ASCE
ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM
https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

June 1, 2023

RESEARCH THEFT: THE TOUGHEST JOB OF SAFEGUARDING UNIVERSITIES

Nathan M. Greenfield | University World News | May 6, 2023

The memo titled "Guidance on Contact with CSIS [Canadian Security Intelligence Service]" sent by the University of Waterloo (UW) in southwestern Ontario, Canada, to its researchers at the end of March alarmed David Robinson, executive director of the Canadian Association of University Teachers. While the memo did not indicate which disciplines CSIS was interested in, the euphemism "high-priority research" was understood to mean science, technology, engineering and mathematics (STEM) fields. CSIS agents, the memo states, "may be concerned that you could be the target of a foreign state or entity, or they may have questions about some aspects of your activities". But the memo makes clear: "You do not have a legal obligation to talk to a CSIS officer"; you are not required to "speak with the officer immediately, or at the place where they approached you. If agents appear at your place of residence, you can ask them to reschedule the meeting to your workplace." After helpfully urging researchers to "remain calm, polite and ... truthful" in their statements, the memo ends by asserting the university's rights: "You must not consent to a search of University of Waterloo property without authorisation from the University of Waterloo."

Read the full article here.

SPOTLIGHT ON BEIJING INSTITUTE FOR GENERAL ARTIFICIAL INTELLIGENCE

Huey-Meei Chang and William Hannas | Center for Security and Emerging Technology | May 2023

China's Beijing Institute for General Artificial Intelligence (BIGAI), established with state backing in 2020, aims openly at artificial general intelligence (AGI) and is assembling the talent and organizational means to pursue it. The project's core is an elite team of Chinese- and U.S.-educated scientists managed by former University of California, Los Angeles (UCLA) researcher Zhu Songchun, whose work in precursor disciplines, professional network, and openness to methodological alternatives lend credibility to the project. The present study—an introduction to BIGAI's goals, staffing, and research—situates this AGI project in the context of China's overall work toward advanced artificial intelligence. BIGAI by choice is not pursuing the massively large natural language models championed by OpenAI, Google, and other U.S. and British companies. BIGAI focuses instead on developing AGI through alternative "small data, big task" research on brain cognition and neuroscience.

Read the full article here.

USTR RELEASES 2023 SPECIAL 301 REPORT ON INTELLECTUAL PROPERTY PROTECTION AND ENFORCEMENT

Executive Office of the President | The Office of the United States Trade Representative | April 26, 2023

The Office of the United States Trade Representative (USTR) today released its 2023 Special 301 Report on the adequacy and effectiveness of U.S. trading partners' protection and enforcement of intellectual property (IP) rights. "Innovation and creativity are at the heart of American competitiveness. That is why the Biden-Harris Administration's new story on trade includes lifting up the 60 million jobs and workers in our IP-intensive industries through robust IP protection and enforcement in foreign countries," said Ambassador Tai. "Our Administration will continue to engage with the trading partners identified in this year's Report to empower our inventors, creators, and brands, and to demonstrate that trade can deliver tangible results across the American economy." This annual report details USTR's findings of more than 100 trading partners after significant research and enhanced engagement with stakeholders.

Read the full article here.

AT RISK IN DEBT TALKS: CUTS TO R&D CAN GIVE CHINA TECH SUPREMACY

Divyansh Kaushik and Matt Hourihan | The Messenger | May 26, 2023

The United States continues to face major challenges in the race for global technology supremacy. Recent political maneuvers within China have underscored its laser focus on scientific and technological advancements as integral to its competitive strategy with the West. A variety of national and economic security stakeholders — as well as political leaders from both parties — continue to sound the alarm over the U.S. ability to invent, innovate and build next-generation technologies here. But the U.S. high-tech trade deficit surpassed $200 billion for the first time ever in 2022, and Congress has missed funding targets for science agencies by billions of dollars. Meanwhile, overseas investments in China and elsewhere continue to ramp up. It's vital that the United States remains on its front foot, making the necessary investments to ensure long-run competitiveness. For these reasons, our leaders must tread cautiously as they negotiate a final fiscal deal. The recent budget plan passed by the Republican-controlled House represents a terrible mistake. Speaker Kevin McCarthy (R-Calif.) has used the U.S.'s approaching debt limit deadline as a bargaining chip with President Joe Biden in an effort to secure the House budget plan's proposed cuts.

Read the full article here.

RESEARCH PROGRAM ON RESEARCH SECURITY

Gordon Long | The MITRE Corporation | National Science Foundation | March 2023

The National Science Foundation (NSF) is at the forefront of US government agencies supporting fundamental research. It has also been a center of activity on the security of federally-funded fundamental research, creating a new position of Chief of Research Security Strategy and Policy. Research security has become a much-used term over the past few years, and it has become apparent that research security is not a commonly understood concept in the fundamental research community. Indeed, many of the US and international attempts to define the nature of the problem do not clearly distinguish between research security and research integrity. Thus, NSF needs to understand the aspects of "research security" that are distinct from "research integrity" as well as how the concepts overlap and how they depend on scientific discipline. This understanding will assist NSF, its federal partners, and the research community to assess in an evidence-based manner which, if any, controls are needed to secure research from undue foreign influence.

Read the full article here.

RESEARCH SECURITY: PROTECTING CANADA'S ACADEMIC RESEARCH FROM FOREIGN ESPIONAGE

Peter K. MacKinnon | Research Money Inc. | May 3, 2023

Today, Canada and its allies are faced with an increasing degree of domestic academic intelligence gathering. This can potentially threaten our economic base through foreign espionage by both cyber and other means. Referred to as Research Security, it concerns the measures taken to protect research data, materials and participants, including partners, from unauthorized access, theft or misuse. The depth of penetration into Canada's research community is currently unknown; however, examples exist and can be anything from gaining cyber to physical access. Cyber protection is achievable if organizations and individuals practice good cyber stewardship. The more insidious penetrations could be a visiting scholar, graduate student or academic partner. It is for the most part the human roles that are shaping the debate about what to do and how. Research Security is a growing concern at the executive level in Canadian universities and is starting to be a responsibility of the vice-presidents for research/innovation. It also is a growing concern of the federal government, with a soon to be released report on Research Security from the Canadian Security Intelligence Service.

Read the full article here.

A PORTAL TO CHINA IS CLOSING, AT LEAST TEMPORARILY, AND RESEARCHERS ARE NERVOUS

Bochen Han | South China Morning Post | March 25, 2023

China's top internet portal for academic papers will suspend foreign access to some databases starting next week, sparking concerns among scholars that they will lose not only an important resource for understanding China but also a useful guardrail to reduce misunderstanding between China and the West. This week, research institutions around the world – including the University of California, San Diego, Kyoto University and the Berlin State Library – notified affiliates that they would indefinitely lose access to up to four databases provided by the China National Knowledge Infrastructure (CNKI) platform starting on April 1. In a notice sent to affected institutions on March 17, CNKI's operator – Tongfang Knowledge Network Technology – noted that the suspension was made in accordance with "the Measures of Data Cross-Border Transfer Assessment and relevant laws effective September 1, 2022".

Read the full article here.

CONFUCIUS INSTITUTES IN THE UNITED STATES: SELECTED ISSUES

Congressional Research Service | May 2, 2023

The People's Republic of China's (PRC's or China's) Confucius Institutes offer instruction in Chinese language in universities around the world. The Institutes have been the subject of controversy since appearing on U.S. university campuses in 2005, particularly for their perceived effects on academic freedom and for their lack of transparency. They have attracted further attention during the past several years as the broader U.S.-China relationship has deteriorated. Some Members of Congress and others have alleged that they may play a role in China's efforts to influence public opinion abroad, recruit "influence agents" on U.S. campuses, and engage in cyber espionage and intellectual property theft. PRC officials have denied such charges, and suggested that the Institutes have become victims of a U.S. "Cold War mentality." Supporters of the Institutes have emphasized that they provide Chinese language and cultural programs that benefit students, universities, and surrounding communities, and that such offerings may not otherwise be available.

Read the full article here.

NIST REVISES SP 800-171 GUIDELINES FOR PROTECTING SENSITIVE INFORMATION

The National Institute of Standards and Technology | May 10, 2023

The National Institute of Standards and Technology (NIST) has updated its draft guidelines for protecting sensitive unclassified information, in an effort to help federal agencies and government contractors more consistently implement cybersecurity requirements. The revised draft guidelines, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST Special Publication [SP] 800-171 Revision 3), will be of particular interest to the many thousands of businesses that contract with the federal government. Federal rules that govern the protection of controlled unclassified information (CUI), which includes such sensitive data as health information, critical energy infrastructure information and intellectual property, reference the SP 800-171 security requirements. Systems that store CUI often support government programs containing critical assets, such as design specifications for weapons systems, communications systems and space systems. The changes are intended in part to help these businesses better understand how to implement the specific cybersecurity safeguards provided in a closely related NIST publication, SP 800-53 Rev. 5.

Read the full article here.

GUIDELINES FOR MANAGING THE SECURITY OF MOBILE DEVICES IN THE ENTERPRISE: NIST PUBLISHES SP 800-124 REVISION 2

The National Institute of Standards and Technology | May 17, 2023

Today mobile devices are ubiquitous, and they are often used to access enterprise networks and systems to process sensitive data. NIST Special Publication (SP) 800-124 Revision 2, Guidelines for Managing the Security of Mobile Devices in the Enterprise, assists organizations in managing and securing mobile devices against the ever-evolving threats. To address these threats, this publication describes technologies and strategies that can be used as countermeasures and mitigations. NIST SP 800-124 Rev. 2 also provides recommendations for secure deployment, use, and disposal of mobile devices throughout the mobile device life cycle. The scope of this publication includes mobile devices, centralized device management, and endpoint protection technologies, while including both organization-provided and personally-owned (bring your own device) deployment scenarios.

Read the full article here.

U.S. THINK TANK REPORTS PROMPTED BEIJING TO PUT A LID ON CHINESE DATA

Lingling Wei | The Wall Street Journal | May 7, 2023

A recent campaign to restrict overseas access to China-based data sources was partly triggered by a drumbeat of U.S. think tank reports on sensitive Chinese practices that alarmed Beijing, according to people with direct knowledge of the matter. Increasingly worried about perceived Western threats, Beijing in recent weeks expanded an anti-espionage law and stepped up pressure on foreign companies specializing in collecting information, such as auditors, management consultants and law firms. In addition, access to Chinese databases including Shanghai-based Wind Information has tightened for foreign think tanks, research firms and other nonfinancial entities. The wider scope of the campaign is intended to ensure the party-state's control over narratives about China. The part of it focused on restricting overseas access to databases began in earnest after some reports based on publicly available information set off alarms among senior Chinese officials, according to the people with knowledge of the matter.

Read the full article here.

DATA MANAGEMENT AND SHARING POLICY

National Institutes of Health | Scientific Data Sharing

NIH has a longstanding commitment to making the results of NIH-funded funded research available. Responsible data management and sharing has many benefits, including accelerating the pace of biomedical research, enabling validation of research results, and providing accessibility to high-value datasets. NIH encourages the sharing of data whenever possible. Learn about the 2003 NIH Data Sharing policy and the 2023 NIH Data Management and Sharing policy as well as how they apply to NIH funded research and data.

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