ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

February 15, 2023

## THE PENTAGON'S QUEST FOR ACADEMIC INTELLIGENCE: (AI)

*Michael T. Klare | The Nation | January 30, 2023*

At this time of intense debate within academia over race, gender, inequality, and our vanishing democracy, one might expect serious engagement with the moral and ethical implications of university-conducted war research. Yet, despite a massive increase in Pentagon support for military-oriented campus research, no such debate exists. Ever since many universities suspended their ties with the Department of Defense in the 1960s and '70s—often in response to impassioned anti-war protests—concern over such ties has largely disappeared. But now, with the military expanding its footprint on campus and an ever-increasing share of the nation's resources being devoted to war preparation, it is time to end this silence and start a rigorous debate on the ethics of university-conducted military research. The Pentagon has, of course, long subsidized research on basic and applied sciences at major US universities in order to ensure access to the latest developments in military-relevant fields. But most of these funds have been channeled to a dozen or so "federally funded research and development centers" (FFRDCs) that are typically housed in restricted, off-campus facilities.

Read the full article here.

## NEW EXASCALE SUPERCOMPUTER CAN DO A QUINTILLION CALCULATIONS A SECOND

*Sarah Scoles | Scientific American | February 9, 2023*

"Exascale" sounds like a science-fiction term, but it has a simple and very nonfictional definition: while a human brain can perform about one simple mathematical operation per second, an exascale computer can do at least one quintillion calculations in the time it takes to say, "One Mississippi." In 2022 the world's first declared exascale computer, Frontier, came online at Oak Ridge National Laboratory—and it's 2.5 times faster than the second-fastest-ranked computer in the world. It will soon have better competition (or peers), though, from incoming examachines such as El Capitan, housed at Lawrence Livermore National Laboratory, and Aurora, which will reside at Argonne National Laboratory. It's no coincidence that all of these machines find themselves at facilities whose names end with the words "national laboratory." The new computers are projects of the Department of Energy and its National Nuclear Security Administration (NNSA). The DOE oversees these labs and a network of others across the country. NNSA is tasked with keeping watch over the nuclear weapons stockpile, and some of exascale computing's raison d'être is to run calculations that help maintain that arsenal. But the supercomputers also exist to solve intractable problems in pure science.

Read the full article here.

## HOW U.S.-CHINA TENSIONS HAVE HURT AMERICAN SCIENCE

*Ilaria Mazzocco and Qin (Maya) Mei | Big Data China | December 9, 2022*

There is a growing concern in Washington that the United States government, its companies, and universities have helped drive the rapid growth of China's high-tech sector to the detriment of America's overall national interest. Accusations of intellectual property (IP) theft and state-sponsored industrial espionage by China have loomed large in the bilateral relationship. These concerns were at the heart of the Section 301 investigation launched by the U.S. Trade Representative (USTR) in 2018, which resulted in the subsequent imposition of tariffs and a trade war between the two countries. Moreover, as competition between Washington and Beijing deepens, the Biden administration has made it clear that it believes the United States must maintain as big of a lead as possible in key technologies, even if this means constraining previously permitted commercial sales and investments. Such sweeping policies on research and technology have had a chilling effect on academic collaboration between the United States and China. Reducing Chinese access to U.S. technology and cutting-edge research may be desirable for national security motivations regardless of the broader impact, but policymakers should be aware of the potential ramifications for the United States.

Read the full article here.

## JI CHAOQUN: CHINESE ENGINEER JAILED FOR EIGHT YEARS FOR SPYING IN US

*Nicholas Yong | BBC News | January 26, 2023*

Ji Chaoqun, 31, had identified scientists and engineers for possible recruitment, according to the US Department of Justice. He also enlisted in the US Army Reserves and lied to recruiters. US authorities said Ji worked under the direction of a key Chinese state intelligence unit. Last September he was convicted for acting as an agent of a foreign government without notifying the US attorney-general - a charge used in espionage cases - and of making false statements to the US Army. Ji had arrived in the US on a student visa a decade ago, according to a Justice Department statement. He was accused of supplying information to the Jiangsu Province Ministry of State Security (JSSD) about eight individuals for possible recruitment. The individuals are all naturalised US citizens who were originally from China or Taiwan, with some working as US defence contractors. Ji also enlisted in the US Army Reserves in 2016 under a programme that recruits foreign nationals with skills considered vital to national interest. He had lied in his application and in an interview that he had not had contact with a foreign government within the past seven years, said US officials. Ji was eventually arrested in September 2018 after he met with an undercover US law enforcement agent who posed as a representative of China's Ministry of State Security (MSS). During those meetings, Ji had explained that with his military identification he could visit and take photos of aircraft carriers.

Read the full article here.

## IT'S BIGGER THAN A BALLOON: CHINESE SPYING IN US INCLUDES RESEARCH LABS AND UNIVERSITIES

*Sen. John Barrasso | USA Today | February 15, 2023*

Like many Americans, residents of my home state of Wyoming could not understand how a Chinese spy balloon could lazily and brazenly pass over their heads. They are rightfully angry that an adversary's spying platform was able to violate and then linger over U.S. airspace for an entire week. They are angry our commander-in-chief did nothing to stop it until it reached the Atlantic Ocean.

Read the full article here.

## CHINESE AI INVESTMENT AND COMMERCIAL ACTIVITY IN SOUTHEAST ASIA

*Ngor Luong, Channing Lee, and Margarita Konaev | Center for Security and Emerging Technology | February 2023*

China's government has pushed the country's technology and financial firms to expand abroad, and Southeast Asia's growing economies — and AI companies — offer promising opportunities. This report examines the scope and nature of Chinese investment in the region. It finds that China currently plays a limited role in Southeast Asia's emerging AI markets outside of Singapore and that Chinese investment activity still trails behind that of the United States. Nevertheless, Chinese tech companies, with support from the Chinese government, have established a broad range of other AI-related linkages with public and commercial actors across Southeast Asia. As part of its pursuit of global technology leadership, China's government has pushed for Chinese firms to go abroad, including to Southeast Asia's growing economies. Consistent with this mandate, Chinese financial and technology companies have scoured the region for opportunities to expand their market and strengthen the country's competitiveness in emerging technologies such as artificial intelligence (AI).

Read the full article here.

## REDDIT HACK SHOWS LIMITS OF MFA, STRENGTHS OF SECURITY TRAINING

*Robert Lemos | Dark Reading | February 10, 2023*

The latest hack of a well-known company highlights that attackers are increasingly finding ways around multifactor authentication (MFA) schemes — so employees continue to be an important last line of defense. On Jan. 9, Reddit notified its users that a threat actor had successfully convinced an employee to click on a link in an email sent out as part of a spearphishing attack, which led to "a website that cloned the behavior of our intranet gateway, in an attempt to steal credentials and second-factor tokens." The compromise of the employee's credentials allowed the attacker to sift through Reddit's systems for a few hours, accessing internal documents, dashboards, and code, Reddit stated in its advisory. The company continues to investigate, but there's no evidence yet that the attacker gained access to user data or production systems, Reddit CTO Chris Slowe (aka KeyserSosa) stated on a follow-up AMA.

Read the full article here.

## A U.S. JUDGE LECTURES THE GOVERNMENT ON HOW ACADEMIC RESEARCH WORKS

*Jeffrey Mervis | Science | January 20, 2023*

A sentencing hearing is a forum to mete out justice for someone convicted of a crime. But this week, U.S. District Court Senior Judge Julie Robinson used the sentencing of Franklin Tao, a chemical engineer formerly at the University of Kansas (KU), Lawrence, to also talk at length about what motivates academic researchers—and how the U.S. government appeared to misunderstand that culture in pursuing criminal charges against Tao. Her remarks are a rare example of a federal judge speaking in public about the U.S. academic enterprise and its pursuit of knowledge. Tao was convicted last year of failing to accurately report his interactions with a Chinese university to KU, which said this week he is no longer a faculty member. But Robinson, who was appointed by then-President George W. Bush in 2001, says the government wrongly portrayed Tao's exploration of an academic job in China as a malicious attempt to share the fruits of federally funded research with the Chinese government.

Read the full article here.

## GLOBAL CHINA: ASSESSING CHINA'S GROWING ROLE IN THE WORLD

*Foreign Policy Media | Brookings | 2023*

From a potential "responsible stakeholder" to a "strategic competitor," the U.S. government's assessment of China has changed dramatically in recent years. China has emerged as a truly global actor, impacting every region and every major issue area. From 2018-2020, the Brookings Global China project produced one of the largest open source diagnostic assessments of China's actions in every major geographic and functional domain. Brookings is now launching Phase 2 of the Global China Project which builds upon the research and analysis of the first phase, and shifts toward prescription, focusing on advancing recommendations on how the United States should respond to China's actions that implicate key American interests and values.

Read the full article here.

## TECHNOLOGY-BASED ECONOMIC DEVELOPMENT

*Sujai Shivakumar | Issues in Science and Technology | Winter 2023*

In "Manufacturing and Workforce" (Issues, Fall 2022), Sujai Shivakumar provides a timely and important review of the CHIPS and Science Act. This landmark legislation aims at strengthening domestic semiconductor research, development, design, and manufacturing, and advancing technology transfer in such fields as quantum computing, artificial intelligence, clean energy, and nanotechnology. It also establishes new regional high-tech hubs and looks to foster a larger and more inclusive workforce in science, technology, engineering, and mathematics—the STEM fields. In a recent article in Annals of Science and Technology Policy, I noted that the act focuses tightly on general-purpose technologies, emanating from technology transfer at universities and federal laboratories. Shivakumar correctly notes that public/private investment in technology-based economic development (TBED) in manufacturing must be accompanied by workforce development to match the human capital needs of producers and suppliers. I have two recommendations relating to workforce development, in the context of technology transfer.

Read the full article here.

## PROTECTING YOUR ORGANIZATION'S SECRETS

*The National Counterintelligence and Security Center | January 3, 2019*

You have access to facilities and computer networks, as well as sensitive information, resources, technologies, research and other data that our foreign adversaries and competitors desperately want. Our adversaries and competitors are interested in you because you have connections and access. You also have social media accounts. A work and/or personal smartphone. Social and professional networks include others in sensitive positions. You may travel, both domestically and abroad. These are all potential vulnerabilities. Phishing is a common method used to compromise computer networks and gain access to valuable information they contain. You may receive a seemingly real and plausible or official-looking email, text message, or pop-up window to lure you into clicking on a link or attachment. That action allows the attacker to bypass your network's technical defense, upload malware, or otherwise infiltrate your network and steal information.

Read the full article here.

## NOBEL PRIZE SUMMIT ON COUNTERING MISINFORMATION AND BUILDING TRUST IN SCIENCE TO BE HELD MAY 24-26

*The National Academies of Sciences, Engineering, and Medicine | February 2, 2023*

The Nobel Prize Summit *Truth, Trust and Hope* will bring together Nobel Prize laureates and other world-renowned experts and leaders for a global dialogue on how to stop misinformation from eroding public trust in science, scientists, and the institutions they serve. Speakers will include Nobel Prize laureates such as journalist and author **Maria Ressa** and astrophysicist **Saul Perlmutter,** along with other distinguished experts including **Tristan Harris,** co-founder of the Center for Humane Technology, and **Åsa Wikforss,** professor of theoretical philosophy and member of the Swedish Academy.

Hosted by the U.S. National Academy of Sciences and the Nobel Foundation, the three-day summit will be held at the NAS building in Washington, D.C., and virtually, and is free and open to the public.

Read the full article here.