RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE
THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary

October 31, 2024

THE US IS THE WORLD'S SCIENCE SUPERPOWER — BUT FOR HOW LONG?

Jeff Tollefson and Richard Van Noorden | NATURE | October 23, 2024

Science in the United States has never been stronger by most measures. Over the past five years, the nation has won more scientific Nobel prizes than the rest of the world combined — in line with its domination of the prizes since the middle of the twentieth century. In 2020, two US drug companies spearheaded the development of vaccines that helped to contain a pandemic. Two years later, a California start-up firm released the revolutionary artificial-intelligence (AI) tool ChatGPT and a national laboratory broke a fundamental barrier in nuclear fusion. This year, the United States is on track to spend US$1 trillion on research and development (R&D), much more than any other country. And its labs are a magnet for researchers from around the globe, with workers born in other nations accounting for 43% of doctorate-holders in the US workforce in science, technology, engineering and medicine (STEM). But as voters go to the polls in November to elect a new president and Congress, some scientific leaders worry that the nation is ceding ground to other research powerhouses, notably China, which is already outpacing the United States on many of the leading science metrics.

Read the full article here.

MORE STEM PHDS COME HOME AS CHINA'S GLOBAL STANDING SOARS

Xiujuan Sun and Hantian Wu | University World News | October 16, 2024

China's positional change within the global political economy has resulted in a continuous expansion in the scale of Chinese students returning home after their overseas studies. Since 2012, more than 80% of overseas Chinese students have opted to return – a big increase from about 5% in 1987 and 30.6% in 2007. Meanwhile, as the competition for academic positions continues to escalate in the Global North, the reverse flow phenomenon is becoming all the more conspicuous among international doctorate holders. And this even affects those from science, technology, engineering and mathematics (STEM) fields, who were far more likely to stay abroad before China transformed itself into a new geo-economic powerhouse. While it is not yet possible to ascertain whether the homebound mobility of international STEM talent will engender a permanent human capital loss for their host countries, it arguably has a key role to play in further reversing the brain drain from China to the developed nations, and importantly, in reshaping global economic dynamics.

Read the full article here.

A HONG KONG UNIVERSITY LAUNCHED THE WORLD'S FIRST LARGE-SCALE AI MODEL EARTH OBSERVATION SATELLITE

Sunny Cheung | The Diplomate | October 21, 2024

In late September, the Chinese University of Hong Kong (CUHK) launched an artificial intelligence (AI)-equipped Earth observation satellite, named the "Hong Kong Youth Science and Technology Innovation Satellite" (香港青年科創號) with support from the ADA Space, a company that is associated with China's central government and its military-civilian fusion strategy. This cutting-edge satellite – billed by the CUHK as "the world's first large-scale AI model scientific satellite" – showcases Hong Kong's growing role in China's space ambitions and highlights the city's strategic importance in technological development. The satellite allegedly focuses on monitoring environmental and geographical data, particularly in Hong Kong and the Greater Bay Area. However, its advanced AI capabilities also suggest its potential for dual-use applications, potentially providing military reconnaissance in addition to serving civilian needs.

Read the full article here.

DEPARTMENT OF THE NAVY'S FLANK SPEED SERVICE SETS NEW STANDARD FOR ZERO TRUST IN DOD

Darren Turner | CHIPS | October 12, 2024

The Navy's Flank Speed cloud service, designed and developed by Program Executive Office for Digital and Enterprise Services (PEO Digital) in partnership with U.S. Fleet Cyber Command (FCC), operated by Navy Network Warfare Command (NNWC) and defended by Navy Cyber Defense Operations Command (NCDOC), has set a new benchmark for Zero Trust (ZT) security across the Department of Defense (DOD). The Department of the Navy's (DON) Impact Level 5 (IL5) unclassified Microsoft Azure and Microsoft 365 (M365) cloud implementation surpassed expectations during its second round of security assessments sponsored by the DOD Zero Trust Portfolio Management Office (PfMO). Known as Flank Speed, this combined cloud service achieved full compliance with all 91 Target ZT activities — a significant milestone completed three years ahead of the DOD Chief Information Officer's (CIO) fiscal year 2027 deadline — while also meeting 60 of the 61 Advanced ZT activities.

Read the full article here.

AGENCIES PREP FOR NEXT PHASE OF 'ZERO TRUST' CYBER UPGRADES

Justin Doubleday | Federal News Network | October 22, 2024

Agencies are due in the coming weeks to submit updated "zero trust" implementation plans to the White House, marking a key checkpoint in efforts to modernize government cyber defenses. The implementation plans are due to the Office of Management and Budget and the Office of the National Cyber Director by Nov. 7. That deadline was set out in a summertime memo on the Biden administration's cybersecurity priorities for the fiscal 2026 budget. The memo states agency plans should particularly focus on the status of initiatives to upgrade cyber defenses for so-called "high value assets" and "high impact systems." The plans will provide federal cyber leaders with a key update on the January 2022 zero trust strategy, which lays out a multi-pronged effort to shift away from perimeter-based cyber defenses toward a "never trust, always verify" approach. The strategy focuses on five technology pillars: identity; devices; networks; applications and workloads; and data.

Read the full article here.

NSA TELLS IPHONE AND ANDROID USERS: REBOOT YOUR DEVICE NOW

Davey Winder | Forbes | October 24, 2024

The NSA's original warning was published in a mobile device best practices guide in 2020. If you are having difficulty opening the PDF document the previous link takes you to, then there is an alternative route to the same document that requires a few more clicks available from the NSA press room. With smartphones running across all operating system platforms becoming an increasingly popular target for threat actors of all flavors, the NSA said that "many of the features provide convenience and capability but sacrifice security" and attempted to pin down simple steps that even the most non-technical users could take to better protect their devices and the data stored within. Earlier this year, I reported on the NSA advice, and that article has continued to stir a myriad of responses to this day.

Read the full article here.

DOD 'FINE TUNES' FINAL CMMC PROGRAM RULE, INDUSTRY TURNS ATTENTION TO IMPLEMENTATION

Justin Doubleday | Federal News Network | October 18, 2024

The Pentagon didn't introduce any groundbreaking changes in the final Cybersecurity Maturity Model Certification rule, but CMMC observers say the Defense Department made several key updates and definitions to help companies as they work to comply with the requirements. Meanwhile, industry groups are now turning their attention to potential challenges with implementing the CMMC requirements through the contracting process. The Defense Department published the final CMMC rule in the Federal Register earlier this week. The rule establishes the underlying processes and governance for the contractor certification program. As many expected, the final rule maintains the three tiers of the CMMC requirements, and the certification program's alignment with National Institute of Standards and Technology cyber standards.

Read the full article here.

CHINA'S GAINS IN QUANTUM THREATENED BY LACK OF TALENT, SELF-SABOTAGING COMPETITION, LEADING CHINESE ACADEMIC WARNS

Matt Swayne | The Quantum Insider | October 25, 2024

- China's quantum sector faces critical challenges due to a shortage of elite talent and an internal culture of *nei juan*, or involution, which hampers long-term innovation, according to a story in the *South China Morning Post* (SCMP).
- Despite substantial investments and goals to lead globally by 2035, the nation's research model prioritizes publication over practical skills, impacting the development of technical expertise essential for quantum computing.
- With mounting competition from the U.S. and external pressures like export controls, experts urge China to foster an environment that values skill-building over short-term achievements to ensure sustained growth in quantum technology.

Read the full article here.

DE-RISKING OF RESEARCH BECOMES HARDER AS 'GREY' ZONES EMERGE

Yojana Sharma | University World News | October 22, 2024

Links between European researchers and Chinese military universities made public in recent weeks have heightened concerns among academics and institutions in Europe about the risk of cooperating with Chinese institutions that may hide their military links. But many researchers are unsure how to identify the danger signals: due diligence is complicated by vague definitions of 'dual-use technologies' that can be for both civilian and military use, as well as emerging 'grey zones'; and the shifting geopolitical environment makes it harder to keep up with research risks linked to economic competitiveness. Compared to even a year or two ago, academics and researchers in Europe, including Germany, Belgium, the Netherlands and the Nordic countries, have become more aware of research security issues in collaborations with universities in China. In part, this is due to a number of cases hitting the headlines concerning Chinese researchers arrested for spying or denied visas.

Read the full article here.

CHINA IS MAKING A PLAY FOR GLOBAL TECHNO-SECURITY LEADERSHIP—HERE'S HOW THE U.S. SHOULD RESPOND

Tai Ming Cheung | Institute on Global Conflict and Cooperation (IGCC) | October 23, 2024

Beijing sees science, technology, and innovation as the key to challenging the United States for global leadership in the 21st century. As Washington and its allies look to thwart its technological rise, China is drawing on its history to overcome Western-imposed barriers and establish itself as a global techno-security superpower. To meet the challenge of U.S. strategic rivalry, the People's Republic of China (PRC), primarily under the leadership of the Chinese Communist Party (CCP), is mobilizing the country's economy and society towards technological goals. The United States' bottom-up, market-based innovation system is a sharp contrast from the CCP's top-down approach, and has been wildly successful at producing innovation. But for the United States to maintain its technological edge, the federal government must supply high-level strategic guidance and support to the nation's scientific enterprise.

Read the full article here.

THE NATIONAL SECURITY MEMORANDUM ON ARTIFICIAL INTELLIGENCE — CSET EXPERTS REACT

Igor Mikolic-Torreira, Hanna Dohmen, Jacob Feldgoise, Sam Bresnick, Emelia Probasco, Kyle Miller, and Owen Daniels | The Center for Security and Emerging Technology (CSET) | October 24, 2024

On October 24, the White House issued the first-ever National Security Memorandum (NSM) on Artificial Intelligence. President Biden directed his national security staff to develop the NSM in October 2023 as part of his Executive Order on Safe, Secure, and Trustworthy AI, which federal agencies have been implementing over the past year. According to a fact sheet released by the White House, the NSM focuses on three critical areas: ensuring U.S. leadership in developing "safe, secure, and trustworthy" AI, using cutting-edge AI to advance U.S. national security interests, and building an international consensus on AI governance. CSET experts offered their reactions and insights into the new AI NSM and its implications for U.S. national security, geopolitical competitiveness, and AI development more broadly.

