RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE

THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary

January 18, 2024

UNIVERSITY RESEARCH FUNDING AT RISK AMID ECONOMIC SLOWDOWN

Yojana Sharma | University World News | January 9, 2024

Universities and research institutes are most directly at risk from China's slowing economy as local government funding comes under increased pressure. Although China's science and technology (S&T) spending is likely to become more thinly spread in the future, not all areas of research and not all provinces will be equally affected, according to a report by a China-focused think tank. While science and technology is still a key priority for the Chinese leadership, "scarcer resources will likely force the government to channel funding more strategically toward a narrower core of national security-relevant technologies and companies". This is according to the report by the Rhodium Group titled Spread Thin: China's Science and Technology Spending in an Economic Slowdown. Weakening fiscal conditions pose a high risk of disruption, the report said. Local governments, many of them facing fiscal crunches, which were responsible for about two-thirds of total government S&T spending in 2022, including funding to universities, have been hard hit by China's slowdown. After years of high growth of around 7% to 10% a year, growth is expected to barely register 5% in 2024, according to various economic estimates.

Read the full article here.

THE SENTENCING OF A US NAVY SAILOR IS A WINDOW INTO CHINESE ESPIONAGE. HERE'S HOW THE US SHOULD RESPOND.

Andrew Brown | Atlantic Council | January 13, 2024

The United States and its allies and partners are under constant threat from pervasive efforts by China to collect intelligence, though this rarely makes it into the public eye. This week provided a clear reminder of this threat. On January 8, US Navy sailor Wenheng Zhao, who pled guilty in October 2023 in the Central District of California to one count of conspiring with a foreign intelligence officer and one count of receiving a bribe, was sentenced to twenty-seven months in prison and ordered to pay a $5,500 fine. Zhao was one of two active duty US servicemembers indicted in August 2023 for providing sensitive US military information to China. The second, Jinchao Wei, was indicted for violating an espionage statute and multiple export violations in the Southern District of California. According to the indictment, he was granted US citizenship while the alleged illegal activities were taking place. (Wei is, of course, presumed innocent until proven guilty in a court of law.) These two cases are playing out as tensions remain high between the United States and China, even after the November 2023 meeting between US President Joe Biden and Chinese leader Xi Jinping.

Read the full article here.

DOD RELEASES FIRST-EVER NATIONAL DEFENSE INDUSTRIAL STRATEGY

The Department of Defense | Press Release | January 11, 2024

The Department of Defense today released its inaugural National Defense Industrial Strategy (NDIS), which will guide the Department's engagement, policy development, and investment in the industrial base over the next three to five years. Taking its lead from the National Defense Strategy (NDS), this strategy will catalyze generational change from the existing defense industrial base to a more robust, resilient, and dynamic modernized defense industrial ecosystem. "The current and future strategic environment demands immediate, comprehensive, and decisive action to strengthen and modernize our defense industrial base ecosystem so it delivers at speed and scale for our warfighters," Deputy Secretary of Defense Kathleen Hicks said. "DoD's first-ever National Defense Industrial Strategy will help ensure we build the modern defense industrial and innovation ecosystem that's required to defend America, our allies and partners, and our interests in the 21st century. "

Read the full article here.

AGE-OLD PROBLEMS TO SHARING CYBER THREAT INFO REMAIN, IG REPORT FINDS

Christian Vasquez | CyberScoop | January 8, 2024

Over-classification, a lack of policy guidance and tensions between private sector cybersecurity firms are continuing to hamper federal government efforts to share cybersecurity threat information, according to a report released Friday by the U.S. intelligence community's top watch dog. Friday's report, released by the Office of the Inspector General of the Intelligence Community, concludes that while federal agencies have broadly improved their ability to share threat information and defensive mitigations long-standing policy and technical concerns are providing barriers to rapid information sharing. The IG's report examines how relevant federal agencies shared cyber threat information and defensive measures over the past two years through a framework created by the Cybersecurity Information Sharing Act of 2015. The report finds that the "policies, procedures, and guidelines" for sharing information are "sufficient" to carry out the requirements of the legislation and noted that "sharing has improved" in the last two years.

Read the full article here.

