ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

September 14, 2023

US FCC CHAIR SAYS CHINA'S IOT CELLULAR COMPONENTS MAKERS QUECTEL, FIBOCOM MAY POSE NATIONAL SECURITY RISKS

David Shepardson | South China Morning Post | September 7, 2023

Federal Communications Commission chairwoman Jessica Rosenworcel asked US government agencies to consider declaring that Chinese companies including Quectel and Fibocom Wireless pose unacceptable national security risks, according to letters seen by Reuters. The Republican chair of the House of Representatives China Select Committee, Mike Gallagher, and the top Democrat on the panel Raja Krishnamoorthi, asked the FCC last month to consider adding to its so-called Covered List the two companies that produce cellular modules that enable Internet of Things (IoT) devices to connect to the internet. Federal funds cannot be used to purchase equipment from companies on the list, and the FCC will not authorise new equipment from companies deemed national security threats. Rosenworcel wrote the FBI, the Justice Department, the National Security Agency, the Defence Department and other agencies on September 1, forwarding the request from the lawmakers.

Read the full article here.

ITALY SEEKS TO LEAVE CHINA'S BELT AND ROAD INITIATIVE—WITHOUT ANGERING BEIJING

Margherita Stancati | The Wall Street Journal | September 4, 2023

Italy is preparing to cancel its controversial membership in China's Belt and Road infrastructure initiative, engaging in an elaborate diplomatic dance to avoid angering Beijing and triggering retaliation against Italian businesses. Italian Foreign Minister Antonio Tajani held talks in Beijing on Sunday and Monday to facilitate as smooth an exit as possible from the initiative while laying the groundwork for alternative economic deals with China. "We didn't achieve great results with the Belt and Road, but that doesn't matter," Tajani told reporters in Beijing. "We are determined to move ahead with plans to strengthen our commercial ties." The Italian government of Prime Minister Giorgia Meloni has long signaled its discomfort with the Belt and Road memorandum that a previous Rome government signed with Chinese President Xi Jinping in 2019.

Read the full article here.

INSIGHT: CHINA QUIETLY RECRUITS OVERSEAS CHIP TALENT AS US TIGHTENS CURBS

Julie Zhu, Fanny Potkin, Eduardo Baptista and Michael Martina | Nextgov / Reuters | August 24, 2023

For a decade until 2018, China sought to recruit elite foreign-trained scientists under a lavishly funded program that Washington viewed as a threat to U.S. interests and technological supremacy. Two years after it stopped promoting the Thousand Talents Plan (TTP) amid U.S. investigations of scientists, China quietly revived the initiative under a new name and format as part of a broader mission to accelerate its tech proficiency, according to three sources with knowledge of the matter and a Reuters review of over 500 government documents spanning 2019 to 2023. The revamped recruitment drive, reported in detail by Reuters for the first time, offers perks including home-purchase subsidies and typical signing bonuses of 3 to 5 million yuan, or $420,000 to $700,000, the three people told Reuters.

Read the full article here.

THE CCP ABSORBS CHINA'S PRIVATE SECTOR: CAPITALISM WITH PARTY CHARACTERISTICS

Matthew Johnson | Hoover Institute | September 7, 2023

Headline-grabbing crackdowns on some of the best-known firms in the People's Republic of China (PRC) are not isolated phenomena. Rather, as this report by Hoover visiting fellow Matthew Johnson shows, the PRC's economic development has entered a new stage of development marked by a reassertion of party-state authority over areas where the private sector has grown rapidly or is threatening CCP General Secretary Xi Jinping's vision of socialism. Xi has launched a massive structural undertaking that harnesses private capital to restore the party's political authority across China's economic landscape, while preserving the technology and capital flows necessary to realize his ambition of making the PRC the world's dominant superpower. Xi's strategy incorporates three key agendas:

- **Offensive decoupling.** Decreasing the PRC's dependency on the world while making the world increasingly dependent on the PRC.

Read the full article here.

CHINA TO ITS PEOPLE: SPIES ARE EVERYWHERE, HELP US CATCH THEM

Vivian Wang | New York Times | September 3, 2023

Beijing sees forces bent on weakening it everywhere: embedded in multinational companies, infiltrating social media, circling naïve students. And it wants its people to see them, too. Chinese universities require faculty to take courses on protecting state secrets, even in departments like veterinary medicine. A kindergarten in the eastern city of Tianjin organized a meeting to teach staffers how to "understand and use" China's anti-espionage law. China's Ministry of State Security, a usually covert department that oversees the secret police and intelligence services, has even opened its first social media account, as part of what official news media described as an effort at increasing public engagement. Its first post: a call for a "whole of society mobilization" against espionage.

Read the full article here.

HOW CHINA DEMANDS TECH FIRMS REVEAL HACKABLE FLAWS IN THEIR PRODUCTS

Andy Greenberg | Wired | September 6, 2023

For State-Sponsored Hacking operations, unpatched vulnerabilities are valuable ammunition. Intelligence agencies and militaries seize on hackable bugs when they're revealed—exploiting them to carry out their campaigns of espionage or cyberwar—or spend millions to dig up new ones or to buy them in secret from the hacker gray market. But for the past two years, China has added another approach to obtaining information about those vulnerabilities: a law that simply demands that any network technology business operating in the country hand it over. When tech companies learn of a hackable flaw in their products, they're now required to tell a Chinese government agency—which, in some cases, then shares that information with China's state-sponsored hackers, according to a new investigation.

Read the full article here.

GOOGLE: STATE HACKERS ATTACK SECURITY RESEARCHERS WITH NEW ZERO-DAY

Sergiu Gatlan | BleepingComputer | September 7, 2023

Google's Threat Analysis Group (TAG) says North Korean state hackers are again targeting security researchers in attacks using at least one zero-day in an undisclosed popular software. Researchers attacked in this campaign are involved in vulnerability research and development, according to Google's team of security experts that protects the company's users from state-sponsored attacks. Google has yet to disclose details on the zero-day flaw exploited in these attacks and the name of the vulnerable software, likely because the vendor is still in the process of patching the vulnerability. "TAG is aware of at least one actively exploited 0-day being used to target security researchers in the past several weeks," Google TAG's Clement Lecigne and Maddie Stone said. "The vulnerability has been reported to the affected vendor and is in the process of being patched."

Read the full article here.

FUNDAMENTAL RESEARCH & NATIONAL SECURITY: RECENT DEVELOPMENTS & NEW ISSUES

Dorsey & Whitney LLP | JDSUPRA | September 7, 2023

According to the National Center for Science and Engineering Statistics ("NCSES"), a key driver in the scientific and technological accomplishments of U.S. research universities is the volume of federal support for research and development ("R&D"). In FY 2021, the U.S. Government supplied some $49 billion in R&D funding to U.S. institutions of higher education, and that contribution was 55% of total R&D spending in U.S. higher education.[1] Of that federal contribution, the Department of Defense ("DoD") supplied $7.4 billion or about 15% of all such federal research funding.[2] Three different national security measures are likely to affect such federal funding of U.S. research institutions, their principal investigators ("PIs") and their international research collaborations in the coming years: (1) the naming of more non-U.S. universities, academies, and institutes (particularly in China and Russia) to U.S. sanctions lists;

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.

TIKTOK’S SECRET EFFORT TO INFLUENCE AMERICAN HIGHER EDUCATION

Neetu Arnold | National Review | September 5, 2023

ByteDance, the parent company of the popular social-media site TikTok, has been vying for influence in the United States even as lawmakers grow concerned with the national-security risks associated with the platform, given its ties to China. Since 2019, ByteDance has spent nearly $18 million on lobbying the American government. But its eight-figure funding campaign to American universities has fallen under the radar. This is because all but one of the recipients of TikTok funds failed to properly report the donations to the Department of Education. Ten American universities signed gift agreements with TikTok, Inc., starting in late 2020 as part of TikTok’s Health Heroes Relief Fund initiative. All but one recipient university were minority-serving institutions, and they each received $1 million to “ensure the success of future Black, Latinx, and Indigenous health heroes.” The funds were meant to be distributed as scholarships to students pursuing medicine.

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