑和有害活动，从而为AI开发下游的客户和流程提供支持。

（2）AI开发人员通常通过软件工具或特定应用程序使关键基础设施能够访问AI

模型。该框架建议AI开发人员采用安全设计方法，评估AI模型的危险能力，并确保模型秉持以人为本的价值观。该框架同时鼓励AI开发人员采取强有力的隐私保护措施，通过评估以检测潜在的偏见、故障模式和安全漏洞；同时，框架还支持对那些对关键基础设施系统及其用户构成高风险的模型进行独立评估。

（3）该框架建议关键基础设施所有者和运营商应采购和部署安全的AI系统。具体包括推进网络安全实践以应对AI相关风险，在微调AI产品时保护客户数据，以及在使用AI向公众提供商品、服务或福利方面时提供有意义的透明度。该框架还鼓励关键基础设施实体积极监测相关AI系统的性能，并与AI开发人员和研究人员分享结果，帮助他们更好地理解模型行为与现实世界结果之间的关系。

（4）该框架建议公民社会和公共部门一起参与标准制定，研究关键基础设施用例的AI评估。公民社会包括大学、研究机构和消费者权益倡导者。

（5）该框架鼓励联邦政府与国际伙伴继续开展合作，以保护全球公民的利益，并鼓励各级政府之间进行协作，共同资助和支持AI安全与保障的基础研究。

唐蘅 供稿自

https://www.dhs.gov/news/2024/11/14/groundbreaking-framework-safe-and-secure-deployment-ai-critical-infrastructure#:~:text

https://apnews.com/article/ai-artificial-intelligence-infrastructure-national-defense-infrastructure-3b4a0c6962ad75ef50422b726e7e04e0

原文标题：Groundbreaking Framework for the Safe and Secure Deployment of AI in Critical Infrastructure Unveiled by Department of Homeland Security

前沿研究动态

[人工智能]谷歌利用大模型在真实环境发现内存安全漏洞

2024 年 11 月 5 日，据“网络杂志”网站（CyberMagazine）报道，谷歌 Project Zero 团队和 DeepMind 的研究人员利用大型语言模型首次在真实环境发现内存安全漏洞。

派拓网络（PaloAlto）、飞塔（Fortinet）和众击（CrowdStrike）等网络安全巨头已经在威胁检测功能中加入了人工智能技术。此次谷歌的突破进一步体现了人工智能在漏洞研究这一领域的应用迈出了一大步。

该漏洞是常见的开源数据库引擎 SQLite 中的一个漏洞，而且 SQLite 现有的测试系统没有办法检测出该漏洞。该方法与传统的检测方法不同，谷歌利用大模型发现了安全漏洞，体现出人工智能辅助漏洞研究的潜力。

谷歌于 2024 年 6 月推出“午睡”项目（Nap time），后更名为“沉睡”，是 Project

Zero 团队和 DeepMind 之间的合作项目，旨在使大型语言模型能够执行漏洞研究，模仿人类安全研究人员的工作流程。“沉睡”的设计重点是人工智能代理和目标代码库之间的交互，为人工智能提供了一套专门的工具，旨在复制人类安全研究人员的工作流程。“沉睡”工具包括：①浏览目标代码库的代码浏览器；②在沙盒环境中运行脚本进行模糊测试的 Python 工具；③观察不同输入下程序行为的调试器；④监控任务进度的报告器。这套全面的工具集使人工智能代理能够以与人类专家的迭代、假设驱动的方法非常相似的方式执行漏洞研究。

这项技术仍处于早期阶段。“沉睡”项目的研究人员强调，他们的研究成果仍然实验性极强。网络安全社区将密切关注人工智能支持的漏洞研究如何发展。

黄茹 供稿自

https://cybermagazine.com/articles/googles-big-sleep-from-concept-to-vulnerability-discovery

原文标题：Google's Big Sleep: From Concept to Vulnerability Discovery

[半导体]SK 海力士推出第五代高带宽存储器芯片

2024 年 11 月 6 日，SK 海力士在首尔“2024 年 SK AI 峰会”上正式宣布开发 48 千兆字节（GB）的 16 层堆叠的高带宽存储器芯片“HBM3E”，这是高带宽存储器芯片迄今为止最大的容量

SK 海力士研究人员表示，已成功通过堆叠 16 个 DRAM 芯片实现了 48GB 容量，应用了已被证明可批量生产的先进 MR-MUF 技术，并且还在开发具有备份工艺的混合键合技术。与 12 层堆叠上一代高带宽存储器芯片相比，新一代 HBM3E 可以将人工智能学习性能提高多达 18%，将推理性能提高多达 32%，并将于 2025 年实现商业化。

黄茹 供稿自

https://news.skhynix.co.kr/post/sk-ai-summit-2024

原文标题：SK하이닉스, SK AI Summit 2024에서 현존 최대 용량의 ‘HBM3E 16단’ 개발 공식화

产业动态

[人工智能]Fastino 推出任务优化 AI 模型

2024年11月12日，微软和Insight Partners等企业联合投资的初创公司Fastino，首次推出了一种面向企业的任务优化AI模型，能在通用CPU上高效运行，无需依赖昂贵的GPU资源，使企业在降低成本的同时，又能满足其对技术性能的需求。

Fastino此次推出的任务优化AI模型专为特定企业用例设计，如文本结构化和任务规划，旨在提高与语言相关任务的准确性、计算速度并降低能耗。该模型基于transformer架构自主研发，区别于传统的LLM和小语言模型（SLM），优化了其在通用CPU上的运行效率，确保了卓越的性能表现。该模型是一个新的模型类别，不是一个仅按参数数量计算的大或小的“通才”模型。Fastino的模型缩小了模型的使用范围，在构建文本数据、优化RAG（检索增强型生成）管道、任务规划和推理等任务中表现优异。

黄茹 供稿自

https://venturebeat.com/ai/microsoft-backed-startup-debuts-task-optimized-enterprise-ai-models-that-run-on-cpus/

原文标题：microsoft backed startup debuts task optimized enterprise ai models that run on cpus

[量子技术]微软和 Atom Computing 公司推出量子计算机

2024年11月19日，美国微软和原子计算公司在容错量子计算方面取得新突破，能够创建24个量子比特的逻辑纠缠GHZ态，计划在2025年推出基于该技术的商用量子计算机，该计算机将拥有1000多个物理量子比特。

量子纠缠是一种非常敏感的物理现象，很容易受到外部环境干扰而产生噪声，从而导致计算错误，这种极高的易错性是量子计算机发展所面临的最大挑战。在该研究中，微软和原子计算公司使用不带电的中性原子，可有效检测出量子比特中的错误，并在计算时对该错误进行纠正，从而使给定的量子计算机输出准确的结果，证明了量子纠错的可能性。

逻辑量子比特是通过量子纠缠相互连接的量子比特组，容错率比普通量子比特更高。GHZ态涉及多个量子的纠缠，可为量子算法提供更强大的工具。在实际应用中，生成高保真度的GHZ态是实现量子技术应用的关键。为创建24个逻辑量子比特纠缠态，微软利用了其新推出的Azure Quantum平台。该平台融合了云计算、AI和逻辑量子比特等技术，能解决传统机器难以处理的问题。

唐蘅 黄茹 供稿自

https://www.nextgov.com/emerging-tech/2024/11/microsoft-and-atom-computing-unveil-24-qubit-quantum-machine/401140/

原文标题：Microsoft and Atom Computing unveil 24-qubit quantum machine

[量子技术]谷歌利用人工智能进行量子纠错

2024年11月27日，谷歌DeepMind与谷歌量子AI团队联合开发了人工智能解码器AlphaQubit，专门解决量子计算中长期存在的纠错难题，相关研究成果发表在《自然》杂志上。

AlphaQubit基于谷歌Sycamore量子计算机的多年研究成果，利用49个量子比特的系统和量子模拟器，生成数亿例量子错误数据，训练深度学习神经网络以精准识别错误。

测试显示，AlphaQubit在高精度场景中实现了6%的纠错提升，而在快速但精度较低的场景下提升高达30%。随后，团队在241个量子比特的更大规模实验中验证了AlphaQubit的可扩展性与鲁棒性。

蒲云强 黄茹 供稿自

https://blog.google/technology/google-deepmind/alphaqubit-quantum-error-correction/

原文标题：AlphaQubit tackles one of quantum computing’s biggest challenges

版权及合理使用声明

《科学研究动态监测快报》（以下简称《监测快报》）是由中国科学院文献情报中心、中国科学院成都文献情报中心、中国科学院武汉文献情报中心以及中国科学院兰州文献情报中心和中国科学院上海生命科学信息中心按照主要科学研究领域分工编辑的科学研究进展动态监测报道类信息快报。

《监测快报》遵守国家知识产权法的规定，保护知识产权，保障著作权人的合法利益，并要求参阅人员及研究人员遵守中国版权法的有关规定，严禁将《监测快报》用于任何商业或其他营利性用途。读者在个人学习、研究目的中使用信息报道稿件，应注明版权信息和信息来源。未经编辑单位允许，有关单位和用户不能以任何方式全辑转载、链接或发布相关科学领域专辑《监测快报》内容。有关用户单位要链接、整期发布或转载相关学科领域专辑《监测快报》内容，应向具体编辑单位发送正式的需求函，说明其用途，征得同意，并与具体编辑单位签订服务协议。

欢迎对《科学研究动态监测快报》提出意见与建议。

信息科技专辑：

编辑出版：中国科学院成都文献情报中心

联系地址：四川省成都市天府新区群贤南街 289 号（610299）

联系人：唐川 王立娜 张娟 徐婧 杨况骏瑜 黄茹 唐蘅 蒲云强 李晨曦

电话：（028）85235556

电子邮件：tangc@clas.ac.cn; wangln@clas.ac.cn; zhangj@clas.ac.cn; jingxu@clas.ac.cn; yangkjy@clas.ac.cn;huangr@clas.ac.cn; tangh@clas.ac.cn; puyq@clas.ac.cn; licx@clas.ac.cn

内部资料

中国科学院成都文献情报中心
新一代信息科技战略研究中心
电话：028-85235075
E-mail：casit@clas.ac.cn
地址：四川省成都市群贤南街289号, 610299