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

Open Source Media Summary

June 20, 2024

RECORD SETTLEMENT OVER CHINA FUNDING PUTS U.S. RESEARCH INSTITUTIONS ON NOTICE

Jeffrey Mervix | Science | June 12, 2024

Over the past 5 years, the U.S. Department of Justice (DOJ) has won only a handful of criminal cases in which it prosecuted scientists alleged to have defrauded the government by not disclosing research support they received from China. But last month DOJ sent a clear message that, despite that poor track record, research institutions will be held accountable for mistakes in monitoring outside support to their faculty. A 17 May settlement with the Cleveland Clinic Foundation (CCF) requires the medical colossus to pay the government $7.6 million to resolve allegations it mismanaged three grants from the National Institutes of Health (NIH). It's a record amount for a case involving foreign research support, a mechanism U.S. policymakers believe China has used to steal U.S. technology. "Today's settlement illustrates the importance of being truthful at every stage of the grants process," U.S. Attorney Rebecca Lutzko said in a statement announcing the settlement. In addition to the fine, the settlement requires a top CCF administrator "to personally attest" to the accuracy of all information it submits to NIH.

Read the full article here.

HOW AI AND THE CLOUD ARE ACCELERATING SCIENTIFIC DISCOVERIES. WILL GOVERNMENT BE READY?

SCOOP News Group | FEDSCOOP | June 13, 2024

The convergence of artificial intelligence (AI) and high-performance cloud computing is dramatically reshaping the landscape of scientific research and discovery. Scientific breakthroughs that once took years to achieve are emerging in weeks, presenting new and powerful solutions to address complex global challenges. However, the accelerating rate of innovation also raises critical strategic questions for government and public policy institutions and whether they are prepared for the surge, suggests a new report. AI's emerging impact in the laboratory has made one thing clear: The scientific and research community is at the cusp of a new era when AI-propelled science will move at unprecedented speed and likely reshape priorities for government agencies responsible for agriculture, environmental protection, health, national security and other domains.

Read the full article here.

COALITIONS OF BUSINESSES AND NONPROFITS URGE LAWMAKERS TO SUPPORT NSF FUNDING

Association of American Universities | Leading Research Universities Report | June 10, 2024

Last week, two state and national coalitions of businesses and nonprofits, including institutions of higher education, sent letters to lawmakers asking them to support robust funding for the National Science Foundation in the FY25 federal budget. In Illinois, 59 businesses and nonprofits – including Northwestern University, the University of Chicago, and the University of Illinois Urbana-Champaign – sent a letter to members of the state's congressional delegation asking them to advocate for increased funding for the NSF. Multinational companies such as Cisco, IBM, Microsoft, and SAP joined the United States Chamber of Commerce in sending another letter making a similar request to leaders in the House and the Senate. The letters focused on the integral role the NSF plays in driving innovation in the United States and in creating an educated STEM workforce.

Read the full article here.

LEGISLATION SEEKS TO ESTABLISH AI RESEARCH PARTNERSHIPS BETWEEN U.S. AND FOREIGN CITIES

Edward Graham | NexGov/FCW | June 12, 2024

New House legislation would create international artificial intelligence research partnerships between U.S. cities and their foreign counterparts to promote collaboration on the development of emerging capabilities. The bill, introduced on Tuesday by Rep. Norma Torres, D-Calif., would direct the State Department to "encourage or support" the establishment of AI research partnerships — either directly or through public-private partnerships that include nonprofit organizations and academic institutions — between willing U.S. localities and foreign cities. "This legislation seeks to cultivate and expand the research and development of artificial intelligence to ensure new AI tools and real-world applications adhere to the shared values of the United States and its allies and in so doing contribute to security, uphold democratic principles, foster economic prosperity and sustain the dignity of every human life," Torres said in a statement.

Read the full article here.

