RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE

THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary
August 15, 2024

UNIVERSITIES TURN TO PRIVATE INTELLIGENCE TO ASSESS CHINA RISK

David Matthews | Science|Business | August 6, 2024

Universities and research institutions are turning to private providers of information - some of them former US intelligence analysts – to understand whether their collaborations with China are risky. With China increasingly seen as an adversary in Europe and the US, universities are under pressure make sure their research links don't contribute to China's military, surveillance state, or give away sensitive technological knowhow. But with few China experts in universities, and limited public tools, private providers are springing up to fill the gap, claiming they can help universities better understand their risks – although some caution these services are no substitute for deep academic knowledge of the research in question. One such service is Data Abyss, run by a former US air force intelligence analyst, L J Eads, based in Dayton, Ohio. Eads has created multiple databases tracking collaborations with Chinese defence-related universities, plus one that looks at US funded research taking place in Russia. He paints a picture of universities that can barely keep track of who they are working with. "I have to ask [universities]: do you even know about some of these collaborations or joint ventures?," he told Science|Business.

Read the full article here.

MAJOR CHINESE HACKING GROUP 'ACTIVE TO THIS DAY' DESPITE US EFFORTS TO STOP THEM

Maggie Miller | Politico | August 9, 2024

The Biden administration has gone all out this year to warn China to back off its hacking campaigns on U.S. computer networks. China doesn't appear to be listening. While the U.S. usually is reticent to discuss cyberattacks or even directly assign blame to nation-states for hacks, it has been notably public in its censure of China since a Chinese-government-linked hacking group called Volt Typhoon was disclosed to be inside U.S. networks last year. At the same time, U.S. federal agencies and critical infrastructure companies have been racing to seal off key computer networks — like those undergirding power grids and transportation hubs — from the Volt Typhoon hackers. Cybersecurity experts working in the trenches, who are gathered in Las Vegas this week for the two largest hacking conferences of the year, say this massive effort to curb the attacks hasn't made a dent. "Volt Typhoon is active to this day," Sherrod DeGrippo, director of threat intelligence strategy at Microsoft, said on the sidelines of the BlackHat conference. "Have they stopped? Absolutely not. Will they stop? Doubt it."

Read the full article here.

AMERICAN SCIENCE SLIPS INTO DANGEROUS DECLINE, EXPERTS WARN, WHILE CHINESE RESEARCH SURGES

Saima S. Iqbal | Scientific American | August 7, 2024

In a first-ever "State of the Science" address at the end of June, National Academy of Sciences president Marcia McNutt warned that the U.S. was ceding its global scientific leadership to other countries—highlighting China in particular. McNutt, a widely respected geophysicist, said this slippage could make it harder for the U.S. to maintain the strength of its economy and protect its national security. She also laid out a provisional plan of action to reverse the decline. The June 26 speech served as a scientific parallel to the State of the Union address by the U.S. president and came from the chief of a body originally chartered to provide nonpartisan advice on science and technology to the nation's government. It surveyed the strengths and weaknesses of the current scientific landscape and underscored an urgent need for a new coordinated approach to research and development. "It's critically important we keep shouting [this message] from the rooftop," says Carrie Wolinetz, a science policy expert who has previously advised the White House and the National Institutes of Health.

Read the full article here.

NEW NSF BOARD CHAIR INTRODUCES VISION FOR A NATIONAL S&T STRATEGY

Clare Zhang | American Institute of Physics (AIP) | July 29, 2024

The National Science Foundation's board met last week for the first time since electing as its chair IBM executive Darío Gil, who used the occasion to reflect on the nearly 75 years since NSF's founding and share his vision for the next 75. He called for the U.S. to pursue a "cross-sectoral national strategy for science and technology" that maintains the creativity and resilience of the country's current decentralized science system yet is more responsive to "radical changes" underway across the global R&D landscape. These shifts include a "dramatic" rise in corporate funding of R&D relative to federal funding, China's emergence as both the biggest competitor and collaborator of the U.S. in science and technology, and weakness in STEM workforce development in the U.S. that amount to a "crisis," Gil said. These trends are highlighted in a policy brief the board released in conjunction with the speech.

Read the full article here.

SENATE WRAPPING UP SCIENCE BUDGET PROPOSALS

American Institute of Physics (AIP) | July 29, 2024

Senate appropriators will meet Thursday to advance their spending bills for the Department of Energy, Department of Defense, and National Institutes of Health, offering a fuller sense of their science priorities for the coming fiscal year. Last week, they released bills for NASA, the National Science Foundation, and the Commerce Department that seek higher budgets than those advanced by their counterparts in the House. For instance, the Senate bill seeks to increase NASA's Science Mission Directorate by 3.3% to $7.6 billion while the House proposes flat funding. The Senate bill also proposes to increase NSF by 5.4% to $9.6 billion while the House seeks a 2.2% increase. For details on other agencies, consult FYI's Federal Science Budget Tracker. Congress is unlikely to reach a final agreement on the budget until after the election in November, meaning all science agencies will start the new fiscal year in October on stopgap funding. Some of the main disagreements between Democrats and Republicans that are yet to be resolved are denoted in the statements of administration policy released by the White House.

Read the full article here.

SCIENTIST AT FOREFRONT OF US ARMY RESEARCH SELECTED TO LEAD PRC'S STRATEGIC CHIP PRODUCTION LINE

Sunny Cheung | The Jamestown Foundation | August 8, 2024

On July 30, the People's Republic of China (PRC) announced the establishment of its third-generation chip production line in Hong Kong (HKCNA, July 30). This represents a significant move that underscores Beijing's ambitions in the semiconductor industry. The new production line is spearheaded by renowned scientist Dr. Yitao Liao, who previously collaborated with the US Army on similar technologies. Both this new production line and Dr. Liao's involvement raise questions about US policies toward the security and supervision of research into dual-use technology amid ongoing US-PRC rivalry.

Read the full article here.

SILICON VALLEY STEPS UP STAFF SCREENING OVER CHINESE ESPIONAGE THREAT

Tabby Kinder, Stephen Morris, and Demetri Sevastopulo | The Financial Times | June 18, 2024

Silicon Valley companies are escalating their security vetting of staff and potential recruits as US officials voice greater concern about the threat of Chinese espionage. Technology giants such as Google and high-profile start-ups like OpenAI have stepped up their screening of personnel, according to several people working directly with the groups. The move comes amid fears that foreign governments are seeking to use compromised workers to access intellectual property and company data. Venture capital firms such as Sequoia Capital, which backs dozens of start-ups including Elon Musk's xAI, have also encouraged some portfolio companies to tighten staff vetting after warnings that spy agencies are targeting US tech developers, the people said. Sequoia split off its own Chinese business last year after almost two decades due to geopolitical pressure. Alex Karp, chief executive of Palantir, the $53bn data analytics contractor to the US defence industry, said Chinese spying on US tech companies was "a huge problem", especially for producers of enterprise software, large language models and weapons systems.

Read the full article here.

AI ON BOTH SIDES OF CYBERSECURITY: ALLY AND THREAT IN THE DIGITAL WORLD

BBVA | August 9, 2024

Imagine receiving an email notifying you of a temporary suspension of your bank account, another alerting you to an undelivered package, and a third proclaiming that you've won a gift card. Each message includes a link, urging you to provide your personal information. At first glance, these emails may appear legitimate, but they are, in fact, anything but. They are prime examples of social engineering—a sophisticated toolkit of manipulation tactics crafted to deceive individuals and extract sensitive information for illicit gain. With the advent of generative artificial intelligence, these deceptive strategies have not only proliferated but have also evolved in complexity, making them increasingly difficult to detect. Targeted phishing attacks, a widespread form of social engineering, traditionally required extensive research on the intended victim. This labor-intensive and costly process was largely manual, which naturally limited the frequency of such attacks. However, the emergence of generative artificial intelligence now enables the automation of these preparatory steps, allowing for the execution of targeted phishing campaigns on a massive scale. According to a report by the U.S. cybersecurity firm Zscaler, phishing attacks leveraging generative AI surged by 60% globally between January and December 2023.

Read the full article here.

NIH SUPPORTS OUR VALUED ASIAN AMERICAN, ASIAN IMMIGRANT AND ASIAN RESEARCH COLLEAGUES

National Institutes of Health (NIH) | August 15, 2024

Over the past several years, NIH has taken actions to address serious threats to the integrity of NIH-funded research. These actions have resulted in significant reductions in violations of peer review confidentiality, failures in reporting foreign employment and financial support, and failures in providing NIH with legally required access to records and scientific data from foreign subrecipients of primary grantees. Many of the concerning practices that NIH has attempted to address have originated from the government of the People's Republic of China (PRC). I recognize that certain government actions to protect against concerning activities by the PRC, (link is external) as recently reported by the Department of Homeland Security(link is external), have had the unintended consequence of creating a difficult climate for our valued Asian American, Asian immigrant and Asian research colleagues who may feel targeted and alienated.

Read the full article here.

THE HUMAN ELEMENT: THE KEY TO UNLOCKING ZERO-TRUST SECURITY

Francis Dinha | Forbes | August 15, 2024

As the CEO of OpenVPN Inc., I've seen firsthand the evolution of cybersecurity and the growing importance of zero trust. This framework, with its "never trust, always verify" mantra, has revolutionized how organizations protect their valuable data and assets. However, in our pursuit of technical safeguards, we often overlook a crucial element: the human factor. No matter how many technical systems and tools we put in place, there will always be humans who use those tools.

Read the full article here.

THE CHINESE COMMUNIST PARTY (CCP): A QUEST FOR DATA CONTROL

The CIS Cyber Threat Intelligence (CTI) Team | The Center for Internet Security, Inc. (CIS)
August 14, 2024

The CIS CTI team assesses that apps owned by the People's Republic of China (PRC) pose a threat to users because of the PRC's ability to leverage these apps for data collection and malign influence operations. Data control is central to the Chinese Communist Party's (CCP's) quest for digital and technological dominance on the world stage. This pursuit is supported by PRC laws granting the CCP the authority to collect data from Chinese companies. Given the popularity of these apps globally, and especially among American users, the CCP likely views the data stored within apps like TikTok, Shein, and Temu as an important resource for their data control goals.

Read the full article here.

USEFUL RESOURCES

CHINA'S GLOBAL CHALLENGE TO DEMOCRACY

National Endowment for Democracy (NED)

A Curated List of Material on China's Global Challenge to Democracy from the International Forum for Democratic Studies and Journal of Democracy.

View the full resource here.

UYGHUR FORCED LABOR PREVENTION (UFLPA) ENTITY LIST

U.S. Department of Homeland Security | August 9, 2024

The U.S. Department of Homeland Security (DHS), as the Chair of the Forced Labor Enforcement Task Force (FLETF), announces the publication and availability of the updated Uyghur Forced Labor Prevention Act (UFLPA) Entity List, a consolidated register of the four lists required to be developed and maintained pursuant to the UFLPA, on the DHS UFLPA website.

View the full resource here.

NIH DECISION MATRIX FOR ASSESSING POTENTIAL FOREIGN INTERFERENCE FOR COVERED INDIVIDUALS OR SENIOR/KEY PERSONNEL

National Institutes of Health (NIH)

NIH presents its Decision Matrix for Assessing Potential Foreign Interference as part of its ongoing efforts to be transparent about its policies and procedures. The Decision Matrix is based on the NIH Grants Policy Statement (GPS), NSPM-33, NSPM-33 Implementation Guidance, and 2 CFR 200.206.

View the full resource here.

BIS PUBLISHES NEW EXPORT CONTROL COMPLIANCE RESOURCES FOR THE ACADEMIC COMMUNITY

U.S. Department of Commerce Bureau of Industry and Security (BIS) | August 14, 2024

Today, the Department of Commerce's Bureau of Industry and Security (BIS) Export Enforcement published new resources for the academic community: a compliance note on voluntary self-disclosure trends and a compendium of export compliance resources. These resources align with BIS's ongoing commitment to support academic institutions in their efforts to comply with export controls.

Read the full article here.