COURT UPHOLDS DECISION TO DENY VISA TO STUDENT FROM CHINA

Nathan Greenfield | University World News | January 8, 2024

The Federal Court of Canada (FCC) has upheld the 2022 decision of a visa officer to deny a Chinese national a visa that would have allowed him to enroll in a PhD science programme at the University of Waterloo (UW), one of Canada's premier science and technology universities. In his 28-page closely reasoned decision, the FCC's Chief Justice, Paul Crampton, found that the visa officer was correct to believe that "there are reasonable grounds to believe that Mr [Yuekang] Li may engage in an act of espionage that is against Canada or contrary to Canada's interests" and that such espionage includes "non-traditional means" such as reporting "open-source" information even after Li returned to China upon completion of his PhD. Li's visa application states that he wanted to improve China's underdeveloped application of advances to point-of-care technology in the field of public health and that a central part of this required the study of microfluidics, an area of micro-nanoscale science and technology.

Read the full article here.

RESEARCH SECURITY: STRENGTHENING INTERAGENCY COLLABORATION COULD HELP AGENCIES SAFEGUARD FEDERAL FUNDING FROM FOREIGN THREATS

U.S. Government Accountability Office | January 11, 2024

Federal agencies can award funds to foreign organizations or individuals to encourage scientific advancements. But some applicants may try to exploit U.S.-funded research—including in ways that jeopardize U.S. national security. While there are safeguards around these funds, not all agencies use the same tools to vet applicants. Also, agencies use available lists to determine which universities, companies, and other organizations are excluded from U.S. funding—but they said they could use more guidance on determining whether an organization is foreign-owned. We recommended agencies better share information to help protect U.S. research funds. GAO found that determining whether federal research and development (R&D) funds were provided to a foreign entity of concern is challenging. Such entities include foreign terrorist organizations and specially designated nationals, among others.

Read the full article here.

CONGRESS FOCUSES ON CHINA RISK AT U.S. COLLEGES AND UNIVERSITIES

Matthew A. Goldstein | Thomson Reuters Westlaw Today | January 8, 2024

Matthew A. Goldstein of Akerman LLP discusses a congressional focus on China's state-sponsored influence and technology transfers at U.S. colleges and universities. Last year ended with a flurry of Congressional reports focused on China's state-sponsored influence and technology transfers at U.S. colleges and universities. Various recommendations made in the reports and pending measures reflect concerns with the Chinese Government's use of open research environments in the United States to circumvent export controls and other national security laws. Accordingly, Congressional proposals seek to limit access to research, expand U.S. Government oversight of partnerships with Chinese research institutions, and increase enforcement efforts. These measures raise the potential for changes that may significantly impact colleges and universities in the new year.

Read the full article here.

CANADA NAMES 100 CHINESE, RUSSIAN, IRANIAN RESEARCH INSTITUTIONS IT SAYS POSE A THREAT TO NATIONAL SECURITY

Catharine Tunney | CBC News | January 16, 2024

Canadian universities and researchers studying advanced and emerging technologies, including artificial intelligence, will soon be ineligible for federal grants if they're affiliated with foreign institutions the government says pose a threat to national security. On Tuesday the federal government named more than 100 institutions in China, Russia and Iran which it says represent the "highest risk to Canada's national security." The government says the listed institutions are connected to those countries' militaries and state security agencies. The federal government also released what it called a list of "sensitive" research areas — including advanced weapons, quantum technologies, robotics, aerospace, space and satellite technology and medical and health-care technology.

Read the full article here.

17 SECURITY PRACTICES TO PROTECT YOUR BUSINESS'S SENSITIVE INFORMATION

Mark Fairlie | Business.com | January 11, 2024

You don't have to look far to see the repercussions of a business's failure to protect sensitive information. Equifax, Adobe and Target, among many others, have been victims of significant data breaches that hurt their reputations and bottom lines. Learn how to manage your online reputation. Indeed, failures in cybersecurity countermeasures have significant costs for businesses. In the U.S., cyberattacks cost small businesses more than $8,000 annually, on average, according to Hiscox. That's enough to dent a large hole in any small business's cash flow. We'll share 17 ways to protect your sensitive information from a cyberattack. Rather than focusing on the technical aspects, we'll look at how to educate your staff and create a culture of cybersecurity across your business. Then, we'll explore three primary attack vectors used by cybercriminals and explain the merits of cybersecurity insurance.

Read the full article here.

FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT STRATEGIC PLAN

Cyber Security And Information Assurance Interagency Working Group Networking And Information Technology Research And Development Subcommittee | National Science And Technology Council December 2023

President Biden has been clear that cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense. That's why the Biden-Harris Administration released the National Cybersecurity Strategy (NCS) in March 2023. The NCS makes it clear that advances in cybersecurity are urgently needed to prevent and thwart malicious activities and adversaries, insider threats, and to strengthen public trust in the digital ecosystem. This 2023 Federal Cybersecurity Research and Development Strategic Plan (the Plan) provides federal agencies updated guidance on the overall priorities for federally funded research and development in cybersecurity.

Read the full article here.

VISION, NEEDS, AND PROPOSED ACTIONS FOR DATA FOR THE BIOECONOMY INITIATIVE

Interagency Working Group On Data For The Bioeconomy | National Science And Technology Council December 2023

In September 2022, President Biden signed the Executive Order on Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy. The bioeconomy refers to economic activity derived from the life sciences, particularly in the areas of biotechnology and biomanufacturing, and includes industries, products, services, and the workforce. The goal of this Executive Order was to advance biotechnology and biomanufacturing towards innovative solutions in health, climate change, energy, food security, agriculture, supply chain resilience, and national and economic security. Action towards these goals requires high-quality, wide-ranging, easily accessible, and secure biological datasets to drive breakthroughs for the U.S. bioeconomy.

Read the full article here.

4 KEY TAKEAWAYS FROM NIST'S NEW GUIDE ON AI CYBER THREATS

Lauren French | SC Media | January 8, 2024

An AI threat guide, outlining cyberattacks that target or leverage machine learning models, was published by the National Institute of Standards and Technology (NIST) on Jan. 4. The nearly 100-page paper, titled "Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations," provides a comprehensive overview of the cybersecurity and privacy risks that come with the rapid development of both predictive and generative AI tools over the last few years. The new guide on adversarial machine learning (ALM) definitions, classifications and mitigation strategies is part of NIST's Trustworthy and Responsible AI initiative and is co-authored by NIST computer scientists and experts from Northeastern University and Robust Intelligence, Inc.

Read the full article here.

USEFUL RESOURCES

US FUNDED CHINESE DEFENSE RESEARCH TRACKER

Data Abyss

The "US Funded Chinese Defense Research Tracker" is a specialized tool designed to monitor and provide transparency regarding research activities funded by the United States with Chinese defense institutions. This tool compiles and displays information on research projects, publications, and funders associated with US funding sources and their affiliations with Chinese institutions. By offering a comprehensive overview of such research endeavors, it serves as a valuable resource for analysts, policymakers, and researchers interested in understanding the dynamics of US-funded defense research collaborations in China, promoting accountability, and facilitating informed decision-making in the realm of international research partnerships and security studies.

View the full resource here.

COMPUTER SECURITY RESOURCE CENTER (CSRC)

National Institute of Standards and Technology

The Computer Security Resource Center (CSRC) has information on many of NIST's cybersecurity- and information security-related projects, publications, news and events. CSRC supports people and organizations in government, industry, and academia—both in the U.S. and internationally.

- Learn more about current projects and upcoming events. Search and browse our publications library of current and historical standards, guidelines, and other reports
- Explore content by topic
- Search our glossary of terms defined in our publications
- Subscribe to CSRC email updates

View the full resource here.

NASA ISSUES NEW SPACE SECURITY BEST PRACTICES GUIDE

Jennifer M. Dooren | NASA | December 22, 2023

As space missions and technologies grow increasingly interconnected, NASA has released the first iteration of its Space Security Best Practices Guide to bolster mission cybersecurity efforts for both public sector and private sector space activities. The guide represents a significant milestone in NASA's commitment to ensuring the longevity and resilience of its space missions and will serve as a resource for enhancing their security and reliability. Additionally, the Space Security Best Practices Guide was designed to benefit users beyond NASA – international partners, industry, and others working in the expanding fields of space exploration and development. The guide is designed to provide security guidance for missions, programs, or projects of any size.

View the full resource here.

THREATS TO U.S. VITAL INTERESTS

The Heritage Foundation

Because the United States is a global power with global interests, scaling its military power to threats requires judgments with regard to the importance and priority of those interests, whether the use of force is the most appropriate and elective way to address the threats to those interests, and how much and what types of force are needed to defeat such threats. This Index focuses on three fundamental, vital national interests:

- Defense of the homeland;
- Successful conclusion of a major war that has the potential to destabilize a region of critical interest to the U.S.; and
- Preservation of freedom of movement within the global commons: the sea, air, outer space, and cyber-space domains through which the world conducts business.

View the full resource here.