HOW CHINA'S CYBER ECOSYSTEM FEEDS OFF ITS SUPERSTAR HACKERS

Tom Uren | Lawfare | June 14, 2024

A new report explores how effectively the Chinese state leverages civilian talent for state-sponsored cyber operations. "From Vegas to Chengdu," by Eugenio Benincasa from the Center for Security Studies at ETH Zurich, focuses on the links between Chinese hacking contests and bug bounties and the country's cyber espionage programs. Interestingly, it finds that People's Republic of China (PRC) vulnerability discovery efforts in recent years depend highly on just "a handful" of Chinese researchers. The report pulls together information made public over the past several years to comprehensively summarize evidence the PRC funnels vulnerability research into state-sponsored espionage efforts. Shortly after 2014, Chinese security researchers began dominating international hacking competitions. The report analyzes the performance of Chinese security researcher teams at the Pwn2Own hacking competition. In 2014, Chinese teams won just 13 percent of the total prize money. By 2017, this had risen to nearly 80 percent.

Read the full article here.

CHINA USING HACKING COMPETITIONS TO DEVELOP DOMESTIC TALENT

Mathew J. Schwartz | Bank Info Security | June 13, 2024

China boasts some of the world's most talented cybersecurity researchers and white hat hackers, as well as a strict cybersecurity law compelling individuals to assist the state. This combination appears to contribute to China's nation-state hacking groups' prowess and ability to wield more zero-day vulnerabilities than any other country, as they support Beijing's robust cyberespionage agenda, as well as intellectual property theft on behalf of public and private entities, according to a new report from cybersecurity researcher Eugenio Benincasa. Beijing is using domestic capture-the-flag and other hacking competitions to spot, develop and recruit new hacking talent domestically, as well as to gather and route information about zero-day flaws to the country's military and intelligence apparatus, according to Benincasa, who's a senior researcher in the Cyberdefense Project with the Risk and Resilience Team at the Center for Security Studies at Switzerland's public research university ETH Zurich.

Read the full article here.

US LAWMAKERS SEEK CHINA PATENT DATA AMID SCIENCE PACT TALKS

Michael Martina | Reuters | June 12, 2024

Republican lawmakers on Wednesday asked the U.S. Commerce Department whether the U.S. government had funded research that resulted in Chinese patents, aiming to highlight what they view as the risks of renewing a bilateral science and technology agreement. The decades-old U.S.-China Science and Technology Agreement (STA) expired in August, but the U.S. State Department has issued two six-month extensions in order to continue negotiations with Beijing over renewing it. The landmark pact, signed when Beijing and Washington established diplomatic ties in 1979 and renewed about every five years since, has underpinned cooperation in areas from atmospheric and agricultural science to basic research in physics and chemistry. But concerns about China's growing military prowess and alleged theft of U.S. scientific and commercial achievements have prompted questions among some lawmakers, officials and researchers about whether the agreement should continue.

Read the full article here.

US RESTRICTS EXPORTS TO TOP QUANTUM LABS IN CHINA

Jacob Taylor | American Institute of Physics (API) | June 10, 2024

Last month, the Commerce Department placed stringent export controls on many of the top quantum research centers in China. The department singled out 22 institutions for "their participation in the People's Republic of China's (PRC) quantum technology advancements and for acquiring or attempting to acquire U.S.-origin items to enhance the PRC's quantum capabilities." It added that these technologies "have substantial military applications and pose a significant threat to U.S. national security." Among the affected institutions are four branches of the Chinese Academy of Sciences, the Hefei National Laboratory for Quantum Information Science, and the University of Science and Technology of China. USTC was also targeted for "advancing China's nuclear program." The department placed these institutions on the "Entity List," requiring them to secure a license to acquire U.S.-origin technologies. The department also indicated it would likely deny such license requests.

Read the full article here.

THE CHALLENGE OF PURSUING RESEARCH SECURITY WHEN NATIONALITY BECOMES A SHORTHAND FOR RISK

Sapna Marwaha | WONKHE | June 10, 2024

A growing regulatory burden coupled with growing financial instability makes a challenging environment for research security best practice to evolve. There are inevitable pressures for efficiency, and the agendas impacting the sector find themselves competing instead of complementing one another. The constant push to do more with less can often drive policy and processes away from an "actor-agnostic" approach – in which security risk considerations and processes apply equally across research partnerships – and towards an "actor-specific" approach, where nations and nationality are used as a shorthand for determining risk levels. The second approach may enable teams to focus their attentions on states of concern – but there are clear risks of unintended consequences, and questions about equity and fairness. The recent shifts in US research security policy relating to China are a clear example of this. And this challenging period explains why it is now much more common to hear research management colleagues from across the pond reflect on equity, diversity and inclusion principles in their approach to research security.

Read the full article here.

CHINESE SCIENTISTS ADMIT TO FAKING RESEARCH OVER INSTITUTIONAL PRESSURE

Mizy Clifton | SEMAFOR | June 11, 2024

Chinese scientists felt pressured to engage in unethical research practices out of fear of losing their jobs, a study found. The Chinese government's 2015 "Double First-Class Scheme" called on universities to boost their global rankings by publishing more articles in international journals. One faculty head reportedly told academics they should "leave as soon as possible" if they did not meet publication targets, according to science journal Nature. Citing such pressures, academics admitted to "falsifying data, plagiarizing, exploiting students without offering authorship, and bribing journal editors." However, other Chinese scientists said the paper painted an overly negative picture and that its author only spoke to a small sample of academics.

Read the full article here.

CYBERATTACKS ARE HITTING RESEARCH INSTITUTIONS — WITH DEVASTATING EFFECTS

Diana Kwon | Nature | June 13, 2024

Last October, a cyberattack hit the Berlin Natural History Museum and brought research to a standstill. Scientists were left without access to the data and programs required for their work, putting projects on hold and leaving students in limbo. Months later, systems have only just begun to crawl back online. The museum is not alone. In the past year, cyberattacks have struck several research institutions in Germany and beyond. Most involve ransomware, in which data or systems are locked until a payment is made. The attacks are part of a growing trend at academic institutions worldwide, where they can have devastating effects — delaying research projects, disrupting student enrolment and affecting researchers' mental health. "In the 13 years I've been here, this is by far the most painful thing I have experienced," says Johannes Vogel, director-general of the Berlin Natural History Museum, which conducts research in a wide range of fields including paleontology, geology and genetics. "The attack is an ongoing challenge."

Read the full article here.

CHINA HAS BECOME A SCIENTIFIC SUPERPOWER

The Economist | June 12, 2024

In the atrium of a research building at the Chinese Academy of Sciences (CAS) in Beijing is a wall of patents. Around five metres wide and two storeys high, the wall displays 192 certificates, positioned in neat rows and tastefully lit from behind. At ground level, behind a velvet rope, an array of glass jars contain the innovations that the patents protect: seeds. CAS—the world's largest research organisation—and institutions around China produce a huge amount of research into the biology of food crops. In the past few years Chinese scientists have discovered a gene that, when removed, boosts the length and weight of wheat grains, another that improves the ability of crops like sorghum and millet to grow in salty soils and one that can increase the yield of maize by around 10%.

Read the full article here.

CHINA'S RISING LEADERSHIP IN GLOBAL SCIENCE

Renli Wu, Christopher Esposito, and James Evans | ARXIV | June 9, 2024

Major shifts in the global system of science and technology are destabilizing the global status order and demonstrating the capacity for emerging countries like China and India to exert greater influence. In order to measure changes in the global scientific system, we develop a framework to assess the hierarchical position of countries in the international scientific collaboration network. Using a machine-learning model to identify the leaders of 5,966,623 scientific teams that collaborated across international borders, we show that Chinese scientists substantially narrowed their leadership deficit with scientists from the US, UK, and EU between 1990 and 2023 in absolute terms. Consequently, China and the US are on track to reach an equal number of team leaders engaged in bilateral collaborations between 2027 and 2028. Nevertheless, Chinese progress has been considerably slower in per-collaborator terms: after adjusting for the number of non-leaders from each country, our models do not predict parity between the US and China until after 2087.

