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

Open Source Media Summary

February 8, 2024

CONGRESS WANTS TO BAN CHINA'S LARGEST GENOMICS FIRM FROM DOING BUSINESS IN THE U.S. HERE'S WHY.

Ken Dilanian | NBC News | January 25, 2024

Bipartisan legislation was introduced in both houses of Congress Thursday that would effectively ban China's largest genomics company from doing business in the U.S., after years of warnings from intelligence officials that Beijing is gathering genetic information about Americans and others in ways that could harm national security. The bills, backed by leaders of the House Select Committee on the Chinese Communist Party and the Senate Homeland Security Committee, target BGI, formerly known as Beijing Genomics Institute, which in 2021 was blacklisted by the Pentagon as a Chinese military company. Five company affiliates also have been sanctioned by the Commerce Department, which accused at least two of them of improperly using genetic information against ethnic minorities in China. In an exclusive interview with NBC News, Rep. Mike Gallagher, R-Wis., and Rep. Raja Krishnamoorthi, D-Ill., said their legislation would ban BGI — or any company using its technology — from federal contracts, a move the company said in a statement would "drive BGI from the U.S. market."

Read the full article here.

WHO SHOULD LEAD EFFORTS TO SAFEGUARD US RESEARCH COLLABORATION ABROAD?

Hoover Institution | January 31, 2024

1. A visiting scholar from China who sought help from an American research university to develop swarms of offensive drones that could attack and overwhelm an aircraft carrier.
2. A partnership between U.S. and Chinese university researchers aimed at developing artificial intelligence (AI) technology that can guide the atmospheric reentry of hypersonic vehicles.
3. A partnership between the United States and China with the purpose of leveraging AI to enhance the acoustic detection of submarines in bodies of water surrounding Asia.

All these technological research projects have actually occurred or been proposed— despite the glaring US national security risks they pose and without proper regulatory oversight and the application of appropriate security measures. It's exactly these sorts of scenarios that participants in the Pacific regional meeting of the National Science, Technology, and Security Roundtable, by the Hoover Institution, Stanford University, and the National Academy of Sciences on January 23 and 24, discussed how to best avoid. For much of the two-day meeting, scholars, government representatives, and industry leaders addressed how best to safeguard academic research from malign foreign influence, theft, and manipulation while encouraging academics to continue to participate in valuable international research collaborations.

Read the full article here.

CHINESE HACKERS PREPARING TO 'WREAK HAVOC' ON AMERICAN CITIZENS, COMMUNITIES, FBI DIRECTOR WARNS

Greg Norman | Fox News | January 31, 2024

FBI Director Christopher Wray warned lawmakers on Capitol Hill Wednesday that Chinese hackers are preparing to "wreak havoc and cause real-world harm to American citizens and communities." Wray and other government officials are testifying in front of the House Select Committee on the Chinese Communist Party for a hearing titled "The Chinese Community Party Cyber Threat to the American Homeland and National Security." "There has been far too little public focus on the fact that PRC [People's Republic of China] hackers are targeting our critical infrastructure – our water treatment plants, our electrical grid, our oil and natural gas pipelines, our transportation systems. And the risk that poses to every American requires our attention now," Wray told lawmakers. "China's hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities, if and when China decides the time has come to strike," he added.

Read the full article here.

CHINA'S HACKERS ARE PREPARING TO 'WREAK HAVOC' AND 'CAUSE REAL WORLD HARM' TO AMERICANS: FBI DIRECTOR

Luke Barr | ABC News | January 31, 2024

China's hackers are preparing to "wreak havoc" and "cause real-world harm" to Americans, FBI Director Christopher Wray will warn in congressional testimony submitted on Wednesday. Director Wray, along with U.S. Cyber Command Cmdr. Gen. Paul Nakasone, Department of Homeland Security Cybersecurity and Infrastructure Security Agency Director Jen Easterly and Harry Coker, the director of the National Cyber Director office, will be testifying in front of the House Select Committee on the Chinese Communist party. "There has been far too little public focus on the fact that PRC hackers are targeting our critical infrastructure -- our water treatment plants, our electrical grid, our oil and natural gas pipelines, our transportation systems. And the risk that poses to every American requires our attention -- now," Wray says in selected testimony released by the FBI ahead of the hearing.

Read the full article here.

GSA TECH PURCHASE: INSPECTOR GENERAL REVEALS UNAUTHORIZED CHINESE CAMERAS WITH SECURITY FLAWS

Peter Sucie | Clearance Jobs | January 29, 2024

An internal audit conducted by the Office of the Inspector General of the U.S. General Service Administration (GSA) found this month that the agency had purchased and then used Chinese-manufactured videoconference cameras. Since these cameras were manufactured in China, they were not compliant with the Trade Agreements Act of 1979 (TAA). The IG was warned in 2022 that the purchase and use had occurred, resulting in the recently completed audit. "GSA Office of Digital Infrastructure Technologies (IDT) employees misled a contracting officer with egregiously flawed information to acquire 150 Chinese-made, TAA-noncompliant videoconference cameras. Before completing the purchase, the contracting officer requested information from GSA IDT to justify its request for the TAA-noncompliant cameras, including the existence of TAA-compliant alternatives and the reason for needing this specific brand.

Read the full article here.

DEFENSE DEPARTMENT LISTS DOZENS OF CHINESE MILITARY COMPANIES OPERATING IN U.S.

Mike Heuer | United Press International (UPI) | January 31, 2024

China has 46 military companies plus subsidiaries operating within the United States while disguised as civilian entities, the U.S. Department of Defense announced Wednesday. The updated list is part of "an important continuing effort in highlighting and countering [China's] Military-Civil Fusion strategy" that "supports the modernization goals of the People's Liberation Army by ensuring it can acquire advanced technologies and expertise developed by [Chinese] companies, universities and research programs that appear to be civilian entities," the DOD said in a news release. Among them are prominent names, such as the Huawei Investment & Holdings Company that owns Huawei Technologies Company, and Semiconductor Manufacturing International Corporation (SMIC), which has seven subsidiaries listed along with the parent corporation.

Read the full article here.

PENTAGON CALLS OUT CHINESE COMPANIES IT SAYS ARE HELPING BEIJING'S MILITARY

Idrees Ali, Alexandra Alper, and Michael Martina | Reuters | February 1, 2024

The United States on Wednesday added more than a dozen Chinese companies to a list created by the Defense Department to highlight firms it says are allegedly working with Beijing's military, as part of a broader effort to keep American technology from aiding China. New additions to the list, opens new tab, first reported by Reuters, were posted on the Department of Defense website and include memory chip maker YMTC, artificial intelligence company Megvii, lidar maker Hesai Technology and tech company NetPosa. Amid strained ties between the world's two biggest economies, the updated list is one of numerous actions Washington has taken in recent years to highlight and restrict Chinese companies that is says may strengthen Beijing's military. A spokesperson for the Chinese embassy in Washington said China opposed the move and called it an abuse of state power, adding that it ran counter to the U.S.'s "alleged commitment to market competition and international fair trade."

Read the full article here.

NEW SECURITY MEASURES CURTAILING THE STUDY OF CHINA ALARM EDUCATORS

Jordyn Haime | China File | February 2, 2024

Late last year, The New York Times reported on a new state-level bill in Florida that was creating unintended consequences for prospective Chinese graduate students. The bill restricts universities from accepting grants from or participating in partnerships with seven "countries of concern," including China. Now, it is creating confusion among Florida universities unsure where Chinese graduate students fall under the confines of that law. It may have already succeeded in scaring off talented students who could make important research contributions, and universities have refrained from making offers until the law is clarified, the Times reported. It's not just Florida. Several states, including Texas, Louisiana, Ohio, and Montana, have pursued laws aiming to limit foreign influence, particularly from the Chinese Communist Party (CCP), by specifically targeting exchange and cooperation with students, researchers, and academic institutions.

Read the full article here.