Read the full article here.

COMMERCE ADDS 26 ENTITIES TO THE ENTITY LIST FOR ACTIONS CONTRARY TO U.S. NATIONAL SECURITY INTERESTS

U.S. Department of Commerce | Bureau of Industry & Security | October 21, 2024

Today, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) added 26 entities to the Entity List for activities contrary to U.S. national security and foreign policy under the destinations of the People's Republic of China (PRC) (6), Egypt (1), Pakistan (16), and the United Arab Emirates (UAE) (3). These additions are related to alleged violations of export controls, involvement in weapons programs of concern, and evasion of U.S. sanctions and export controls on Russia and Iran. Nine of the entities under the destination of Pakistan were added for acting as front companies and procurement agents for the Advanced Engineering Research Organization, a Pakistan-based company added to the Entity List in 2014. The remaining 7 Pakistani entities were added for contributions to Pakistan's ballistic missile program.

Read the full article here.

ENGAGING WITH SECURITY RESEARCHERS: EMBRACING A "SEE SOMETHING, SAY SOMETHING" CULTURE

Tod Beardsley, Known Exploited Vulnerability Team Lead & Daniel Larson, Coordinated Vulnerability Disclosure Team Lead | America's Cyber Defense Agency | October 23, 2024

In an age where digital systems have an electronic tendril in nearly every aspect of our lives, the role of cybersecurity researchers is more important than ever. These individuals and groups proactively identify weaknesses in software, networks, and hardware, often before malicious actors get a chance to exploit them. Yet even though we've collectively developed a set of norms and standards for coordinated vulnerability disclosure, companies, open-source projects, and government agencies sometimes respond to these unsolicited reports with fear, uncertainty, and doubt, rather than engagement, driving away the very allies we all rely on to keep our systems safe.

Read the full article here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute

USEFUL RESOURCES

SAFEGUARDING THE US SPACE INDUSTRY

National Counterintelligence and Security Center

According to US financial sector estimates, the global space economy is projected to grow from $469 billion in 2021 to more than $1 trillion by 2030. The United States is the main driver of this growth through its role as a global leader in space investment, research, innovation, and production. Space is fundamental to every aspect of our society, including emergency services, energy, financial services, telecommunications, transportation, and food and agriculture. All rely on space services to operate.

Read the full article here.

FVEY PARTNERS WARN OF EVOLVING EFFORTS TO RECRUIT CURRENT AND FORMER WESTERN SERVICE MEMBERS TO BOLSTER THE PRC'S MILITARY

Office of the Director of National Intelligence | June 2024

The Office of the Director of National Intelligence's National Counterintelligence and Security Center (NCSC) today joined partners from Australia, Canada, New Zealand, and the United Kingdom in warning about continued efforts by the People's Republic of China (PRC) to recruit current and former Western military personnel to train the PRC military. "To overcome their shortcomings, China's People's Liberation Army (PLA) has been aggressively recruiting Western military talent to train their aviators, using private firms around the globe that conceal their PLA ties and offer recruits exorbitant salaries.

View the full resource here.

FIVE EYES LAUNCH SHARED SECURITY ADVICE CAMPAIGN FOR TECH STARTUPS

Office of the Director of National Intelligence

Today, members of the Five Eyes intelligence partnership launched Secure Innovation, shared security guidance to help protect emerging technology companies from a range of threats, particularly those from nation-state actors. The launch of this joint protective security guidance aimed at protecting the tech sector from national security threats follows last October's unprecedented summit which brought together the heads of the domestic security and intelligence agencies from Australia, Canada, New Zealand, the UK, and the US to announce Five Shared Principles to protect technology companies.

View the full resource here.

REGISTRATION NOW OPEN FOR THE ASCE 2025 ANNUAL SEMINAR FEBRUARY 25-27, TO BE HELD AT TEXAS A&M UNIVERSITY

Born from a commitment to safeguarding the integrity of academic research, the Academic Security and Counter Exploitation (ASCE) program, spearheaded by The Texas A&M University System's RISC Institute, fosters a sense of community among university research security professionals, uniting them in a collaborative defense against emerging threats. Since its inception in 2016, ASCE has been a beacon in the fight against foreign influence, equipping academic institutions with the knowledge and tools needed to protect their invaluable research. Now in its ninth year, the annual ASCE Seminar stands as the preeminent gathering for training, networking, and collaboration, laser-focused on fortifying the academic research enterprise.

View the full resource here.

ASCE 2025 CALL FOR PROPOSALS

If you would like to present, please submit your proposal by clicking on the link below.
The seminar committee will review all proposals, and the selection will be based on relevance to the seminar theme, quality of the abstract, and potential audience engagement. Presenters will be notified of acceptance or rejection no later than December 15, 2024. T**he submission deadline is November 15, 2024.**

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute