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

Open Source Media Summary

January 25, 2024

INTERVIEW: HOW CHINA WIELDS ITS "SHARP POWER"

Hoover Institution | January 17, 2024

Jonathan Movroydis: What was the genesis of the project on China's Global Sharp Power?

Glenn Tiffert: Hoover's project on China's Global Sharp Power (CGSP) grew out of a 2018 report jointly edited by Larry Diamond and Orville Schell of the Asia Society called China's Influence & American Interests. This report took a hard look at the various ways in which China had penetrated different sectors of American society and was exerting influence in ways that were underappreciated and not readily apparent to the eye. The media, local government, national government, think tanks, academia—sectors of that sort. The report was seminal to the larger discussion the United States has since been having about how China exerts influence—sometimes malign influence—in democratic societies. When we finished it, we realized that there was a lot more work to be done and CGSP was born.

Movroydis: Covert, coercive, and corrupting: are those generally the attributes of sharp power? What are some of its other characteristics?

Tiffert: Those were the words former Australian prime minister Malcolm Turnbull used to describe it.

Read the full article here.

CANADA'S NEW RESEARCH SECURITY RULES TARGET INSTITUTIONS IN CHINA, IRAN, RUSSIA

Jim Bronskill | The Toronto Star | January 16, 2024

The federal government will not bankroll sensitive scientific research tied to dozens of schools, institutes and labs in China, Iran and Russia under new restrictions announced Tuesday. Among the 11 strategically important research areas are artificial intelligence and big data technology, quantum science and aerospace and satellite systems. Ottawa is concerned that foreign adversaries are determined to acquire sensitive Canadian research and intellectual property by partnering on projects with academics in Canada. The announcement builds on a federal statement issued Feb. 14, 2023, that research in key fields will not be funded if those involved are affiliated with institutions linked to military, defence or state security organizations of counties deemed a risk to Canada. The government has published a list of the sensitive technology research areas and a complementary list of named research organizations with which researchers should avoid ties if they're seeking federal funding.

Read the full article here.

CHINA TAKES AIM AT CANADA'S MOVE TO BLOCK CHINESE, RUSSIAN, IRANIAN RESEARCH LINKS

Jack Lau | South China Morning Post | January 17, 2024

China has hit out at Canada's plan to stop funding sensitive research linked to certain Chinese, Russian and Iranian military and security institutions, saying it politicises and weaponises technological cooperation. "The relevant policy from Canada is short-sighted, unwise and harms another without benefiting itself," Chinese foreign ministry spokeswoman Mao Ning told reporters in Beijing on Wednesday. Ties between Canada and China have been strained in recent years, even after the saga ended over the arrest in Vancouver of a Huawei Technologies executive on fraud charges and the detention of two Canadians in China for suspected espionage. All three were released in 2021. Ottawa in May expelled a Chinese diplomat accused of trying to intimidate a member of parliament, resulting in a tit-for-tat move from Beijing.

Read the full article here.

E&C, CHINA SELECT COMMITTEES LAUNCH INQUIRY INTO TAXPAYER FUNDING STREAMS FUNNELED TO CCP-BACKED RESEARCHER

House Energy and Commerce Committee | Press Release | January 17, 2024

House Energy and Commerce Committee (E&C) Chair Cathy McMorris Rodgers (R-WA), E&C Subcommittee on Communications and Technology Chair Bob Latta (R-OH), E&C Subcommittee on Oversight and Investigations Chair Morgan Griffith (R-VA), E&C Subcommittee on Innovation, Data, and Commerce Chair Gus Bilirakis (R-FL), and House Select Committee on the Chinese Communist Party, launched an investigation into grants made to an AI scientist at the University of California, Los Angeles (UCLA) with ties to the Chinese Communist Party (CCP). The Chairs made requests for documents to UCLA, the National Science Foundation (NSF), and the U.S. Department of Defense (DOD).

BACKGROUND:

- On November 1, 2023, a Newsweek investigation found that the federal government awarded at least $30 million in federal research grants led by Mr. Song-Chun Zhu, who is now "at the forefront of China's race to develop the most advanced artificial intelligence."

Read the full article here.

MANY US SCIENTISTS SAY SECURITY MEASURES AGAINST CHINA AND OTHERS GO TOO FAR

Richard Hudson | Science/Business | November 22, 2022

For years, big advances in science and technology have propelled economic growth world-wide. Now, as geopolitical tensions mount, leaders of the US scientific community fret that rising government security measures may kill the goose that laid the golden egg. A tightening of US security procedures for science, begun in the Trump administration but still continuing today, risks disrupting the open nature of science, said Tobin Smith, senior vice president of the Association of American Universities. Speaking at a Washington science policy workshop, he said, "I caution against going too far [on security]. Our very job at universities is to disseminate knowledge." Likewise, Ernest Moniz, a former MIT administrator and US energy secretary, warned, "We are overreacting" on security. In the case of China relations, the US has already "taken a number of missteps, or at least questionable steps", including prosecuting some researchers on charges of hiding ties to Chinese institutions.