WEAK POINT: FEDS MUST STOP OUTSOURCING RESEARCH SECURITY TO UNIVERSITIES

Paul Moore | The Hill | February 2, 2024

Willie Sutton, the fabled bank robber, supposedly explained that he robbed banks "because that's where the money is." Like Sutton, China's communist regime has targeted America's research universities because that's where much of our cutting edge research product is found. America's research enterprise, developed at universities and funded through federal research grants, remains highly vulnerable to malign foreign influence operations, according to warnings from Congress, the FBI and the Government Accountability Office. Taxpayer investments in university research programs are vast. In Fiscal 2022 nearly $55 billion in federal taxpayer dollars made up 55 percent of total university research expenditures to develop emerging technologies in aerospace, biomedical, chemical, mechanical and metallurgical engineering, and other sciences.

Read the full article here.

CANADA NEEDS TO BE ONE STEP AHEAD OF CHINA ON RESEARCH SECURITY

Alex Joske and Margaret Mccuaig-Johnston | The Globe and Mail | February 1, 2024

For years, China has cast itself as a scientific powerhouse – but the reality is that a great deal of its innovation has come from collaboration with scientists from other countries. The country's military modernization and its interest in harnessing its research sector in service of its strategic ambitions has made that spirit of collaboration fraught, with China's defence complex effectively using the West's open education system to accumulate know-how and technology. The integration of China's universities with its military and intelligence apparatus has reached new heights under Xi Jinping. More than a hundred Chinese universities have the credentials to carry out classified research; last year, McGill University professor Benjamin Fung described efforts by the Chinese government to offer Canadian academics lucrative deals to operate under Beijing's thumb. Human rights abuses, such as the genocide of Uyghurs as recognized by Canada's Parliament, are being executed with technologies based on research done at non-Chinese universities.

Read the full article here.

CHINESE FM ACCUSES US OF POLITICIZING ACADEMIC RESEARCH, DAMAGING PEOPLE-TO-PEOPLE EXCHANGES

Global Times | January 31, 2024

China has made solemn démarches to the US, and accuses it politicizing and weaponizing academic research, and overstretching the concept of national security to wantonly suppress and ill-treat Chinese students. Such moves undermine Chinese citizens' lawful rights and interests and basic human rights, cause the chilling effect and sour the atmosphere for China-US people-to-people exchanges, Chinese Foreign Ministry spokesperson Wang Wenbin said on Wednesday, in response to the revelation that some Chinese students had experienced unwarranted harassment and even deportation at the US border. Some Chinese students with valid visas to enter the US were subjected to unwarranted interrogation and harassment, and some were deported at Washington Dulles International Airport, according to media reports. Chinese individuals, including students, have been denied entry into the US in recent months, despite having valid visas, clean records and legitimate reasons for their travel.

Read the full article here.

CANADA WAKES UP TO CHINA, RUSSIA, IRAN THREAT TO INTELLECTUAL PROPERTY

Christopher Burgess | CSO Online | January 29, 2024

Restricting foreign involvement in government-funded research, Canada has made a start toward protecting intellectual property from malign nation-states, but there's more to be done. It is as if a light went on within the Canadian government this month as it took steps to tighten control over the risk presented by China, Russia, and Iran to sensitive research being funded by the federal government. With its "New Policy on Sensitive Technology Research and Affiliations of Concern," Canada named more than 100 entities, all of which fall under the rubric of presenting a high risk to the country's national security. The policy includes documents that inform research entities desiring government funding around sensitive technology areas that there are new swim lanes in effect.

Read the full article here.

RUSSIAN SPIES IMPERSONATING WESTERN RESEARCHERS IN ONGOING HACKING CAMPAIGN

Alexander Martin | The Record | February 1, 2024

Hackers working for Russia's intelligence services are impersonating researchers and academics in an ongoing campaign to gain access to their colleagues' email accounts, according to messages and files seen by Recorded Future News and independently analyzed by two cybersecurity companies. Keir Giles, the British author of "Russia's War on Everybody" and a consulting fellow at the Chatham House think tank, shared with Recorded Future News several suspect emails sent by accounts purporting to be fellow researchers. Other correspondence we have seen shows multiple researchers who did not consent to being identified in this report also being targeted over the past three months.

Read the full article here.

HACKERS PUSH USB MALWARE PAYLOADS VIA NEWS, MEDIA HOSTING SITES

Bill Toulas | Bleeping Computer | January 31, 2024

A financially motivated threat actor using USB devices for initial infection has been found abusing legitimate online platforms, including GitHub, Vimeo, and Ars Technica, to host encoded payloads embedded in seemingly benign content. The attackers hide these payloads in plain sight, placing them in forum user profiles on tech news sites or video descriptions on media hosting platforms. These payloads pose no risks to users visiting these web pages, as they are simply text strings. However, when integrated into the campaign's attack chain, they are pivotal in downloading and executing malware in attacks. The hackers responsible for this campaign are tracked by Mandiant as UNC4990 and have been active since 2020, predominately targeting users in Italy.

Read the full article here.

USEFUL RESOURCES

CHINA & THE US: SAFEFUARDING OPEN RESEARCH AGAINST AUTHORITARIAN RIVALS

Policy Ed

Distinguished Research Fellow, Glenn Tiffert, warns that the Chinese government strategically exploits the openness of American scientific research to advance its own interests, oftentimes at odds with those of the United States. Intellectual property theft and exposure of state secrets are a significant concern. Rather than enact broad restrictions against working with China, however, the United States must remain an open society and, instead, be more thorough in vetting its partners and use data-based risk assessments to secure the integrity of our research.

View the full resource here.

HEARING ON EMERGING TECHNOLOGIES AMID U.S.-CHINA COMPETITION

C Span | February 1, 2024

The U.S.-China Economic and Security Review Commission held a hearing on current and emerging technologies that are affecting U.S.-China competition. Topics included supply chains for commercial development and military use, the use of artificial intelligence in biotechnology and biological warfare, and electric vehicle production.

Read the full article here.

THREATS TO THE U.S. RESEARCH ENTERPRISE: CHINA'S TALENT RECRUITMENT PLANS

U.S. Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs

American taxpayers contribute over $150 billion each year to scientific research in the United States. Through entities like the National Science Foundation, the National Institutes of Health and the Department of Energy's National Labs, taxpayers fund innovations that contribute to our national security and profoundly change the way we live. America built this successful research enterprise on certain values: reciprocity, integrity, merit-based competition, and transparency. These values foster a free exchange of ideas, encourage the most rigorous research results to flourish, and ensure that researchers receive the benefit of their intellectual capital. The open nature of research in America is manifest; we encourage our researchers and scientists to "stand on the shoulders of giants." In turn, America attracts the best and brightest.

Read the full article here.

2023 COST OF INSIDER RISKS GLOBAL REPORT

Ponemon Institute & DTEX | January 2024

The upward trends associated with incident costs, frequency, and time to contain demonstrate that current approaches to insider risk are simply not working. In fact, the numbers clearly show we are going backwards. Funding is being inadvertently misdirected due in part to a widespread misunderstanding of insider risks and how they manifest based on early warning behaviors. A whole-of-industry approach is required to educate and find common ground on how we define and discuss insider risks with enterprise and government entities. On a positive note, more and more organizations are building insider risk programs and seeking budget and executive buy-in to fund and champion them. Our research echoes similar findings from other leading analysts and research organizations, notably Forrester, Gartner, MITRE Corporation and Verizon.

Read the full article here.

PROTECTIVE SECURITY

National Protective Security Authority | Trusted Research

The UK has a thriving research and innovation sector that attracts investment from across the world. Trusted Research aims to secure the integrity of the system of international research collaboration, which is vital to the continued success of the UK's research and innovation sector.

Read the full article here.

INTELLIGENCE DELIVERED: A CONVERSATION WITH GENERAL PAUL NAKASONE

National Security Agency | YouTube Agency | February 1, 2024

General Paul M. Nakasone concludes his tenure as Director of the National Security Agency on February 2, 2024. In this retrospective conversation, he reflected on his nearly six years as Director, covering topics ranging from election security to AI to his proudest moment.

Read the full article here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute