ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

February 23, 2023

U.S. OUTBOUND INVESTMENT INTO CHINESE AI COMPANIES

Emily S. Weinstein and Ngor Luong | Center for Security and Emerging Technology | February 2023

Policymakers in the United States and abroad are increasingly concerned about the national security implications associated with outbound investment, and some in Washington are advocating for a potential outbound investment security review or regime to address the national security risks associated with outgoing U.S. capital. This policy brief analyzes data from Crunchbase on U.S. outbound investment into Chinese artificial intelligence companies between 2015 and 2021 to better understand the scope and nature of these transactions. This report aims to identify: 1) the main U.S. investors active in the Chinese AI market, and 2) the set of AI companies in China that benefitted from U.S. capital during this period. It also lays out potential implications and next steps for U.S. policy. Our key findings include the following: Chinese investors remain the dominant investors in Chinese AI companies. Between 2015 and 2021, at least 71 percent of the transaction value and 92 percent of the investment transactions with no U.S. participation came from Chinese investors alone. Based on available data in Crunchbase, between 2015 and 2021, 167 U.S. investors participated in 401 investment transactions—or 17 percent of 2,299 global investment transactions—into Chinese AI companies.

Read the full article here.

NAVAL INTELLIGENCE ADMIRAL: 'NAÏVE' AMERICAN PUBLIC HAS A 'CHINA BLINDNESS' PROBLEM

Justin Katz | Breaking Defense | February 15, 2023

Following a week where most of the country's attention was transfixed on a high-altitude balloon deployed by the Chinese government, a top Navy intelligence officer said it is "unsettling" how blind most Americans have become to the threat China poses. "I'll be very honest with you. It's very unsettling to see how much the US is not connecting the dots on our number one challenge," Rear Adm. Mike Studeman, the commander of the Office of Naval Intelligence, told attendees here at the West 2023 conference in San Diego. "It's disturbing how ill-informed and naïve the average American is on China. I chalk this up, if I could summarize, into a China blindness. We face a knowledge crisis and a China blindness problem," he continued. Studeman's blunt comments come as the White House, the Pentagon and the country at-large deal with the fall-out of a Chinese high-altitude balloon that violated US airspace. The Chinese government claimed the first balloon, shot down over the Atlantic Ocean near South Carolina, was used for civilian scientific research and went severely off-course, while the Pentagon has said the balloon was an intelligence, reconnaissance and surveillance asset.

Read the full article here.

INTERNATIONAL BASIC RESEARCH COLLABORATION AT THE U.S. DEPARTMENT OF DEFENSE

Alison K. Hottes, Marjory S. Blumenthal, Jared Mondschein, Matthew Sargent, and Caroline Wesson | Rand National Security Research Division | 2023

In response to concerns about the research strength and practices of strategic competitors, the Basic Research Office within the Office of the Under Secretary of Defense for Research and Engineering asked the RAND National Defense Research Institute to study how the U.S. Department of Defense (DoD) approaches international basic research collaboration (IBRC) and formulate suggestions for DoD to improve how it uses IBRC. Benefits of IBRC include reducing technological surprise, leveraging investments of partners and allies, accessing diverse resources, and integrating international scientific thought leaders into DoD networks. Although strategic considerations add to or detract from the scientific benefits for some collaborations, not participating in IBRC would carry costs in the form of lost opportunities.

Read the full article here.

NATIONAL QUANTUM INITIATIVE

National Quantum Coordination Office | 2023

Welcome to quantum.gov, the home of the National Quantum Initiative and its ongoing activities to explore and promote Quantum Information Science (QIS). The National Quantum Initiative Act provides for the continued leadership of the United States in QIS and its technology applications. It calls for a coordinated Federal program to accelerate quantum research and development for the economic and national security of the United States. The United States strategy for QIS R&D and related activities is described in the National Strategic Overview for QIS and supplementary documents. Quantum-based technologies have already transformed society and the American economy. Examples include the Global Positioning System (GPS) for navigation, Magnetic Resonance Imaging (MRI) for medical imaging, semiconductors for computer chips, and lasers for telecommunications. Quantum information science (QIS) holds promise for another revolution in technology, with new, more powerful approaches to computing, networking, and sensing. The National Quantum Initiative (NQI) is a whole-of-government approach to ensuring the continued leadership of the U.S. in QIS and its technology applications.

Read the full article here.

CANADA CLAMPS DOWN ON MILITARY RESEARCH AS CHINA CONCERNS GROW

Randy Thanthong-Knight | Bloomberg | February 14, 2023

Canadian Prime Minister Justin Trudeau’s government will stop funding projects affiliated with universities, institutes or labs connected to foreign military, national defense or state security entities. Tuesday’s announcement seeks to close the loop on so-called sensitive research areas that pose risks to national security, according to a government statement. The Globe and Mail reported last month that 50 Canadian universities had extensive research collaborations with the Chinese military since 2005. The projects with China’s National University of Defence Technology included areas such as quantum cryptography, photonics and space science, the newspaper said. “This new action is one of many significant steps the government of Canada is taking to protect our country, our institutions and our intellectual property,” the government said, adding that guidelines were introduced for due diligence and risks to research security. Like many of its allies including the US, Canada has been taking a tougher stance against China in recent months.

Read the full article here.

VIEWPOINT: COMPANIES, NOT GOVERNMENTS, SHOULD LEAD GLOBAL TECH COLLABORATION

Bruce Guile | Science Business | February 6, 2023

War, pandemic, climate change, economic stress and rapid innovation are roiling the lives of people around the world and disrupting relations among nations. But in all this, one thing is clear: there is no path forward for advanced democracies that does not depend on tightening technological and economic security relationships with other democracies. To prosper, advanced democracies must navigate two paradoxes. First is that economic reality dictates that national sovereignty in technology requires collaboration with allies; talent and R&D capability are too globally distributed for any one nation to go it alone. The second paradox is that in liberal, free-market democracies, public authorities depend on private interests to achieve their goals. Multinational companies are the only enterprises that can credibly lead efforts to promote national tech security. Economic growth and globalisation since the end of the Cold War have remade the global landscape of national and regional capabilities in every aspect of science and technology.

Read the full article here.

TRUSTED RESEARCH GUIDANCE FOR ACADEMIA

Centre for the Protection of National Infrastructure | March 29, 2022

The UK has a thriving research and innovation sector that attracts investment from across the world. More than half of UK research is a product of international partnerships. Trusted Research aims to support the integrity of the system of international research collaboration, which is vital to the continued success of the UK's research and innovation sector. It is particularly relevant to researchers in STEM subjects, dual-use technologies, emerging technologies and commercially sensitive research areas. The advice has been produced in consultation with the research and university community and is designed to help the UK's world-leading research and innovation sector get the most out of international scientific collaboration whilst protecting intellectual property, sensitive research and personal information. Trusted Research outlines the potential risks to UK research and innovation, helps researchers, UK universities and industry partners to have confidence in international collaboration and make informed decisions around those potential risks, and explains how to protect research and staff from potential theft, misuse or exploitation. In addition to the following guidance we have produced Trusted Research for Senior Leaders which outlines some key considerations for academia leaders.

Read the full article here.

NSA RELEASES BEST PRACTICES FOR SECURING YOUR HOME NETWORK

National Security Agency | Central Security Service | February 22, 2023

The National Security Agency (NSA) released the "Best Practices for Securing Your Home Network" Cybersecurity Information Sheet (CSI) today to help teleworkers protect their home networks from malicious cyber actors. "In the age of telework, your home network can be used as an access point for nation-state actors and cybercriminals to steal sensitive information," said Neal Ziring, NSA Cybersecurity Technical Director. "We can minimize this risk by securing our devices and networks, and through safe online behavior." The guide includes recommendations for securing routing devices, implementing wireless network segmentation, ensuring confidentiality during telework, and more. Spearphishing, malicious ads, email attachments, and untrusted applications can present concerns for home internet users. NSA not only shows teleworkers how to secure their home networks, but also provides tips for staying safe online.

Read the full article here.

IS CHATGPT A THREAT TO ACADEMIC HONESTY?

Kelsey Ayton | PlagiarismSearch | February 17, 2023

Can education stay behind when it goes about technical progress? When the whole world is discussing amazing opportunities ChatGPT gives, should schools say 'No' or 'Yes' to progress? Does it make sense to let the students use the help from ChatGPT if it means that they do not do research themselves? On the other hand, can teachers forbid using it? Will it be technically possible to control whether the papers is done without the use of this magic helper? There are so many questions about threats to integrity and prospects of education in general that it is important to do in-depth analysis of all relevant aspects and try to conclude whether the challenges outweigh the advantages progress and artificial intelligence bring into our lives. Going viral, ChatGPT has initiated a lot of concerns related to possible cheating by the students. This powerful program of artificial intelligence emulates human thinking and writing so well that a student may simply ask a machine to complete his tasks and compose essays for school. Communicating directly with a computer, one can expect precise responses and addressing all specific requests.

Read the full article here.