Read the full article here.

LAWMAKERS QUESTION OPTICS SOCIETY FOR USING ANONYMOUS DONATIONS FROM HUAWEI

Mitch Ambrose | American Institute of Physics (API) | May 22, 2024

The House Science Committee is questioning Optica, a professional society focused on optical science, for agreeing to let the Chinese telecommunications company Huawei anonymously finance a prize competition that supports early-career researchers. Committee leaders sent a letter to Optica CEO Liz Rogan last week probing the society's decision to not disclose the company's involvement in the competition to the public or to applicants, citing a May 2 article published by Bloomberg that revealed the arrangement. (Optica is an AIP Member Society and Rogan is on AIP's Board of Directors.) The annual competition was launched in 2022 by the society's charitable arm, the Optica Foundation, and provides $100,000 in seed funding to ten early-career professionals who are using optical sciences to address global challenges related to the environment, health, and telecommunications.

Read the full article here.

RESEARCH SECURITY POLICIES: AN OVERVIEW

Congressional Research Service | February 8, 2024

The international scientific community generally views the free and open exchange of information as vital to the process of scientific inquiry, including the vetting of ideas and the verification of research results. The U.S. research ecosystem broadly operates on these principles. Sources have documented a variety of mechanisms employed on behalf of foreign governments—most notably the People's Republic of China—to influence and exploit the openness of the U.S. research ecosystem. The acquisition of U.S. advances in science and technology, intellectual property, and talent by strategic competitors may pose a risk to U.S. national defense and global economic competitiveness. Congress and the executive branch have taken several actions to try to maintain the benefits of an open research ecosystem while attempting to protect it from external threats.

View the full resource here.

NSA CYBERSECURITY COLLABORATION CENTER

Ethan Bresnahan | The National Security Agency/Central Security Service (NSA/CSS)

The NSA Cybersecurity Collaboration Center (CCC) is how NSA scales intel-driven cybersecurity through open, collaborative partnerships. The CCC works with industry, interagency, and international partners to harden the U.S. Defense Industrial Base, operationalize NSA's unique insights on nation-state cyber threats, jointly create mitigations guidance for emerging activity and chronic cybersecurity challenges, and secure emerging technologies.

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute

UPCOMING RESEARCH SECURITY EVENTS

NCURA RESEARCH SECURITY SYMPOSIUM: BUILDING A PROGRAM RESPONSIVE TO REGULATORY REQUIREMENTS

Despite delays in the implementation of final guidance for National Security Policy Memorandum 33 and the resulting Research Security Program requirements, scrutiny of how research institutions conduct research, and particularly how that research is protected from unwanted foreign interference or theft, continues to grow in the U.S. and globally. This symposium will explore the current political environment and provide updates on upcoming regulatory changes that research institutions should consider. Whether your institution is research intensive and will have a federally mandated Research Security Program or a small primarily undergraduate institution, you will learn practices and strategies to assist in developing and improving research security at your institution.

- June 25, 2024
- Old Town, Alexandria, VA

View the full resource here.

TRADE SECRETS PROTECTION AND ENFORCEMENT PRACTICE IN CHINA

Trade secrets play an important role in firm competitiveness and strategic positioning, especially for startups and in research and development–intensive industries. Firms should actively prevent unauthorized disclosures of trade secrets. In case of a theft, they may need to pursue enforcement. Protecting trade secrets is an ongoing challenge for companies doing business in the United States and the People's Republic of China. Join us at United States Patent and Trademark Office (USPTO) headquarters in Alexandria, Virginia, for an examination of enforcement avenues against trade secret misappropriation in China.

- June 28, 2024
- United States Patent and Trademark Office, 600 Dulany Street, Alexandria, VA 22314

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute