RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE

THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary

February 1, 2024

WHY IS THE PENTAGON ENABLING CHINA'S THEFT OF AMERICA'S TECH? | OPINION

Gordan G. Chang | Newsweek | January 22, 2024

Last month, Newsweek reported that the Department of Defense had funded a Chinese-born researcher, Song-Chun Zhu, who at the time was openly transferring sensitive technologies to Chinese institutions, including those relating to artificial intelligence with military implications. It was just the latest sign that China's espionage has reached crisis proportions. "The U.S. government estimates that China's intellectual-property theft costs America as much as $500 billion a year," wrote John Ratcliffe while serving as director of national intelligence in December 2020. He titled his Wall Street Journal piece "China Is National Security Threat No. 1." There has been over the course of decades a fundamental failure to prevent researchers in America from helping China develop military technologies, especially AI. While working in the United States and funded by the Pentagon, Zhu was a member of the Chinese central government's "Thousand Talent Plan," designed to transfer critical technologies to China. Zhu, according to Newsweek, "effectively trained a generation of students from China, with many returning there to work in top laboratories, universities, or companies that often were connected to Zhu or to other top scientists."

Read the full article here.

INSULATING OURSELVES FROM CHINESE TECH AND TALENT WILL STIFLE AMERICAN INDUSTRY | OPINION

David P. Goldman | Newsweek | January 19, 2024

Last November, Newsweek uncovered $30 million in federal research grants which had gone to Chinese AI researcher Song-Chun Zhu, who had received National Science foundation and Defense Department funding while working for Chinese institutions with reported ties to the Chinese military. The exposé led to an inquiry by several House committees, announced on Jan. 17. I won't second-guess the House investigators or pre-judge the case, but the Zhu affair points to a much bigger problem: China already has decisive advantages in critical data and their application to Artificial Intelligence, making it hard for American researchers to eschew collaboration with China in key fields like medical research and industrial automation. China now graduates more engineers and computer scientists than the rest of the world combined, and it's hard to conduct AI research without Chinese researchers. Trickiest of all is that China—in sharp contrast to the United States—steers its top computer science graduates toward its military industry. The most qualified Chinese specialists are likeliest to have military ties.

Read the full article here.

US-CHINA SCIENCE DEAL MUST ADDRESS AMERICAN NATIONAL SECURITY CONCERNS: SENIOR STATE DEPARTMENT OFFICIAL

Khushboo Razdan | South China Morning Post | January 24, 2024

The future of a seminal US-China science deal depends on both sides agreeing on new stronger terms to address Washington's national security concerns, a top government official negotiating the pact said, amid calls from American academics for its renewal. Washington's posture going into the talks was to bolster the US-China Science and Technology Cooperation Agreement "to have it be more robust, to have the guardrails be more firm and more clear", according to Jason Donovan, director of science and technology cooperation at the US State Department. An amended STA must ensure "fewer opportunities" for any activity compromising US national interests, he said in response to a question from the Post at a National Science, Technology and Security Round-table meeting at Stanford University in California. "If we are able to do that in negotiations, we will do so. If we're unable to do that, we won't do so," Donovan added.

Read the full article here.

AUSTRALIA RISKS FALLING BEHIND ALLIES ON RESEARCH SECURITY. WILL IT TAKE A SPY SCANDAL IN OUR UNIVERSITIES TO CATCH UP

Jon Callow | The Conversation | January 22, 2024

Late last year, a PhD student named Yuekang Li was refused a study visa to enter Canada. Why? Canada's Federal Court was concerned he could be "targeted and coerced into providing information that would be detrimental to Canada". Li wasn't the only one. Earlier this month, Iranian computer engineering student Reza Jahantigh was denied a visa to study his PhD in Canada, because of his previous service in the Iranian military. Some observers have called the decisions "deeply unhelpful", and said they risked the prospects of future international students coming to Canada. Despite such criticisms, Canada is at the forefront of an international charge for stricter "research security" – the idea of protecting certain university courses and research programs from espionage, foreign interference and technology theft. While countries including the United States, the United Kingdom and the Netherlands are moving swiftly to make their research more secure, Australia lags behind. And our need for research security is only set to grow.

Read the full article here.

VENTURE CAPITAL AND SUPPLY CHAIN VULNERABILITIES

National Counterintelligence and Security Center

One of the most potentially damaging vulnerabilities to a company comes in the form of a foreign adversary masquerading as a private investor. Whether seed money for early stage, highrisk start-ups, or an engine of pivotal middle market transformation, venture capital (VC) investors may provide the extra financial boost that a company needs to succeed. VC investors often gain a substantial foothold in a company through investment opportunities including capital expenditures (e.g. land and/or equipment purchases), or other operational or financial improvements to achieve growth. These investments may appear limited or are otherwise masked in a way that would not raise any alarms. However, these seemingly nonthreatening transactions give foreign adversaries the opportunity to quietly insert board members, secure voting rights and/or access sensitive corporate data. They can then lie in wait for the right time to perform a sleight of hand that advances the interests of the foreign adversary, at the expense of the company and also, possibly, to U.S. economic or national security.

Read the full article here.

FEDERAL WORKFORCE: ACTIONS NEEDED TO IMPROVE THE TRANSFER OF PERSONNEL SECURITY CLEARANCES AND OTHER VETTING DETERMINATIONS

U.S. Government Accountability Office | January 22, 2024

The government's security clearance and other "personnel vetting" processes help ensure that federal employees are trustworthy. Personnel vetting decisions are supposed to be reciprocal: if one agency clears an employee, that employee should be able to transfer to another agency without a new background check. But the Offices of Personnel Management and the Director of National Intelligence—who oversee the vetting processes—don't have good data on how often this works. We recommended addressing this and other challenges, such as agency access to a classified IT system. The personnel security clearance process is on our High Risk List.

What GAO Found
The Office of the Director of National Intelligence (ODNI) and the Office of Personnel Management (OPM)—two agencies with key personnel vetting oversight responsibilities—do not have reliable data on the extent to which agencies have honored previously granted vetting determinations, known as reciprocity.

Read the full article here.

NORTH KOREAN TACTICS, TECHNIQUES, AND PROCEDURES FOR REVENUE GENERATION

National Counterintelligence and Security Center | January 24, 2024

North Korea is evading US and UN sanctions by targeting private companies to illicitly acquire income and fund the regime's priorities, including its WMD and ballistic missile programs. This product provides an overview of the common tactics, techniques, and procedures (TTPs) North Korean cyber actors use to target and gain access to financial institutions and entities associated with cryptocurrency for cyber exploitation and revenue generation. In addition, this product provides mitigation measures to identify and deter North Korean IT workers deployed worldwide who pose as other nationalities to gain employment. North Korea's cyber actors employ a range of tactics in their operations to further their larger espionage and financial goals.

Read the full article here.

FEDERAL AGENCIES DON'T TRUST EACH OTHER'S SECURITY CLEARANCES

Molly Weisner | Federal Times | January 23, 2024

More than half of federal agencies don't trust each other to properly vet security clearances for employees transferring between departments, according to a survey by an independent government watchdog. Though agencies are bound by the same rules when it comes to evaluating employees for a security clearance, the Government Accountability Office found that many agencies feel the need to double-check an existing clearance. That risks duplicative work and prolonging the process for government employees awaiting approval to work in classified environments. "Of the 31 agencies we surveyed, respondents for 17 stated that they, at times, do not trust other agencies' security clearance process, which can affect their decisions to grant reciprocity," according to the GAO report published Monday.

Read the full article here.

CHINESE-MANUFACTURED DRONES 'POSE A SIGNIFICANT RISK TO CRITICAL INFRASTRUCTURE AND U.S. NATIONAL SECURITY,' DHS AND FBI WARN

Luke Barr | ABC News | January 17, 2024

The Department of Homeland Security's cyber agency and the Federal Bureau of Investigation are warning that Chinese-manufactured drones "pose a significant risk to critical infrastructure and U.S. national security," and could steal American data, according to a public service announcement released on Wednesday. DHS' Cybersecurity and Infrastructure Security Agency (CISA) and the FBI say that because of Chinese law that allows for the government to access data held by private firms, American data that's connected to drones could be at risk. "The use of Chinese-manufactured UAS requires careful consideration and potential mitigation to reduce risk to networks and sensitive information," the document read.

Read the full article here.

WASHINGTON EYES GIVING NEW SPY POWERS TO COMMERCE DEPARTMENT

Ryan Lovelace | The Washington Times | January 26, 2024

It's not just about business anymore.

Efforts to transform the Commerce Department into America's "19th intelligence agency" are quietly under consideration in Washington as lawmakers and Biden administration officials struggle to find new tools to stop the loss of strategic technology and intellectual property to China and other U.S. adversaries. Policymakers have discussed housing a new intelligence unit inside the Commerce Department, a long-term second-tier player in the Cabinet pecking order with the lead responsibility for export controls and foreign investment screening that supporters say will be crucial to the country's growth.

Read the full article here.

POISONED AI WENT ROGUE DURING TRAINING AND COULDN'T BE TAUGHT TO BEHAVE AGAIN IN 'LEGITIMATELY SCARY' STUDY

Keumars Afifi-Sabet | LiveScience | January 26, 2024

AI researchers found that widely used safety training techniques failed to remove malicious behavior from large language models — and one technique even backfired, teaching the AI to recognize its triggers and better hide its bad behavior from the researchers. Artificial intelligence (AI) systems that were trained to be secretly malicious resisted state-of-the-art safety methods designed to "purge" them of dishonesty, a disturbing new study found.

Read the full article here.

USEFUL RESOURCES

NSF RESEARCH SECURITY TRAINING MODULES NOW AVAILABLE

U.S. National Science Foundation | January 30, 2024

The U.S. National Science Foundation is pleased to announce the launch of four interactive online research security training modules, now available to researchers and institutions across the U.S. These modules are designed to facilitate principled international collaboration in an open, transparent and secure environment that safeguards the nation's research ecosystem. Fueled by the "CHIPS and Science Act of 2022," these training modules signify a major first step in reconciling the needs of the research, law enforcement and intelligence communities to pursue trusted relationships in the global research community while minimizing economic and security risks. They provide researchers with clear guidelines and effective strategies to protect against existing and emerging research security threats.

View the full resource here.

SEVEN SONS OF NATIONAL DEFENCE (国防七子) TRACKER

Data Abyss

The Seven Sons of National Defence (国防七子) is a grouping of the public universities affiliated with the Ministry of Industry and Information Technology of China. They are widely believed to have close scientific research partnerships and projects with the People's Liberation Army. SOURCE

- Three quarters of university graduates recruited by defense related state-owned enterprises in China come from the Seven Sons.
- The Seven Sons devote at least half of their research budgets to military products.
- According to the Hoover Institution, the Seven Sons "operate as prime pathways for harvesting US research and diverting it to military applications."
- In 2020, the United States government banned students from the Seven Sons schools to study in graduate programs in the United States.

View the full resource here.

NATIONAL OPERATIONS SECURITY (OPSEC) AWARENESS MONTH

National Counterintelligence and Security Center | January 2024

January is National Operations Security (OPSEC) Awareness Month. WHAT IS OPSEC? A security discipline designed to deny adversaries the ability to collect, analyze, and exploit information that might provide an advantage against the United States by preventing inadvertent compromise of critical information. This is done through a process of continual assessment that identifies and analyzes critical information, vulnerabilities, risks and external threats.

View the full resource here.

ORGANIZATION OF THE AVIATION INDUSTRY CORPORATION OF CHINA (AVIC)

J.J. Long, Thomas Corbett, and Dan Shats | Air University | January 22, 2024

Established in 1951, the Aviation Industry Corporation of China (AVIC) is China's largest aviation enterprise, responsible for producing essentially all of China's domestic military aircraft, UAVs, and helicopters, as well as a wide range of civilian aircraft and other aviation and non-aviation products and services. From a U.S. perspective, AVIC can be thought of as if Lockheed Martin, Northrup Grumman, Sikorsky, at least parts of Boeing and Raytheon, and essentially all other domestic aviation companies were all subsidiaries of a single corporation, which also was heavily invested in automobiles, commodities, insurance, finance, and a range of other schemes.

View the full resource here.

UK FUNDED CHINESE DEFENSE RESEARCH TRACKER

Data Abyss

The "UK Funded Chinese Defense Research Tracker" is a specialized tool designed to monitor and provide transparency regarding research activities funded by the United Kingdom 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 UK-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.

PROTECT YOURSELF: COMMERCIAL SURVEILLANCE TOOLS

The National Counterintelligence and Security Center (NCSC)

Companies and individuals have been selling commercial surveillance tools to governments and other entities that have used them for malicious purposes. Journalists, dissidents, and other persons around the world have been targeted and tracked using these tools, which allow malign actors to infect mobile and internet-connected devices with malware over both WiFi and cellular data connections. In some cases, malign actors can infect a targeted device with no action from the device owner. In others, they can use an infected link to gain access to a device.

View the full resource here.

THE US IS HAMSTRINGING ITSELF IN ITS SPY WAR WITH CHINA

Douglas London | The Hill | January 42, 2024

FBI Director Christopher Wray routinely warns of the near apocalyptic threats and consequences from Beijing's massive counterintelligence campaign. China's spying aims to secure the military advantage observers caution might enable it to prevail in a war with the U.S. — a war that is likely to incur unprecedented American casualties.

View the full resource here.

BIG QUESTION: HOW DOES DIGITAL PRIVACY MATTER FOR DEMOCRACY AND ITS ADVOCATES?

Amaris Rancy, Maya Recanati and Beth Kerley | National Endowment for Democracy |January 22, 2024

Emerging technologies are creating new digital privacy risks that can undermine key democratic values and practices. For example, generative AI tools simultaneously increase incentives for data collection and accelerate authoritarian influence operations; 5G networks enable more and more devices to join the Internet of Things (IoT); and immersive technologies such as augmented and virtual reality collect unprecedented types of information on users. Amid this rapidly changing landscape, authoritarian actors like China are exporting surveillance technologies that enable mass data collection and processing to democracies and autocracies alike, impacting the work and safety of democratic activists and creating risks for everyday citizens. There is not yet a shared understanding of digital privacy's implications for democracy, particularly across varying political and legal contexts. While the EU's landmark General Data Protection Regulation (GDPR) has set a legal benchmark for data privacy in many global settings, enforcement challenges and the evolving nature of digital technologies themselves leave many fundamental questions in this space unresolved.

View the full resource here.

HOW WILL GEOPOLITICAL TENSIONS IMPACT ON EUROPEAN RESEARCH?

Jan Palmowski | National Endowment for Democracy | January 26, 2024

The European Commission's sweeping proposals on Economic Security, published 24 January, address key concerns for researchers around international collaboration, academic freedom, and the purpose of EU-funded research and innovation. Universities must engage with these proposals with determination and confidence. In the Proposal for a Council Recommendation on enhancing research security, the Commission proposes political guidance to member states on how to work with universities and research organisations to prevent R&I being abused for military or other unintended purposes by foreign actors. It is a very carefully worded document which underlines the importance of academic freedom and institutional autonomy.

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute

EVENTS OF NOTE

2024 ASCE ANNUAL SEMINAR TO BE HELD MARCH 4-8, AT TEXAS A&M UNIVERSITY

Now in its eighth year, the annual ASCE Seminar has become the premier event for training, networking, and collaboration specifically targeted at the academic research enterprise. For ASCE 2024, we expect over 400 participants from various federal agencies, more than 150 universities, and 15 countries.

View the full resource here.

THE DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DCSA) 2024 VIRTUAL DCSA SECURITY CONFERENCE FOR INDUSTRY TO BE HELD FEBRUARY 28-29, 2024

This virtual event will provide Industry Security Professionals timely and relevant information about the rapidly changing security landscape. The agenda will cover topics such as DD254s, Facility Clearance Process, CUI, Cyber Program and Capabilities, Personnel Security, panel discussions at the end of each day, and more!

View the full resource here.

REGISTRATION OPEN FOR DARPA DISCOVERY EVENT IN SAN FRANCISCO TO BE HELD FEBRURY 21-22, 2024

The Defense Advanced Research Projects Agency (DARPA) is hosting an in-person gathering in San Francisco Feb. 21-22 to engage with science and technology companies, universities, and other research and engineering organizations interested in exploring scientific areas ripe for disruption. The event, called Discover DSO Day (D3), is sponsored by DARPA's Defense Sciences Office (DSO), whose goal is to identify and pursue high-risk, high-payoff research initiatives across a broad spectrum of science and engineering disciplines and transform them into important, new game-changing technologies for U.S. national security.

View the full resource here.