ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

June 15, 2022

NEW EVIDENCE ON THE ROLE OF SUBNATIONAL DIPLOMACY IN CHINA'S PURSUIT OF U.S. TECHNOLOGY

Ryan Scoville | Lawfare | June 10, 2022

In a recent interview, FBI Director Christopher Wray explained that the People's Republic of China has stolen more U.S. corporate data than all other nations combined and is seeking to acquire American trade secrets and intellectual property "on a scale that is unprecedented in history." China reportedly relies on a combination of industrial espionage, academic contacts, investment, and cyber theft in pursuit of this acquisition. Senior U.S. officials have observed that China also relies on subnational relations with U.S. state governments, but the nature and extent of those relations have generally been unclear. In this post, I will help to address that lack of clarity by presenting new evidence that China has entered into a substantial collection of written agreements with U.S. states for the purpose of promoting technology transfer in a number of strategically sensitive fields of innovation, including information technology, nanotechnology, aerospace, biotechnology, and semiconductors. Most of these agreements appear to have been adopted not only without federal notice, consultation, or approval, but also at China's initiative and without public disclosure. The evidence thus suggests that subnational diplomacy has played an inconspicuous but material role in Beijing's effort to acquire cutting-edge American technology.

Read the full article here.

US DECLINES ACROSS ALL METRICS IN LATEST GLOBAL RANKINGS

Brendan O'Malley | University World News | June 11, 2022

The United States declines across all metrics despite remaining the world's pre-eminent higher education system and despite Massachusetts Institute of Technology (MIT) celebrating 11 years as the world's best university in the latest QS World University Rankings, released on Wednesday. In the top 10 there is a little movement, with the University of Oxford (fourth) dropping two places while the University of Cambridge moves up one place to second. But there are no new entrants. At the top is MIT (US), followed by the University of Cambridge (United Kingdom), Stanford University (US), the University of Oxford (UK), Harvard University (US), the California Institute of Technology (US), Imperial College London (UK), UCL (UK), ETH Zurich (Switzerland) and the University of Chicago (US). The US continues to decline broadly across its 201 ranked universities with more than 50% dropping down the table – representative of a trend that has persisted for several years due largely to rapidly growing global competition, QS reports. Of these 201 universities, 29 improve (14.4%), 44 remain stable (22%), but 103 decline (51%). On the plus side, 25 are newly ranked (14% increase year on year).

Read the full article here.

EXPORT CONTROLS: ENFORCEMENT AGENCIES SHOULD BETTER LEVERAGE INFORMATION TO TARGET EFFORTS INVOLVING U.S. UNIVERSITIES

U.S. Government Accountability Office | June 14, 2022

Millions of foreign students and scholars study at U.S. universities, and many contribute to U.S. research. But, there's a risk that some may illegally access and share sensitive information, such as data or technology, with their home countries. Agencies involved in addressing this threat said that outreach and education increases university officials' awareness of research security threats and builds stronger relationships with university officials. To help prevent illegal transfers, we recommended that agencies determine which universities are at greater risk for such transfers and target outreach and education to them. According to U.S. government agencies, foreign entities are targeting sensitive research conducted by U.S. universities and other institutions.

Read the full article here.

RESEARCH SECURITY RULES: IS UNIVERSITY AUTONOMY AT RISK?

Jan Petter Myklebust | University World News | June 4, 2022

The Danish Ministry of Higher Education and Science published a report on 25 May which calls for a "paradigm shift" in the Danish approach to international research and innovation and offers practical guidelines for Danish educational and research institutions to "reduce risks and increase the potential for benefits in international research and innovation collaboration". The Danish measures are part of broader efforts by Nordic countries to combat intellectual espionage and information misuse in international research collaborations. While cooperation with countries such as China and Russia tends to be foregrounded as current security threats, most of the measures are designed to be applied more generally. "Danish universities shall in the future follow a set of guidelines when collaborating with international partners to prevent [a situation in which] international researchers in reality are used for espionage or theft of technology for military use," the report said.

Read the full article here.

OPPORTUNITIES EXIST TO STRENGTHEN NIH GRANTEES' OVERSIGHT OF INVESTIGATORS' FOREIGN SIGNIFICANT FINANCIAL INTERESTS AND OTHER SUPPORT

Suzanne Murrin, Deputy Inspector General for Evaluation and Inspections | U.S. Department of Health and Human Services, Office of Inspector General | June 2022

In fiscal year (FY) 2020, the National Institutes of Health (NIH) awarded $31 billion to grantee institutions (hereafter grantees) to support biomedical research. These grantees play key roles in protecting the integrity and security of U.S. biomedical research by requiring investigators to report (1) significant financial interests (hereafter financial interests) and (2) all sources of their other support (hereafter support), which includes all resources in support of and/or related to all of their research endeavors. This includes foreign financial interests and support. Failures by some investigators at these grantees to disclose substantial contributions of resources from foreign entities (including foreign governments) have raised concerns about threats to the integrity of NIH-supported research. To determine how grantees (1) ensure that investigators disclose all foreign financial interests and support and (2) review this information prior to reporting information to NIH, we administered online surveys to 773 grantees that (as of July 1, 2020) received NIH funding for FY 2020.

Read the full article here.

THE BRITISH WEAPONS EXPERT COSYING UP TO CHINA

David Rose | UnHerd | May 26, 2022

His audience hung on his every word. Here was one of Britain's foremost weapons experts chairing a prestigious, two-day conference devoted to exploring new ways of making arms more deadly. But the packed conference hall, its walls lined with oak and marble, wasn't in Britain. It was in Jinan, the capital of Shandong province in eastern China. Clive Woodley, 67, currently attached to the Department of Shock Physics at Imperial College in London, has worked on high-tech weaponry since his youth. So he had much to say about the conference theme: "New Material Technology for Ammunition." The event "marked a new chapter in the development of artillery, shells and missiles", according to an official report issued afterwards. Most of Woodley's research has been funded by the Ministry of Defence. A former president of the International Ballistics Society, he served as Chief Scientist at the MoD-controlled company QinetiQ from its inception in 2001 — when the MoD privatised its own labs — to 2018. He has advised the MoD about many of its key lethal systems.

Read the full article here.

PROTECTING FROM THE THREAT WITHIN: HOW TO MANAGE INSIDER RISK

Paul Furtado | InformationWeek | June 9, 2022

Insider risk exists in every organization, and it can be difficult to identify. Organizations typically invest in security tools to keep external actors at bay, but don't often prioritize tools to protect the organization from trusted users and accounts. Whether through malice, negligence or error, the security risks posed by employees, contractors and integrated third-party partners must be addressed. The reality is that insiders have an advantage over an external attacker -- they know where the data exists and how to get it. It is critical that security and risk management leaders understand and address the threat of insider risk to protect the enterprise perimeter. Insider risk is the potential for an individual with authorized access to act in a way that could negatively affect the organization -- either maliciously or unintentionally. Every employee, contractor or third party that is connected to enterprise systems poses an insider risk. It's important to distinguish between insider risk and insider threats. An insider threat is a specific user that is committing an isolated act with malicious intent. Not every insider risk becomes an insider threat, but every insider threat starts as an insider risk.

Read the full article here.

OPERATION CUCKOOBEES: CYBEREASON UNCOVERS MASSIVE CHINESE INTELLECTUAL PROPERTY THEFT OPERATION

Cybereason Nocturnus | Cybereason | May 4, 2022

Cybersecurity often focuses on malware campaigns or the latest zero-day exploit. Surveys and reports reveal the average cost of a data breach or how much it typically costs to recover from a ransomware attack. Those are the attacks that make noise and capture attention, though. The attacks that fly under the radar are often more insidious and much more costly. Researchers at Cybereason recently discovered such an attack, which was assessed to be the work of Chinese APT Winnti. Cybereason briefed the US Federal Bureau of Investigation (FBI) and Department of Justice (DOJ) on the investigation into the malicious campaign, which Cybereason researchers dubbed Operation CuckooBees. For years, the campaign had operated undetected, siphoning intellectual property and sensitive data. The team published two reports–one that examines the tactics and techniques of the overall campaign and another that provides a more detailed analysis of the malware and exploits used.

Read the full article here.

FORTHCOMING DISCLOSURE AND SECURITY REQUIREMENTS FOR INSTITUTIONS HOSTING FEDERALLY FUNDED RESEARCH

David Aaron and Thea Percival | Perkins Coie | June 7, 2022

National Security Presidential Memorandum-33 (NSPM-33) and implementation guidance from the National Science and Technology Council (NSTC) direct federal agencies to standardize and enhance disclosure and security requirements that apply to federally funded research and development (R&D). These new requirements will have direct effects on academic and research institutions that receive federal funding. All federal research funding agencies will be required to bolster and standardize reporting and disclosure requirements. Academic and research institutions that receive federal funding for research will be subject to disclosure requirements as a condition of eligibility for federal R&D awards. Moreover, institutions that receive significant federal funding will incur additional requirements related to research security and integrity. In particular, research security programs that include cybersecurity, insider threat, and export control components must meet certification requirements.

Read the full article here.

CANADIAN UNIVERSITIES STILL PARTNERING WITH HUAWEI DESPITE 5G BAN OVER SECURITY

Robert Fife and Steven Chase | The Globe and Mail | June 9, 2022

Leading Canadian universities say they intend to continue research and development with Huawei Technologies Co. – which reaps intellectual property from the partnerships – after Ottawa's decision to ban the Chinese telecommunications giant from 5G wireless networks over national-security concerns. When the Trudeau government announced on May 19 that it would bar Huawei from selling 5G equipment to Canadian telecommunications companies, it did not take action against Huawei's extensive dealings with Canadian universities. Huawei spends roughly $25-million annually on university R&D projects aimed at the development of advanced communications technologies including 5G and 6G wireless. The company participates in research programs, often as a sponsor, at about 20 Canadian postsecondary institutions including the University of Toronto, University of British Columbia, McGill University, Carleton University, University of Calgary and the University of Waterloo.

Read the full article here.

TAXPAYER-FUNDED RESEARCH PROJECTS DIDN'T CHECK FOR SCIENTISTS TAKING MONEY FROM CHINA: IG

Ryan Lovelace | The Washington Times | June 10, 2022

Federal internal investigators have uncovered alarming failures by universities to require scientists doing taxpayer-funded research to disclose when they also pocket money from China and other foreign countries. The Health and Human Services Department's inspector general said the failure to enforce disclosure rules exposes critical biomedical research to theft by China. Joanna Bisgaier, a deputy regional inspector general who worked on the report, said the widespread disregard for government rules was unanticipated and she did not know whether it was attributable to grantees' ignorance, recklessness or malice. "We were not expecting quite a large percentage of grantees who failed to comply with the federal requirements regarding disclosure of foreign financial interest and support," Ms. Bisgaier said in an interview. More than two-thirds of National Institutes of Health grant recipients examined by the inspector general — 69% — failed to require their researchers and scientists to disclose at least one type of foreign financial interest or support as required under HHS and National Institutes of Health rules, according to the report, which was published this month.

Read the full article here.

UNIVERSITIES FACING NEW CHINA CASH CRACKDOWN

Ben Ellery | The Times | June 13 2022

Universities will be forced to reveal investment from “foreign actors” under plans being put forward by the government this week to crack down on undue influence. Michelle Donelan, the universities minister, will set out rules requiring them to report any financial arrangements they have with individuals or organisations overseas, “to ensure that UK values cannot be compromised”. The change, which will be proposed today as an amendment to the Higher Education (Freedom of Speech) Bill, is proposed against a backdrop of universities accepting money from hostile nations such as China and Russia. The threshold for reporting will be £75,000.

Read the full article here.

9 WAYS HACKERS WILL USE MACHINE LEARNING TO LAUNCH ATTACKS

Maria Korolov | CSO | June 13, 2022

Machine learning and artificial intelligence (AI) are becoming a core technology for some threat detection and response tools. The ability to learn on the fly and automatically adapt to changing cyberthreats give security teams an advantage. However, some threat actors are also using machine learning and AI a to scale up their cyberattacks, evade security controls, and find new vulnerabilities all at an unprecedented pace and to devastating results. Here are the nine most common ways attackers leverage these technologies. Defenders have been using machine learning to detect spam for decades, says Fernando Montenegro, analyst at Omdia. "Spam prevention is the best initial use case for machine learning," he says. If the spam filter used provides reasons for why an email message did not go through or generates a score of some kind, then the attacker can use it to modify their behavior. They'd be using the legitimate tool to make their own attacks more successful. "If you submit stuff often enough, you could reconstruct what the model was, and then you can fine-tune your attack to bypass this model," Montenegro says.

Read the full article here.

CONTROLLED UNCLASSIFIED INFORMATION QUICK REFERENCE GUIDE

Office of Prepublication and Security Review | U.S. Department of Defense | April 1, 2021

Controlled Unclassified Information is similar to FOUO as it is handled, stored, transmitted, and destroyed in basically the same manner as the legacy FOUO program: When the option is available, should be processed on Government Furnished Equipment (GFE), must be encrypted if sent via NIPRNet, limit access to those with a lawful government purpose, and destroyed by means approved for destroying classified or in a manner making it unreadable, indecipherable, and irrecoverable.

For information to be considered CUI it must fall within a category, such as:

- Critical Infrastructure
- Defense
- Export Control
- Financial & Tax
- Immigration
- Intelligence
- International Agreements
- Law Enforcement

View the full reference guide 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