HOW TO AVOID CHINESE TECH THAT MAY BE SPYING ON YOU

Kim Komando | USA Today | February 16, 2023

Color me surprised that TikTok hasn't been banned in the U.S. yet. Can't stop using it? Take this simple step to keep your data from going back to China. It's not just apps. More than a third of the world's electronics are produced in China. There's a difference between products made in China and those made by companies with ties to the Communist Chinese government. Now, before we dive in, know that there are plenty of allegations the companies below have government ties, but it's up for debate how much the Chinese government is genuinely involved in operations. I'm sharing this to help you make more informed decisions on what you purchase and use daily. TikTok is a dominant force. More than 138 million Americans use the video-sharing app owned by a company called ByteDance. FCC Commissioner Brendan Carr said ByteDance must comply with Chinese government laws. FBI Director Chris Wray said TikTok could be used for "influence operations" and that user data is in the hands of the Chinese government. That's not just conjecture. Late last year, TikTok was forced to admit that it used this same data to spy on individual Americans, including journalists. Without question, TikTok is a Trojan Horse. At least 27 states and the federal government have banned the use of the app on government devices.

Read the full article here.

CANADA VOWS TO PROTECT RESEARCH FROM FOREIGN THREATS

Florin Zubașcu and David Matthews | Science Business | February 16, 2023

The Canadian government has announced it will restrict international research cooperation to fend off potential foreign threats, amid mounting concerns in the west about technology espionage and intellectual property theft. In a joint statement published on Tuesday, innovation and science minister François-Philippe Champagne, health minister Jean-Yves Duclos, and public safety minister Marco Mendicino detailed steps the Canadian government will be taking to protect research from foreign interference. The government has requested the Canadian foundation for innovation and the federal research funding councils to adopt "a further enhanced posture regarding national security." Grant applications in areas the government deems "sensitive" will not be funded if any of the researchers are affiliated with a university, research institute or laboratory connected to military, defence and intelligence entities of countries that pose a risk to Canada's national security. The ministers say the research system could be a target for foreign powers. "We have made great strides in protecting Canada's research ecosystem, but with a constantly evolving threat environment, further action is needed," the statement said.

Read the full article here.

SF-86 AND OTHER SENSITIVE DATA EXPOSED IN U.S. MILITARY EMAIL SPILL

Jillian Hamilton | ClearanceJobs | February 21, 2023

The U.S. Department of Defense discovered over the weekend that one of their servers was sharing U.S. military emails out on the open internet for the past two weeks, according to TechCrunch. A missing password was the culprit for the server hosting the Microsoft Azure government cloud used for DoD customers. U.S. Special Operations Command (USSOCOM) and other DoD customers were impacted by this oversight. Anyone who might know the IP address for the sensitive mailbox data was able to access it for the past two weeks. Security researcher Anurag Sen discovered this oversight this past weekend, reaching out to TechCrunch, who in turn alerted the U.S. government. The impacted server did not hold classified information. However, internal military email messages and other sensitive information was exposed. But it wouldn't be a data breach or system oversight without an SF-86 being impacted.

Read the full article here.

INTRODUCTION TO COMMERCE DEPARTMENT EXPORT CONTROLS

U.S. Department of Commerce Bureau of Industry and Security | Office of Exporter Services | November 2018

The Department of Commerce's Bureau of Industry and Security (BIS) is responsible for implementing and enforcing the Export Administration Regulations (EAR) (15 CFR Parts 730-774), which regulate the export, reexport, and transfer (in-country) of most commercial and some military items. We often refer to items that BIS regulates as "dual-use" – items that have both commercial and military or proliferation applications – but some military items and purely commercial items without an obvious military use are also subject to the EAR. The EAR do not control all goods, services, and technologies. Other U.S. government agencies regulate more specialized exports. For example, the U.S. Department of State has authority over defense articles and defense services.

Read the full article here.

AS CHINA TECH CRACKDOWN CONTINUES, DON'T OVERLOOK THE DANGER OF LENOVO

Roslyn Layton | Forbes | December 28, 2022

The Chinese government got a lump of coal for Christmas, as the U.S. Department of Commerce placed twenty-five Chinese companies and other organizations on the Entity List – essentially prohibiting them from using strategic American technologies. 2022 marked important developments toward the goal of protecting Americans from Chinese tech threats. In addition to the takedown of Chinese chipmaker YMTC in the latest export controls, TikTok is under greater scrutiny as a Trojan Horse. But there is one Chinese entity which has largely escaped policymakers' notice, despite its presence in many American IT systems and its connection to one of the Chinese organizations which just landed on the Entity List. That company is Lenovo. Many are familiar with the name Lenovo from the ubiquity of the company's laptops – especially popular with many American businesses.

Read the full article here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Academic Security and Counter Exploitation Program is coordinated by The Texas A&M University System Research Security Office as a service to the academic community.
https://rso.tamus.edu

ASCE
ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

Academic Security and Counter Exploitation Program | *The Open Source Media Summary* | February 23, 2023 | Page 5 of 5