Read the full article here.

CHINA'S RULING PARTY TAKES DIRECT CONTROL OF COUNTRY'S UNIVERSITIES

Gu Ting | Radio Free Asia (RFA) | January 18, 2024

The Chinese Communist Party is taking a direct role in the running of universities across the country amid ongoing mergers of embedded party committees with presidents' offices, Radio Free Asia has learned. While the ruling party already has branches and committees embedded in universities and other academic institutions, commentators said it has never actually merged itself with administrative structures before, not even during the political turmoil of the Cultural Revolution. The party committee at Beijing's Tsinghua University issued a notice on Jan. 14 announcing that its office had merged with the office of the university president to form a new Party Committee Office that would run the school. Tsinghua's website was recently updated to reflect the changes, on a page titled "Departmental Overview." An employee who answered the phone at the new office on Jan. 15 confirmed that media reports about the change were accurate. "[The merger happened] last year," the employee said.

Read the full article here.

OTTAWA CLAMPS DOWN ON UNIVERSITY RESEARCH PARTNERSHIPS WITH CHINA, IRAN AND RUSSIA

Robert Fife and Steven Chase | The Globe and Mail | January 18, 2024

The federal government has unveiled strict new national-security rules to protect cutting-edge science and advanced technology from ending up in the hands of China, Russia and Iran. The long-promised package of reforms would ban federal granting agencies and the Canada Foundation for Innovation (CFI) from funding sensitive technology research at any university, laboratory and research institution that co-operates with military, national defence or state security bodies of countries posing a risk to Canada. Innovation Minister François-Philippe Champagne promised tougher restrictions last year after The Globe and Mail reported that Canadian universities had for years collaborated with a top Chinese army scientific institution on hundreds of advanced-technology research projects, generating knowledge that could help drive China's defence sector in high-tech industries.

Read the full article here.

WHY ISN'T AUSTRALIA SECURING ITS CRITICAL RESEARCH?

Brendan Walker-Munro | Australian Association for Research in Education (AARE) | January 18, 2024

Just before Christmas last year, the National Science Foundation (NSF) of the United States announced aims to establish a network which would enable the funders of university research to share information about applications, applicants and programs of national security concern. That same news story mentioned that the NSF had already established a dialogue with the main funding body for the United Kingdom (UK), Research and Innovation, as well as Canada's Ministry of Innovation, Science and Economic Development and the Natural Science and Engineering Research Council. Talks have also been planned with The Netherlands government, home of the National Contact Point for Knowledge Security. What was interesting – and somewhat chilling – about the announcement was the obvious omission of Australia and its principal funding body, the Australian Research Council (ARC). This apparent lack of engagement with Australia over securing research seems a little at-odds with the United States' other foreign policy measures, such as the AUKUS Agreement under which Australia will become just the seventh country with nuclear-powered submarines.

Read the full article here.

CCP COMMITTEE PROPOSES RESEARCH SECURITY AND TECH DEVELOPMENT INITIATIVES

Jacob Taylor | American Institute of Physics | December 18, 2023

The House Select Committee on the Chinese Communist Party adopted a bipartisan report last week that proposes the U.S. "reset" its economic relationship with China in part through new research security measures and controls on technology exports. The recommended actions include:

- Prohibiting U.S. entities from conducting research with Chinese entities that are "involved with military and defense R&D," such as those on the list of China's Defense Science and Technology Key Labs developed by the U.S. Air Force
- Requiring research institutions to "obtain an export control license if they intend to use any export-controlled item that has a clear and distinct national security nexus, during the course of research collaboration on critical and emerging technologies with any foreign adversary entity"
- Empowering the president to ban entities owned or controlled by foreign adversaries from selling certain technology products in the U.S. market, including quantum computing, biotechnology, artificial intelligence, autonomous systems, and surveillance products
-

Read the full article here.

NATIONAL SECURITY ACTS COULD DAMAGE RESEARCH AND EXCHANGES, SAY US UNIVERSITIES

Helen Packer | The Pie News | January 19, 2024

Increased training for researchers on security threats, enhanced scrutiny of foreign partnerships and reviews of international contracts are among the steps US institutions have taken to address foreign security threats, according to a new briefing from the Association of American Universities. Keen to avoid over-regulation, the group emphasised that researchers "take seriously" national security threats posed by international actors and that universities are still navigating newly-introduced requirements to protect American research. But, with Congress now considering a raft of additional measures to protect federally funded research data and intellectual property at US institutions, the compliance burden on universities may continue to grow.

Read the full article here.

FEDERAL OFFICIALS WERE WARY OF CREATING 'CHILL' OVER RESEARCH SECURITY: DOCUMENTS

Jim Bronskill | Global News | January 16, 2024

Federal officials were wary of creating a chill within ethnic communities and rattling Canada's bilateral relations as they fleshed out next steps to secure vital scientific research, internal documents show. The federal government has been working for months to prepare a list of sensitive research areas and the names of labs and institutions considered a risk to national security. Officials are scheduled to provide a detailed update on the delicate process in a briefing Tuesday. The announcement builds on a Feb. 14, 2023, federal statement that research in sensitive areas will not be funded if personnel are affiliated with institutions linked to military, defence or state security organizations of foreign counties deemed to be a risk to Canada.

Read the full article here.

NEW GENERATIVE AI GUIDELINES AIM TO CURB RESEARCH MISCONDUCT

Yojana Sharma | University World News | January 20, 2024

China's Ministry of Science and Technology last month published new guidelines on the use of generative artificial intelligence in scientific research, as part of its efforts to improve scientific integrity and reduce research misconduct. The new rules notably include a ban on the 'direct' use of generative AI tools when applying for research funding and approval. Under the guidelines, generative AI can still be used in research, but any content or findings that use the technology must be clearly labelled as such. The ministry noted in particular that the rapid development of technologies such as AI "may give rise to new problems in the handling of research data, the formation and attribution of research works, and the attribution of intellectual property rights", noting that the rapid development of such technologies has prompted "profound changes in the nature of scientific research". The document, Guidelines for Responsible Research Conduct, issued by the ministry's Supervision Department, was drawn up after extensive research and solicitation of opinions, according to the ministry.

Read the full article here.

CISA DIRECTS AGENCIES TO MITIGATE WIDESPREAD VPN BUGS

Adam Mazmanian | NEXTGOV/FCW | January 19, 2024

Federal civilian agencies are under emergency orders to address recently discovered flaws in a widely used virtual private network appliance from Ivanti that is currently being targeted by hackers linked to the People's Republic of China, officials said on Friday. The Cybersecurity and Infrastructure Security Agency issued an emergency directive, ordering agencies to apply temporary mitigation measures to the as-yet unpatched vulnerability in Ivanti's Connect Secure VPN. Eric Goldstein, CISA's executive assistant director for cybersecurity, told reporters on Friday that the vulnerability was serious. "Exploitation allows deep access into the target network enabling data exfiltration, or persistence to achieve other objectives," Goldstein said, noting that about 15 agencies were using these products and have already applied mitigation measures. "We are not at this time in a place where we can confirm compromise for any federal agencies," Golstein said, adding later in response to questions: "We are not assessing a significant risk to the federal enterprise, but we know that that risk is not zero."

Read the full article here.

CONGRESS IS FAILING TO DELIVER ON ITS PROMISE OF BILLIONS MORE IN RESEARCH SPENDING, THREATENING AMERICA'S LONG-TERM ECONOMIC COMPETITIVENESS

Jason Owen-Smith | The Conversation | January 16, 2024

The battle to keep the government open may feel just like the crisis of the day. But these fights pose immediate and long-term risks for the U.S. The federal government spends tens of billions of dollars every year to support fundamental scientific research that is mostly conducted at universities. For instance, the basic discoveries that made the COVID-19 vaccine possible stretch back to the early 1960s. Such research investments contribute to the health, wealth and well-being of society, support jobs and regional economies and are vital to the U.S. economy and national security. If Congress can't reach an agreement, then a temporary government shutdown could happen on Jan. 19, 2024. If lawmakers miss a second Feb. 2 deadline, then automatic budget cuts will hit future research hard.

Read the full article here.

HOW TO VET A CORPORATE INTELLIGENCE VENDOR

Maria Robson-Morrow, Katherine Tucker, and Paul R. Kolb | Harvard Business Review
January 19, 2024

Imagine you're the CEO of a major technology firm and your chief operations officer is conducting a site visit in Asia to scope out a potential new investment. Your company needs: 1) an on-the-ground security provider to protect your COO during the trip, 2) an assessment of the country, including security and geopolitical conditions that could facilitate or jeopardize business, and 3) better understanding of your potential partners. To understand geopolitical and security operating conditions, multinational companies rely on intelligence vendors who complement or substitute for in-house teams. "Vendor relationships augment a team's headcount and can provide real-time support and intelligence," explains Angela Lewis, who worked in corporate intelligence at Salesforce and The Walt Disney Company and whose PhD focused on corporate intelligence. Demand for intelligence vendors is substantial and increasing. In 2022, global cyber threat intelligence was estimated to be a $4.93 billion industry, and U.S. security services was a whopping $48.1 billion. Geopolitical and security risk intelligence is an unquantified but essential and rapidly growing part of the story.

Read the full article here.

THE TEXAS A&M
UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute

USEFUL RESOURCES

GLOBAL CHINA HUB

Atlantic Council

The Global China Hub researches and devises allied solutions to the global challenges posed by China's rise, leveraging and amplifying the Atlantic Council's work on China across its fifteen other programs and centers.

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute