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

Open Source Media Summary

November 21, 2024

THE RISC OPEN SOURCE MEDIA SUMMARY WILL NOT BE PUBLISHED THE WEEK OF NOVEMBER 25 IN OBSERVANCE OF THE THANKSGIVING HOLIDAY

REGISTRATION NOW OPEN FOR THE ASCE 2025 ANNUAL SEMINAR FEBRUARY 25-27, TO BE HELD AT TEXAS A&M UNIVERSITY

Born from a commitment to safeguarding the integrity of academic research, the Academic Security and Counter Exploitation (ASCE) program, spearheaded by The Texas A&M University System's RISC Institute, fosters a sense of community among university research security professionals, uniting them in a collaborative defense against emerging threats. Since its inception in 2016, ASCE has been a beacon in the fight against foreign influence, equipping academic institutions with the knowledge and tools needed to protect their invaluable research. Now in its ninth year, the annual ASCE Seminar stands as the preeminent gathering for training, networking, and collaboration, laser-focused on fortifying the academic research enterprise.

View the full resource here.

ASCE 2025 CALL FOR PROPOSALS

If you would like to present, please submit your proposal by clicking on the link below.
The seminar committee will review all proposals, and the selection will be based on relevance to the seminar theme, quality of the abstract, and potential audience engagement. Presenters will be notified of acceptance or rejection no later than January 15, 2025.

The submission deadline is December 15, 2024.

View the full resource here.

CANADA SHOULD SHARPLY CURTAIL RESEARCH COLLABORATIONS WITH CHINA, LAWMAKERS SAY

Brian Owens | Science | November 13, 2024

Canada should immediately end all government-funded research collaborations with China in a host of sensitive technology areas, a parliamentary committee has recommended in a new report. The ban is needed, the panel said, to counter the Chinese government's "increasingly assertive" efforts to build up its military and scientific might, sometimes through espionage. "While international collaboration to advance scientific knowledge for the benefit of humanity is important, it does not supersede the need for the government to protect the national security of Canada," states the report, which the Special Committee on the Canada-People's Republic of China Relationship presented to Parliament on 4 November. Prime Minister Justin Trudeau's government has until early March 2025 to respond to the recommendation, which would significantly expand existing Canadian restrictions on research collaborations with China.

Read the full article here.

ACADEMIC SAYS AUSTRALIAN SPY AGENCY ASKED HER TO REPORT ON CHINESE STUDENTS

Stephen Dziedic | ABC News | November 14, 2024

An Australian National University academic has sharply criticized Australia's domestic intelligence agency, saying it asked her to report on Chinese international students and put a "chill" on China research as the bilateral relationship deteriorated. Amy King is an associate professor from the Strategic and Defense Studies Centre whose academic work focuses heavily on China and North Asia. She used an address to the Australian Institute of International Affairs conference on Monday to criticize the scrutiny applied to her work, and to warn against Australia approaching China from a "position of fear". "Over the past decade, I have been asked by our security services to justify my visits to China," she said. "I have been reported on to our security services when I have been overheard in public talking with Chinese-Australian academics here in Canberra.

Read the full article here.

ENABLING THE DRAGON: THE DANGERS OF CHINA'S ACADEMIC OUTSOURCING TO THE UNITED STATES

M. Miles Yu | Hoover Institution, Stanford University | November 13, 2024

In recent years, the United States has awoken to the multifaceted threats posed by the Chinese Communist Party (CCP) and its ambitions for global dominance. This revelation stems from a critical understanding of China's three defining realities: it remains a non-market economy, controlled by the CCP without constitutionally guaranteed property rights; it is a communist regime that stifles free thought and academic autonomy; and, perhaps most ominously, it harbors an unrelenting ambition for global hegemony. These traits reveal a nation incapable of nurturing the intellectual and technological talent it requires for such ambitions—an Achilles' heel the CCP has resolved by exploiting the very openness of the United States. For decades, China has outsourced its talent training to America's world-renowned universities. But today, the risks of this academic relationship have begun to eclipse any potential benefit, casting a shadow over U.S. national interests and security.

