ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

December 1, 2021

EVEN ON U.S. CAMPUSES, CHINA CRACKS DOWN ON STUDENTS WHO SPEAK OUT

Sebastian Rotella | ProPublica | November 30, 2021

On the bucolic campus of Purdue University in Indiana, deep in America's heartland and 7,000 miles from his home in China, Zhihao Kong thought he could finally express himself. In a rush of adrenaline last year, the graduate student posted an open letter on a dissident website praising the heroism of the students killed in the Tiananmen Square massacre in 1989. The blowback, he said, was fast and frightening. His parents called from China, crying. Officers of the Ministry of State Security, the feared civilian spy agency, had warned them about his activism in the United States. "They told us to make you stop or we are all in trouble," his parents said. Then other Chinese students at Purdue began hounding him, calling him a CIA agent and threatening to report him to the embassy and the MSS. Kong, who goes by the nickname Moody, had already accepted an invitation from an international group of dissidents to speak at a coming online commemoration of the Tiananmen massacre anniversary. Uncertain if he should go through with it, he joined in rehearsals for the event on Zoom. Within days, MSS officers were at his family's door again. His parents implored him: No public speaking. No rallies. Moody realized it didn't matter where he was. The Chinese government was still watching, and it was still in charge. Just before the anniversary event, he reluctantly decided not to give his speech.

Read the full article here.

CHINA TIGHTENS ITS GRIP ON HONG KONG UNIVERSITIES

Dennis Normile | Science | November 30, 2021

When prodemocracy demonstrations erupted in Hong Kong in 2019, its publicly funded universities were hotbeds of unrest. A year later, five university presidents signed a statement supporting a law that would make such protests difficult if not impossible. Two did not sign the document, which endorsed the new National Security Law Beijing was about to pass: Wei Shyy of the Hong Kong University of Science and Technology (HKUST) and Kuo Way of the City University of Hong Kong. Both universities have now announced their presidents will step down. Kuo's departure is timed to the end of his third 5-year contract in 2023, by which time he'll be 72, dampening speculations about political pressure. But Shyy, 66, will resign in October 2022, a year before his contract ends. "Everybody is wondering what's his rationale for stepping down a year early," says Carsten Holz, a development economist at HKUST. Many other Hong Kong academics are leaving, too.

Read the full article here.

HEARING: HOW CHINA USES ECONOMIC COERCION TO SILENCE CRITICS AND ACHIEVE ITS POLITICAL AIMS GLOBALLY

U.S. Congressional – Executive Commission on China Hearing on December 7, 2021

The People's Republic of China uses a variety of coercive economic measures to silence criticism and influence discussion of its human rights violations in the United States and internationally. For example, recently China has stoked domestic boycotts of international brands that condemned forced labor in Xinjiang, and it continues to wage a high-profile, comprehensive campaign of economic coercion against Australia in response to criticism China deems sensitive. In addition, China recently has sanctioned individuals and companies, including Members of Congress and academic researchers, and taken significant steps to provide a legal basis for further measures. The Commission will hold a hearing that examines these challenges and developments in the context of China's international efforts to stifle criticism and achieve its political aims globally, spotlights the costs of China's economic coercion, and solicits recommendations from expert witnesses for further action by Congress and the Administration. The hearing will be livestreamed on the CECC's YouTube Channel.

Read the full article here.

CHINA MANIPULATING US ACADEMIC INSTITUTIONS OF REPUTE

Devdiscourse | November 28, 2021

Across western higher education, elite institutions are normalizing authoritarian political systems--such as the Chinese Communist Party (CCP)--when they should instead be under scrutiny. Georgia l. Gilholy writing for Newsweek magazine has alleged that academic institutions based in the US and the UK ranked high in repute have been manipulated for Chinese interest. She also alleged that Universities in the west that adhere to the principles of forming democratic institutions have pushed the notion that "Chinese-style" governance could be adopted by other countries. Georgia L. Gilholy is the media director at the Pinsker Centre and editor-in-chief for the Foundation for Uyghur Freedom. It's also a fact that the Chinese state and its linked corporations have been effective in their lobbying of university administrators despite the fact that other countries may find China's governing system impossible and unfavorable to internationally implement.

Read the full article here.

PATTERNS, TRENDS, ISSUES, CHALLENGES, AND OPPORTUNITIES IN THE INTERNATIONALIZATION OF CHINESE HIGHER EDUCATION

Xue Lang Rong and Shuguang Wang | Oxford | November 29, 2021

A theoretical model of positioned, positioning, and repositioning is used to conceptualize the evolving process of the internationalization of Chinese higher education and answer the following three questions: (a) How have the quantitative trends of Chinese students studying abroad and international students studying in China changed over the past 30 years? (b) What are the differences between Chinese students studying abroad and international students studying in China in recent years, in terms of the host and sending countries, the level of study, and the fields of study, and what do the differences mean when compared to those in other countries? (c) What are the challenges, opportunities, and strategies in the years to come? To answer the first question, a compilation of descriptive quantitative data is used from numerous large national and international data sources, which reports a long-term upward trend (with some fluctuations) of inbound international students in China and outbound Chinese international students around the world over the past 30 years.

Read the full article here.

AS U.S. HUNTS FOR CHINESE SPIES, UNIVERSITY SCIENTISTS WARN OF BACKLASH

Amy Qin | The New York Times | November 28, 2021

The F.B.I. agents spent nearly two years tailing the professor, following him to work, to the grocery store, and even keeping his college-age son under surveillance. They told the university where he held a tenured position that he was a Chinese operative, prompting the school to cooperate with their investigation and later fire him. But the F.B.I. was unable to find evidence of espionage, according to an agent's testimony in court. Federal prosecutors pressed charges anyway, accusing Anming Hu of concealing his ties with a university in Beijing and defrauding the government in connection with research funds he had received from NASA. The trial ended in a hung jury. One juror called the case "ridiculous." In September, a judge took the rare step of acquitting the Chinese-born scientist on all counts. "It was the darkest time of my life," Dr. Hu said in his first in-depth interview since being acquitted. Universities in the United States once welcomed the best and brightest scientific talents from around the world.

Read the full article here.

BIOMETRICS, SMARTPHONES, SURVEILLANCE CAMERAS POSE NEW OBSTACLES FOR U.S. SPIES

Warren P. Strobel | The Wall Street Journal | November 27, 2021

Operatives widely suspected of working for Israel's Mossad spy service planned a stealthy operation to kill a Palestinian militant living in Dubai. The 2010 plan was a success except for the stealth part—closed-circuit cameras followed the team's every move, even capturing them before and after they put on disguises. In 2017, a suspected U.S. intelligence officer held a supposedly clandestine meeting with the half brother of North Korean leader Kim Jong Un, days before the latter was assassinated. That encounter also became public knowledge, thanks to a hotel's security camera footage. Last December , it was Russia's turn. Bellingcat, the investigative website, used phone and travel data to track three operatives from Moscow's FSB intelligence service it said shadowed and then attempted to kill Russian opposition politician Alexei Navalny. Bellingcat named the three. And published their photographs. Espionage and covert action aren't what they used to be. A trained CIA case officer could once cross borders with a wallet full of aliases or confidently travel through foreign cities undetected to meet agents.

Read the full article here.

NCSC WARNS INDUSTRY, ACADEMIA OF FOREIGN THREATS TO THEIR INTELLECTUAL PROPERTY

Christopher Burgess | CSO | November 25, 2021

CISOs of companies both small and large understand how intellectual property (IP) and company infrastructure may be targeted from one of four vectors: malevolent insiders, unscrupulous competitors, criminals, or nation states. While ransomware attacks emphasize how criminals monetize their ability to socially engineer individuals to click that link or attachment, nation states are quietly working to fleece the IP and gain foothold within targets of interest. The U.S. National Counterintelligence and Security Center (NCSC—an entity within the Office of the Director of National Intelligence) recently published a ten-page primer on the targeting of emerging U.S. technologies by these foreign threats. The primer cites artificial intelligence, the bioeconomy, autonomous systems, quantum information science and technology, and semiconductors as key sectors being targeted by foreign adversaries. But by no means are those the only sectors being targeted.

Read the full article here.

US MANUFACTURING DECLINE IS HURTING NATIONAL SECURITY, REPORT WARNS

Marcus Weisgerber | Defense One | November 16, 2021

Unless the federal government helps train two million extra workers by 2030 and spends $100 billion annually to improve American manufacturing, the U.S. economy may become unable to keep up with China's national-security threats, a new think tank report warns. The findings of a study conducted by the conservative Ronald Reagan Institute arrive as supply chain meltdowns highlight the U.S. reliance on foreign-made items and the tired American infrastructure that brings them from ports to domestic assembly lines. "Our declining manufacturing competitiveness leaves America's economic infrastructure and defense capabilities underprepared for geopolitical events, global competition, and even major armed conflict," the report states. "To revive our manufacturing base and maintain our edge as the world's leading economy, the United States must employ innovative thinking from both the public and private sectors." But there's no easy fix.

Read the full article here.

CHINA'S 5 BIG TECH ISSUES FOR 2022

Arjun Kharpal | CNBC | November 24, 2021

China's technology sector has taken a wild ride over the past year, with regulations tightened, billions of dollars wiped off companies' market value, and a continuing push from Beijing for technological self-sufficiency. Those are among the important themes that will be addressed at CNBC's annual East Tech West event in the Nansha district of Guangzhou in southern China. Here's a look at the top concerns and focuses of China's technology sector right now. In November 2020, what would have been a world record-setting initial public offering of fintech giant Ant Group was suspended. Following that, Beijing introduced a slew of new rules in areas from antitrust for internet platforms and a bolstered data protection law. Both e-commerce giant Alibaba and food delivery firm Meituan have faced antitrust fines. That has weighed heavily on China's internet names. For example, Alibaba's shares are down 41% year-to-date. Several questions are swirling: Will China introduce more new regulation and in what areas? What companies could be targeted next? What does it mean for growth of the tech sector in China? CNBC tackled some of this in a recent episode of the "Beyond the Valley" podcast below. Those conversations will continue at East Tech West.

Read the full article here.

PALANTIR CEO SAYS COMPANIES WORKING WITH U.S. ADVERSARIES SHOULD JUSTIFY THEIR POSITION

Samantha Subin | CNBC | November 23, 2021

Technology companies doing business with China or U.S. adversaries need to justify their position, Palantir CEO Alex Karp told CNBC's "Squawk Box" on Tuesday. "If you want to work in China or in any other country that is adversarial … you should disclose it and defend it," he said. Apple and many chip companies are among the major U.S. tech firms that continue to operate in China. The comments from Karp come as more tech companies pull out of the country amid harsher internet censorship. Most recently, Yahoo said it was leaving China and Microsoft said in October it would shut down professional networking platform LinkedIn and replace it with a jobs board. Google decided to shutter operations in 2010 and social media platforms including Twitter and Facebook have been blocked for more than a decade. Apple's CEO Tim Cook recently responded to questions about operating in China..

Read the full article here.

REPORT: CHINA MAY STEAL ENCRYPTED GOVERNMENT DATA NOW TO DECRYPT WITH QUANTUM COMPUTERS LATER

Brandi Vincent | Nextgov | November 22, 2021

Though they are years from being fully realized, quantum technologies are altering the U.S. cyber threat landscape in serious ways and organizations should start acting now to ensure their infrastructure and data will be protected as the field evolves, according to a new report from Booz Allen Hamilton. In the recently released 32-page document, experts warn that China, specifically, has become a major player in quantum computing and will likely soon collect encrypted American data in hopes to eventually decrypt it when the advanced quantum systems go into operation. "Quantum computing is a rapidly evolving technology with far-reaching disruptive potential, and China is a leading developer of it," BAH's Head of Strategic Cyber Threat Intelligence Nate Beach-Westmoreland told Nextgov. "So, Booz Allen wanted to know how and when Chinese cyber threats might be shaped by this change to help our clients manage their changing risk profile."

Read the full article here.

VICKIE DOESN'T EXIST: DEEPFAKES IN YOUR LINKEDIN

Patrick Miller | Ampere Industrial Security | November 16, 2021

LinkedIn is for making connections. But you may be forming connections with fake people trying to break into your world and cause destruction. We found a deepfake profile that's already racked up hundreds of potentially sensitive connections on LinkedIn. And she's still going. Is she ---or someone like her --- on your connections list? I received a connection request from a person claiming to be Vickie O'Shea-Fowler from Raleigh, North Carolina, CEO of a company called Data Smart Consulting. Behind her vague smile, Vickie hides a secret. She's not real. Just a computer-generated face. " Vickie's asymmetrical earrings are a dead giveaway aside from the uncanny-valley-esque smile," said deepfake researcher Max Rizzuto with the Atlantic Council's Digital Forensic Research Lab. "Anyone who hides behind a false face likely has something to hide or an ulterior motive in mind." She spread a broad net on LinkedIn, connecting with many people. Of special note, she's connected with hundreds in security and tech. "It's disturbing," said Susan Embry-Busch, a contractor at Nike and one of the people on Vickie's connection list. "It concerns me about what the ultimate goal is."

Read the full article here.

UK INTRODUCES NEW CYBERSECURITY LEGISLATION FOR IOT DEVICES

James Coker | Info Security | November 24, 2021

The UK government has today introduced new legislation to Parliament that aims to better protect consumers' IoT devices from hackers. The Product Security and Telecommunications Infrastructure (PSTI) Bill places new cybersecurity standards on manufacturers, importers and distributors of internet-connectable devices, such as phones, tablets, smart TVs and fitness trackers. The legislation will also apply to products that can connect to multiple other devices but not directly to the internet, like smart light bulbs and smart thermostats. These requirements include banning universal default passwords, forcing firms to be transparent about actions they are taking to fix security flaws in their products and creating a better public reporting system for any vulnerabilities discovered. In addition, these companies will have a duty to investigate compliance failures, produce statements of compliance and maintain appropriate records of this.

Read the full article here.

PENTAGON DETAILS CHINA'S INFORMATION WAR AGAINST THE UNITED STATES

Bill Gertz | World Public News | November 2021

China is engaged in influence operations targeting American society in an effort to bolster support for the policies and strategies of the communist nation, according to the Pentagon's latest annual report on the Chinese military. "The PRC conducts influence operations, which target cultural institutions, media organizations, businesses, universities and political communities in the United States, other countries and international institutions, to achieve results favorable to its strategic objectives, "the report says. Little academic research has been done in the United States to track influence operations, which have been successful in shaping Americans' understanding of China. Many media and think tanks often reflect Chinese government propaganda and messages, such as the theme that China poses no threat to the United States. Beijing uses its funding and access to travel to China as a means of influencing US institutions to avoid criticizing threatening activities such as human rights violations and China's spread of nuclear weapons and equipment in the world. The ruling Chinese Communist Party (CCP) "seeks to condition domestic, foreign and multilateral political establishments and public opinion to accept Beijing's narratives and remove obstacles preventing the achievement of the goals," the 192-page report says. . Communist leaders in Beijing believe that open democratic societies are more sensitive to its influence operations.

Read the full article here.