THE OPEN SOURCE MEDIA SUMMARY

ASCE
ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

April 8, 2021

MARSHA BLACKBURN INTRODUCES LEGISLATION TARGETING BEIJING'S INFLUENCE AT AMERICAN COLLEGES

Clarksville Online | April 6, 2021

U.S. Senator Marsha Blackburn (R-Tenn.) along with Senators Ted Cruz (R-Texas), Kevin Cramer (R-N.D.), Tommy Tuberville (R-Ala.), Mike Braun (R-Ind.), Josh Hawley (R-Mo.), and Rick Scott (R-Fla.) introduced the Transparency for Confucius Institutes Act. Confucius Institutes, which are run and paid for by the CCP, currently operate at 55 American colleges and universities. They allow China to discretely influence what college students are taught about topics like Hong Kong and Tiananmen Square and impede freedom of speech on campus. Beijing's propaganda officials have even recently "rebranded" Confucius Institutes as centers for "language exchange and cooperation" to avoid government oversight. "Beijing will look for any opportunity to gain a foothold in American communities and push propaganda," said Senator Blackburn. "Confucius Institutes allow Communist China to have leverage over students at American colleges and universities. We cannot allow students to be brainwashed by revisionist history." "The Chinese Communist Party engages in propaganda and censorship to control what Americans see, hear, and ultimately think about China," Senator Cruz said.

Read the full article here.

US UNIVERSITIES CALL FOR CLEARER RULES ON SCIENCE ESPIONAGE AMID CHINA CRACKDOWN

Nidhi Subbaraman | Nature | April 6, 2021

The US government is converging on a long-awaited set of rules designed to protect American science from theft by foreign spies. A series of announcements this year describe steps that US universities and researchers must take when reporting foreign financing and collaborations to US science funders. But university groups say they need more clarity on how to implement the rules. And the guidelines do not spell out how institutions can address concerns of racial profiling sparked by the US government's crackdown on foreign interference in recent years. The issue of foreign influence and interference in US research has loomed large as geopolitical tensions between the United States and China have risen. The new guidelines date back to the last days of former US president Donald Trump's administration; so far, President Joe Biden's administration has not indicated that it will seek to change the policies and that it is open to feedback. Before he left office in January, Trump issued a memorandum describing the US government's responsibility to protect the country's research.

Read the full article here.

ASCE
ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

CHINA AS A 'CYBER GREAT POWER': BEIJING'S TWO VOICES IN TELECOMMUNICATIONS

Rush Doshi, Emily de La Bruyère, Nathan Picarsic, and John Ferguson | Brookings | April 2021

External Chinese government and commercial messaging on information technology (IT) speaks in one voice. Domestically, one hears a different, second voice. The former stresses free markets, openness, collaboration, and interdependence, themes that suggest Huawei and other Chinese companies ought to be treated like other global private sector actors and welcomed into foreign networks. Meanwhile, domestic Chinese government, commercial, and academic discourse emphasizes the limits of free markets and the dangers of reliance on foreign technologies — and, accordingly, the need for industrial policy and government control to protect technologies, companies, and networks. Domestic Chinese discourse also indicates that commercial communication networks, including telecommunications systems, might be used to project power and influence offensively; that international technical standards offer a means with which to cement such power and influence; and — above all — that IT architectures are a domain of zero-sum competition.

Read the full article here.

COCA-COLA TRADE SECRET THEFT UNDERSCORES IMPORTANCE OF INSIDER THREAT EARLY DETECTION

Christopher Burgess | CSO | April 6, 2021

The trial of Xiaorong You is set to begin today, April 6, in Greenville, TN. She is accused of trade secret theft and economic espionage after allegedly stealing bisphenol-A-free (BPA-free) technologies owned by several companies, including her former employers Coca-Cola and Eastman Chemical Company. The value placed on the development of the stolen technologies is $119.6 million. Other affected companies include Azko-Nobel, Dow Chemical, PPG, TSI, Sherwin Williams and ToyoChem. The details of the case suggest that the damages You is allegedly responsible for could have been minimized if better real-time insider threat detection methods had been in place. They also outline possible motives for the theft of the intellectual property: ego and money. You (a.k.a. Shannon You) is a naturalized US citizen with a PhD in Polymer Science and Engineering from Lehigh University. She has worked in US industry since May 1992.

Read the full article here.

REP. GOSAR UNVEILS BILL TO EXPOSE 'SPEWING OF PROPAGANDA' IN CONFUCIUS INSTITUTES

Isabel Van Brugen | The Epoch Times | April 2, 2021

Rep. Paul Gosar (R-Ariz.) on Thursday unveiled a bill that seeks to expose Confucius Institutes and other foreign influence programs in the United States. The legislation, called the Higher Education Transparency Act, mandates complete transparency to expose Chinese Communist Party (CCP) funded Confucius Institutes (CI) and other foreign influence programs on college campuses disguised as cultural and language programs. It would require American universities to be transparent about any agreement they have with foreign entities, including CIs. These foreign entities, said Gosar, are "seeking to leverage influence on American college campuses." Billed as language and culture centers, Beijing-funded CIs have drawn intense scrutiny over their role in spreading Chinese propaganda and stifling academic expression across college campuses around the world. They're funded and largely staffed by Hanban, a nonprofit that claims to be non-governmental but is directly controlled by the CCP, according to a report by the Senate Homeland Security committee's investigations subcommittee.

Read the full article here.

IT'S TIME FOR A NEW POLICY ON CONFUCIUS INSTITUTES

Jamie P. Horsley | Lawfare | April 1, 2021

On March 5, the U.S. Senate voted to deny Department of Education funding to universities that host Confucius Institutes (CIs)—the controversial Chinese language and culture centers partially financed by the People's Republic of China (PRC)—unless they meet oversight requirements. A federal campaign against their alleged "malign influence," pressure from politicians and Department of Defense funding restrictions have prompted and accelerated closure of more than half the CIs in the United States. Faculty concerns over preserving academic freedom and university budget constraints concerning operating funds have all contributed to the trend. But so has a decline of American student interest in China studies and learning Mandarin Chinese. These closings and the attendant inflammatory rhetoric exacerbate a national foreign language deficit at a time when training Mandarin speakers familiar with an ever more consequential China should be a national priority. To meet this challenge, the U.S. government should increase funding for Mandarin language and China studies courses, but also stop forcing cash-strapped universities to choose between federal funding and properly managed CI programs.

Read the full article here.

SUSPECTED NORTH KOREAN HACKERS SET UP FAKE COMPANY TO TARGET RESEARCHERS, GOOGLE SAYS

Shannon Vavra | Cyber Scoop | March 31, 2021

North Korean-linked hackers have set up a fake security company and social media accounts as part of a broad campaign targeting cybersecurity researchers with malware, according to Google research published Wednesday. Hackers have leveraged at least two fake accounts on LinkedIn that impersonate recruiters appearing to be from antivirus software and security companies, Google said. One of the recruiters, supposedly named "Carter Edwards," works at a company allegedly named "Trend Macro," which someone quickly searching for a new information security job may confuse with the legitimate security firm Trend Micro. The campaign also relies on a smattering of Twitter accounts. The fake Turkey-based company, which the hackers call "SecuriElite," claims to be based in Turkey and focused on offensive security, penetration tests, software security assessments and exploits, according to Google. The hackers set up the apparent company in March, Google said.

Read the full article here.

BIDEN TAKES ON CHINA

Marvin C. Ott | Foreign Policy Research Institute | April 1, 2021

Future historians may well consider President Joseph Biden's recent comments on China as a pivotal moment in the history of American foreign policy. It was not long ago—early in the 2020 Democratic presidential primary process—that Biden dismissed the idea that China was a truly serious competitor, much less a threat, to the United States. His view today represents a 180-degree swing on both counts. It was not long ago when U.S. political leaders, academic experts, and foreign correspondents tended to portray the rapid rise of China as a largely economic phenomenon that was broadly good for the United States and the world. President Bill Clinton spoke confidently of how the internet would inevitably democratize China. Presidents George H.W. and George W. Bush emphasized the shared interests of Beijing and Washington. The corporate world put its money behind the same assessment, investing heavily in manufacturing and banking in China. Meanwhile, Chinese students flocked to American universities.

Read the full article here.

BALKING AT AN INTERNATIONAL PARTNERSHIP

Elizabeth Redden | Inside Higher Ed | April 7, 2021

Members of the Faculty Senate and Student Assembly at Cornell University voted separately last week to formally oppose a proposed dual-degree program involving Cornell's School of Hotel Administration and the Guanghua School of Management at Peking University (PKU), in Beijing. Members of Cornell's Faculty Senate voted to oppose the proposed dual-degree program with PKU by a 39 to 16 margin, with 20 senators abstaining. Another 51 senators did not participate in the vote, which is advisory and not binding. The main concerns voiced by faculty were focused on the severe constraints on academic freedom in China and the Chinese government's treatment of the Uighurs, a Muslim minority group. A U.S. State Department report on human rights practices globally released last week described the perpetration of "genocide and crimes against humanity" against Uighurs and other members of ethnic minority religious groups -- including "the arbitrary imprisonment or other severe deprivation of physical liberty of more than one million civilians" -- in China's northwestern region of Xinjiang.

Read the full article here.

CHINA BUILDS ADVANCED WEAPONS SYSTEMS USING AMERICAN CHIP TECHNOLOGY

Ellen Nakashima and Gerry Shih | The Washington Post | April 7, 2021

In a secretive military facility in southwest China, a supercomputer whirs away, simulating the heat and drag on hypersonic vehicles speeding through the atmosphere — missiles that could one day be aimed at a U.S. aircraft carrier or Taiwan, according to former U.S. officials and Western analysts. The computer is powered by tiny chips designed by a Chinese firm called Phytium Technology using American software and built in the world's most advanced chip factory in Taiwan, which hums with American precision machinery, say the analysts. Phytium portrays itself as a commercial company aspiring to become a global chip giant like Intel. It does not publicize its connections to the research arms of the People's Liberation Army. The hypersonic test facility is located at the China Aerodynamics Research and Development Center (CARDC), which also obscures its military connections though it is run by a PLA major general, according to public documents, and the former officials and analysts, many of whom spoke on the condition of anonymity to discuss a sensitive matter.

Read the full article here.

UNIVERSITY NEWSPAPER 'CAPITULATED' AFTER REMOVING ARTICLE CRITICAL OF CHINESE COMMUNIST PARTY

News.com.au | April 4, 2021

The editors of a renowned university newspaper have been accused of being silenced by China after removing an article critical of the Communist government's activities on Australian campuses. Honi Soit, the student-run newspaper from the University of Sydney, removed the investigative feature linking two of its university's engineering academics to Chinese government programs. That's despite the fact nothing in the article has yet proved to be inaccurate. The editors claimed it risked escalating racism towards people of Chinese descent. That reasoning has met a furious response with the publication accused of running a pro-CCP "propaganda rag". The editors of Honi Soit told news.com.au the article was removed out of safety concerns for the individuals named in the article. They stressed the people named hadn't been accused of "personal wrongdoing".

Read the full article here.

PENTAGON RELEASES GUIDES FOR MARKING CONTROLLED UNCLASSIFIED INFORMATION AHEAD OF CMMC PROGRAM LAUNCH

Sara Friedman | Inside Defense | April 7, 2021

The Defense Department has issued two new resources for contracting officials regarding the identification of controlled unclassified information and how it should be identified on government documents. Controlling the flow of CUI is critical to the Pentagon's Cybersecurity Maturity Model Certification program, which aims to make acquisition officials and government contractors more aware of DOD information that is communicated throughout their supply chains. The Pentagon released a "Quick Reference Guide" brochure last week, which outlines categories of CUI and examples of how it should be marked in DOD documents. DOD also added a slide deck on CUI cleared for publication on April 1 that goes into more depth on its CUI website. The CUI program is a government-wide standard established by the National Archives and Records Administration. DOD has developed a mandatory CUI training for Pentagon contracting officials. "The course provides information on the 11 training requirements for accessing, marking, safeguarding, decontrolling and destroying CUI along with the procedures for identifying and reporting security incidents," according to the training website. CMMC level three focuses on the need to protect CUI and is largely built upon National Institute of Standards and Technology Special Publication 800-171.

Read the full article here.