Read the full article here.

CANADA URGED TO CUT GOVERNMENT-FUNDED RESEARCH COLLABORATIONS WITH CHINA: REPORT

Alex Karpa | CTV News | November 14, 2024

A newly released report is urging Canada to immediately end all government-funded research collaborations with China in a variety of different areas. Some areas include advanced digital infrastructure technology, advanced sensing and surveillance, advanced weapons, and space and satellite technology. "The safety and security of Canadians must be the top priority of the Government of Canada," reads the report, which houses a list of 12 recommendations. "While international collaboration to advance scientific knowledge for the benefit of humanity is important, it does not supersede the need for the government to protect the national security of Canada, and the safety and security of Canadians." The report says China's actions through foreign interference and espionage have become "increasingly assertive." "This is the sensible approach to take," says Christian Leuprecht, a Royal Military College professor at Queen's University. "The risk with China in many areas of research simply cannot be mitigated."

Read the full article here.

T-MOBILE HACKED IN MASSIVE CHINESE BREACH OF TELECOM NETWORKS, WSJ REPORTS

Reuters | November 15, 2024

T-Mobile's (TMUS.O), opens new tab network was among the systems hacked in a damaging Chinese cyber-espionage operation that gained entry into multiple U.S. and international telecommunications companies, The Wall Street Journal reported on Friday citing people familiar with the matter. Hackers linked to a Chinese intelligence agency were able to breach T-Mobile as part of a monthslong campaign to spy on the cellphone communications of high-value intelligence targets, the Journal added, without saying when the attack took place. "T-Mobile is closely monitoring this industry-wide attack," a company spokesperson told Reuters in an email. "At this time, T-Mobile systems and data have not been impacted in any significant way, and we have no evidence of impacts to customer information." It was unclear what information, if any, was taken about T-Mobile customers' calls and communications records, according to the WSJ report.

Read the full article here.

US LAWMAKERS URGE REVIEW OF CHINA THREAT FROM PHOTONICS TECHNOLOGY

Stephen Nellis | Reuters | October 28, 2024

A bipartisan group of U.S. lawmakers on Monday urged the Department of Commerce to examine national security threats from China's development of silicon photonics technology, a fast-developing field that could speed up artificial intelligence. At its core, silicon photonics relies on light, rather than electrical signals, to move information inside of computer systems and has uses in artificial intelligence systems where tens of thousands of computer chips are connected. Leading AI chip firms such as Nvidia (NVDA.O), opens new tab and Advanced Micro Devices (AMD.O), opens new tab have published research on how to integrate photonics into their chips, while Silicon Valley startup Lightmatter recently raised $400 million for its photonic technology, pushing the firm's value to $4.4 billion. China has also been aggressively pursuing the technology, with Guangdong province in recent weeks joining a spate of funding programs aimed at building photonics chips in China, according to state media.

Read the full article here.

WHAT IS AND ISN'T CONCERNING ABOUT CHINA'S AI SURPRISE

Matthew Mittelsteadt | The Hill | November 14, 2024

Reuters recently reported that researchers affiliated with China's People's Liberation Army released studies demonstrating that they had applied versions of Meta's Llama AI system to experimental military applications. Within hours, there were renewed congressional calls to slam the gate on unrestricted commercial exports of AI products. Although concern about China's global AI ambition is warranted, officials are misinterpreting this event and drawing the wrong lessons. In one case, Llama's 13b version from 2023 was found to be useful for intelligence analysis and military-relevant information queries. In another, Llama 2 was applied to "support electronic warfare and self-defense jamming strategies." This raised immediate concern that U.S. companies were brazenly sharing our most advanced technology without restrictions. To address that, we need to ground the conversation and determine whether this incident truly represents a threat.

Read the full article here.

SPECTER OF CHINA HOVERS OVER US COLLEGES

Tara McKelvey | Radio Free Asia (RFA) | November 11, 2024

The leaves were turning red and orange at Georgia Institute of Technology on a recent afternoon, and students were studying for midterms. Yet within this quiet haven, a global conflict has raged. Georgia Tech, as the university is known, has been pulled into the geopolitical strife between the United States and China. A group of U.S. lawmakers say that Chinese officials have been trying to pilfer research from Georgia Tech and other American universities and use their resources to strengthen China's military. In a September report, Republican members of two separate committees in the House of Representatives said that Beijing has been benefiting from the U.S.-funded research done at Georgia Tech and other universities in this country. The report claimed that research intended to help the U.S. military has inadvertently given a boost to the Chinese armed forces by allowing Chinese researchers access to knowledge and technology that could ultimately have militaristic ends.

Read the full article here.

SCIENCE POLICY OUTLOOK FOR THE SECOND TRUMP PRESIDENCY

Mitch Ambrose | AIP | November 14, 2024

How President-elect Donald Trump will approach science policy during his second term is difficult to predict, as the subject did not often surface during the 2024 campaign season. But Trump's stances on broader issues have clear implications for science policy in some cases. Trump's general hostility toward China will likely prompt further restrictions on scientific and technological exchanges, continuing the trend that started in his first administration and was expanded on by President Joe Biden. Meanwhile, Trump's opposition to Biden's equity initiatives will likely force a rapid retreat from the subject by federal science agencies, and his promise to convert thousands of civil service jobs into political roles could prompt major turnover of scientists. It is unclear who is responsible for science policy on Trump's transition team, but among those focused on technology policy is Michael Kratsios, who served in the first Trump administration as U.S. chief technology officer in the White House Office of Science and Technology Policy and later became the acting head of the Defense Department's R&D arm. Kratsios previously worked for venture capitalist Peter Thiel, who has close ties to Vice President-elect J.D. Vance.

Read the full article here.

U.S. OUTLINES SCOPE OF NEW CURBS ON INVESTMENT IN CHINA'S 'SENSITIVE TECHNOLOGY' SECTORS

Xiaoting (Maya) Liu, Karen Hui, Steve Zhu | Asia Pacific Foundation of Canada | November 15, 2024

The U.S. Treasury Department has published the fine print on a new set of restrictions on outbound investment in China's high-tech sectors. These restrictions are part of Washington's ongoing efforts to limit Beijing's ability to use U.S. technologies for its military advancement. The new rules are expected to impact a range of cross-border companies and investors and prompt policy changes by Washington's allies, including Canada.

Read the full article here.

HOW US-CHINA SCIENCE PACT'S FATE COULD SHAKE GLOBAL R&D LANDSCAPE

Rahul Pandey | MyNews | September 3, 2024

The expiration of the US-China Science and Technology Agreement (STA) on August 27 marks a critical juncture in the scientific collaboration between the two global giants. It was one of the formative bilateral agreements signed between US president Jimmy Carter and China's paramount leader Deng Xiaoping on January 31, 1979. The agreement was designed to foster mutual advancement in science and technology by promoting joint research efforts, information sharing and enhancing bilateral ties. After renewals every five years until 2018, and six-month extensions last August and in February this year, its expiration increases uncertainty over the future of US-China scientific relations. Initially, it was a landmark bilateral accord aimed at strengthening cooperation in scientific and technological domains. It was built on the principles of equality, reciprocity and mutual benefit, emphasizing collaborative research and the exchange of experts. *(Note: Subscription may be required to access article.)*

Read the full article here.

GROUNDBREAKING FRAMEWORK FOR THE SAFE AND SECURE DEPLOYMENT OF AI IN CRITICAL INFRASTRUCTURE UNVEILED BY DEPARTMENT OF HOMELAND SECURITY

Department of Homeland Security | November 14, 2024

Today, the Department of Homeland Security (DHS) released a set of recommendations for the safe and secure development and deployment of Artificial Intelligence (AI) in critical infrastructure, the "Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure" ("Framework"). This first-of-its kind resource was developed by and for entities at each layer of the AI supply chain: cloud and compute providers, AI developers, and critical infrastructure owners and operators – as well as the civil society and public sector entities that protect and advocate for consumers. The Artificial Intelligence Safety and Security Board ("Board"), a public-private advisory committee established by DHS Secretary Alejandro N. Mayorkas, identified the need for clear guidance on how each layer of the AI supply chain can do their part to ensure that AI is deployed safely and securely in U.S. critical infrastructure. This product is the culmination of considerable dialogue and debate among the Board, composed of AI leaders representing industry, academia, civil society, and the public sector. The report complements other work carried out by the Administration on AI safety, such as the guidance from the AI Safety Institute, on managing a wide range of misuse and accident risks.

Read the full article here.

USEFUL RESOURCES

COUNTERINTELLIGENCE THREAT VIA SOCIAL MEDIA

Defense Counterintelligence and Security Agency | Center for Development of Security Excellence

Social networking sites (SNS) are everywhere in today's society. Worldwide SNS usage provides foreign intelligence entities (FIE) vast opportunities to exploit personnel, cleared or uncleared. The FIE goal is to obtain U.S. critical technology, proprietary data, advanced research and development, and many other aspects of valuable information in U.S. industry.

Read the full article here.

2023 TOP ROUTINELY EXPLOITED VULNERABILITIES

Joint Cybersecurity Advisory

This advisory provides details, collected and compiled by the authoring agencies, on the Common Vulnerabilities and Exposures (CVEs) routinely and frequently exploited by malicious cyber actors in 2023 and their associated Common Weakness Enumerations (CWEs).

View the full resource here.

INNOVATING THE DATA ECOSYSTEM: AN UPDATE OF THE FEDERAL BIG DATA RESEARCH AND DEVELOPMENT STRATEGIC PLAN

Executive Office of the President of the United States

This document, Innovating the Data Ecosystem: An Update of The Federal Big Data Research and Development Strategic Plan, updates the 2016 Federal Big Data Research and Development Strategic Plan.

View the full resource here.

DEFENSE PRIMER: UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

Congressional Research Service | November 15, 2024

Advances in science and technology (S&T) have long played a critical role in ensuring the technological preeminence of the U.S. military. For this reason, the Department of Defense (DOD) is the largest funder of federal research and development. The Under Secretary of Defense for Research and Engineering (USD (R&E)) is a civilian official reporting directly to the Secretary of Defense. The USD (R&E) serves as the principal advisor to the Secretary of Defense for DOD research, engineering, and technology development activities and programs.

View the full resource here.

EVENTS AND VIDEOS

EVENT: PROMOTING EUROPEAN COOPERATION IN DEVELOPING RESPONSES TO RESEARCH SECURITY CHALLENGES: ONLINE EVENTS SERIES

Loughborough University, University of Sterling and Network and Foundation Consultancy Limited

December 12, 2024 is the third and final online event for this series.

View the video here.

VIDEO: CRITICAL ISSUES IN THE US-CHINA SCIENCE AND TECHNOLOGY RELATIONSHIP

Hoover Institution | November 14, 2024

Both the United States and the People's Republic of China see sustaining leadership in science and technology (S+T) as foundational to national and economic security. Policymakers on both sides of the Pacific have taken action to promote indigenous innovation, and to protect S+T ecosystems from misappropriation of research and malign technology transfer. In the US, some of these steps, including the China Initiative, have led to pain, mistrust, and a climate of fear, particularly for students and scholars of and from China. Newer efforts, including research security programs and policies, seek to learn from these mistakes. A distinguished panel of scientists and China scholars discuss these dynamics and their implications. What are the issues facing US-China science and technology collaboration? What are the current challenges confronting Chinese American scientists? How should we foster scientific ecosystems that are inclusive, resilient to security challenges, and aligned with democratic values?

View the video here.

THE TEXAS A&M
UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute