ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

February 3, 2021

US ASKS TAIWAN TO FILL VOID AS CONFUCIUS INSTITUTES CLOSE

Nick A. Spinwall | Nikkei Asia | February 2, 2021

As Confucius Institutes are shuttered across university campuses in America due to academic freedom concerns, the top U.S. representative to Taiwan is calling on the Mandarin-speaking democracy to fill the void. Taiwan can "play a key role" in addressing interest among U.S. students in learning Mandarin -- and should use the opportunity to tout its culture and democracy, Brent Christensen, director of the American Institute in Taiwan, told Nikkei Asia. Confucius Institutes, which offer Mandarin language and culture classes on U.S. campuses, are being closed rapidly by host universities concerned about Chinese Communist Party influence on their academic freedom. The U.S. State Department labeled its headquarters a "foreign mission" of China last August, hastening their decline. "The CCP considers Taiwan -- and many other subjects -- to be politically sensitive," Christensen said. "China's sensitivities should not dictate the academic environment or curriculum on U.S. campuses."

Read the full article here.

SCRUTINY OF CHINESE RESEARCHERS THREATENS INNOVATION

Caroline Wagner | University World News | January 30, 2021

The arrest of Massachusetts Institute of Technology (MIT) Engineering Professor Gang Chen on 14 January has drawn attention to the role of China in the United States science and technology system. It's not the first time that suspicions have fallen on a Chinese-born scientist – Chen is a naturalised US citizen – for work they conduct openly in the United States. The charges against Gang Chen – wire fraud, failing to report a foreign bank account and a false statement on a tax return – stem from failing to disclose Chinese funding for his research. MIT called the allegations "distressing", and the school's president and 100 faculty members are defending a Chinese university's investment in MIT research. No evidence of spying has been made public, but a Department of Justice criminal complaint expressed suspicions that Chen's loyalty may not be aligned with American interests.

Read the full article here.

NEW CISOS SURVEY REVEALS HOW SMALL CYBERSECURITY TEAMS CAN CONFRONT 2021

The Hacker News | January 29, 2021

The pressure on small to medium-sized enterprises to protect their organizations against cyberthreats is astronomical. These businesses face the same threats as the largest enterprises, experience the same (relative) damages and consequences when breaches occur as the largest enterprises but are forced to protect their organizations with a fraction of the resources as the largest enterprises. Cybersecurity company Cynet just released findings from a survey of 200 CISOs in charge of small security teams (Download here) to shine "a spotlight into the challenges of small security teams everywhere." In addition to better understanding the challenges these CISOs face, the 2021 Survey of CISOs with Small Security Teams delves into the strategies CISOs will employ to ensure their organizations are protected from the ongoing onslaught of cyber threats - all while saddled with limited budgets and headcount.

Read the full article here.

DEMAND FOR TRANSPARENCY IN RESEARCH MISCONDUCT PROBES

Yojana Sharma | University World News | January 28, 2021

A prominent scientist and president of a prestigious university investigated by Chinese authorities for alleged data falsification has been cleared of plagiarism and research fraud, but the high-profile exoneration has attracted criticism and renewed focus on China's policing of research misconduct. In particular, academics have called for more transparency over the workings of such high-level ethics panels investigating prominent individuals. Immunologist Cao Xuetao, who is president of Nankai University in the port city of Tianjin, and an academician of the Chinese Academy of Engineering, came under investigation in late 2019 when San Francisco-based microbiologist Elisabeth Bik uncovered alleged problems related to 'misused images' in several articles authored by Cao, and then flagged up almost 60 papers by the same author regarded as problematic.

Read the full article here.

CHINESE INNOVATION IS SURGING — WE MUST FUND SCIENCE TO COMPETE

Neal Lane and Norman Augustine | The Hill | January 26, 2021

When America seeks to address a crisis or achieve preeminence, it looks to science. This is true whether the issue is the economy, climate change, national security or even a pandemic. And yet, today, Americans spend more on potato chips than on energy research. For President Biden and the new Congress, the time is now for new thinking about how we prioritize and fund science, as well as public primary and secondary education. In 2019 we spent one tenth of one percent of the GDP on biomedical basic research but nearly 18 percent of the GDP on health care. And what of overall competitiveness? Mainland China is increasing research and development investment by double digit percentages each year while U.S. investment, as a percentage of GDP, has remained stagnant for nearly half a century. China is close to passing the United States in total R&D investment based on purchasing power parity. China's entire GDP is projected to pass that of the United States, using currency exchange rates, by around the end of the decade. If PPP conversion is applied to GDP, China passed the United States several years ago.

Read the full article here.

CHINESE BIOTECH FIRM OFFERED TO BUILD COVID LABS IN US, LIKELY TO TRY TO COLLECT AMERICANS' DNA: REPORT

Peter Aitken | Fox News | January 29, 2021

A Chinese company offered to build COVID-19 testing labs in the U.S. at the start of the pandemic, with intelligence officials warning it might have been an effort to collect DNA from American citizens, according to a "60 Minutes" report. BGI Group, touted as the largest biotech firm in the world, offered to build and run testing labs in Washington, New York and California, among other states. The offer raised suspicions and led Bill Evanina, then-director of the National Counterintelligence and Security Center, to warn the states against the offer. "Foreign powers can collect, store and exploit biometric information from COVID tests," Evanina said in a public notice, according to "60 Minutes." Evanina, like many officials, worries that China might use companies like BGI Group to collect biodata, which he believes poses a national security threat as the world starts to pay more attention to such assets. Biodata can determine the path of health care, indicating the kinds of medical concerns prevalent now or in the future, allowing an entity to create a monopoly over the therapy or drugs necessary to treat them, he told "60 Minutes."

Read the full article here.

RUSSIAN HACK OF US AGENCIES EXPOSED SUPPLY CHAIN WEAKNESSES

Eric Tucker | The Associated Press | January 25, 2021

The elite Russian hackers who gained access to computer systems of federal agencies last year didn't need to painstakingly break one-by-one into the networks of each department in order to do damage. Instead, they got inside by sneaking malicious code into a software update pushed out to thousands of government agencies and private companies. That hackers were able to exploit vulnerabilities in the supply chain to launch a massive intelligence gathering operation wasn't especially surprising. U.S. officials and cybersecurity experts have sounded the alarm for years about a problem that has caused havoc, including billions of dollars in financial losses, while also defying easy solutions from the government and private sector. "We're going to have to wrap our arms around the supply-chain threat and find the solution, not only for us here in America as the leading economy in the world, but for the planet," William Evanina, who resigned last week as the U.S. government's chief counterintelligence official, said in an interview.

Read the full article here.

THE WEST NEEDS TO RESPOND TO CHINA'S BID FOR TECHNOLOGY DOMINANCE: NEW REPORT

The London School of Economics and Political Science | January 28, 2021

Western countries urgently need to develop a coordinated response to China's growing dominance in the development of new technology. This is one of the key findings from a new report from LSE IDEAS, a foreign policy think tank based at the London School of Economics and Political Science (LSE). In the new report, 'Protect, Constrain, Contest', published this week, academics and China watchers set out the important policies needed to put Western relationships with China on a firmer and more manageable footing. The report details concerns about China's selective adherence to international trade rules, the use of investment in foreign companies to gain access to and control of advanced technologies and its abuse of economic power through unilateral and punitive tariffs. It provides recommendations as to how allies can present a coordinated front against such practices.

Read the full article here.

FRIEND OR FOE? THE DOC ISSUES NEW INTERIM RULE ON TRANSACTIONS INVOLVING INFORMATION AND COMMUNICATION TECHNOLOGY OR SERVICES ("ICTS") AND FOREIGN ADVERSARIES

J. Scott Maberry, Fatema Merchant, and Mario Andres Torrico | JD Supra | January 28, 2021

On January 19, 2021, the U.S. Department of Commerce ("DOC") issued an interim final rule governing transactions in Information and Communication Technology or Services ("ICTS") involving "foreign adversaries." Although the rule takes effect on March 22, 2021, it allows DOC to review covered transactions initiated, pending, or completed on or after January 19, 2021. The interim rule grants DOC the authority to regulate certain transactions between U.S. persons and foreign adversaries involving ICTS that pose under or unacceptable risks. The DOC is accepting public comments on the rule through March 31, 2021. The rules are designed to implement EO 13873, issued on May 15, 2019, entitled "Securing the Information and Communications Technology and Services Supply Chain." That EO sought to address concerns that foreign adversaries are exploiting ICTS to economic and industrial espionage and other adverse actions against the U.S.[2] The new rules follow the issuance of a proposed rule on November 26, 2019 (see our prior post here).

Read the full article here.

BIDEN'S DOJ NEEDS TO END WAR ON CHINESE-AMERICAN SCIENTISTS

Peter R. Zeidenberg | Bloomberg Law | January 28, 2021

The Biden Justice Department needs to reevaluate the Trump administration's "China Initiative" and refocus its enforcement priorities on the harm it was meant to address—the theft of trade secrets by China—and put an end to harassment of supremely talented Chinese-American scientists in the U.S., says Arent Fox partner Peter R. Zeidenberg. For the past two years, the Department of Justice has waged a short-sighted and highly counter-productive war against Chinese-American scientists. The stated purpose of this assault was to stop the theft of intellectual property from the U.S. by China. But the impact has landed on dedicated, talented and patriotic Chinese-American scientists who, despite having stolen nothing, are being summarily dismissed from tenured positions and prosecuted for what amounts to paperwork errors.

Read the full article here.

A SCIENTIST IS ARRESTED, AND ACADEMICS PUSH BACK

Ellen Barry | The New York Times | January 26, 2021

It was Donald J. Trump's last full week in office, so Andrew E. Lelling, the federal prosecutor in Boston, knew he had limited time left in his job. But there was one more important arrest to announce, one that had been in the works for more than a year and would burnish his record on a key initiative of his tenure. Police officers that morning had arrested Gang Chen, a professor of mechanical engineering at the Massachusetts Institute of Technology, on suspicion of hiding affiliations with Chinese government institutions in order to secure $19 million in U.S. federal grants. Dr. Chen's prosecution was the latest in the Justice Department's two-year-old China Initiative, which aims to root out research scientists passing sensitive technology to China. At a news conference that morning, Mr. Lelling said he believed that Dr. Chen, 56, who became a naturalized U.S. citizen two decades ago, had remained loyal to the country of his birth.

Read the full article here.

CHINESE ESPIONAGE THREATENS U.S. TELECOM SECURITY, EX-FCC HEAD SAYS

D. Howard Kass | MSSP Alert | January 24, 2021

Chinese cyber spying poses the greatest threat to U.S. telecommunication networks and internet freedom, former Trump administration Federal Communications Commission (FCC) chairman Ajit Pai said in a recent interview. Pai, who served as FCC chairman beginning in 2017, relinquished his post on January 20 to Jessica Rosenworcel, installed as acting FCC chairwoman by new President Joseph Biden. Federal regulators will be hard pressed to secure telecommunications from Chinese state sponsored cyber surveillance, economic espionage and network malware attacks, Pai told Reuters. "There are a number of bad things that can happen when insecure equipment is used to handle sensitive information," he said. During his three year term, Pai supported securing the nation's communications networks from foreign cyber intrusion, backing a ban on Chinese telecom suppliers Huawei and ZTE over concerns surveillance back doors would be baked into their equipment.

Read the full article here.

WHAT THE COLD WAR CAN TEACH WASHINGTON ABOUT CHINESE TECH TENSIONS

Brendan Thomas-Noone | Brookings | January 12, 2021

In a 1982 speech, then-U.S. Secretary of Defense Caspar W. Weinberger warned that the United States had for the better part of a decade facilitated unfettered technological transfer and trade with the Soviet Union. This high-tech transfer, the secretary argued, was being done through "legal and illegal channels" and was effectively the technological "rope to hang us," as it was bolstering Soviet military capability. Replace the Soviet Union with China, and the themes of Weinberger's speech would not seem out of place today. At the time, a strategic competitor appeared to be rapidly advancing on U.S. technological superiority through a concerted campaign of technology transfer, aided by U.S. scientific engagement policies, an open academic system, and intellectual property theft. In some cases, this had been abetted by U.S. high-tech trade with the Soviets over the previous decade: The sale of advanced ball bearing machines had helped improve the accuracy of Soviet missiles, the Pentagon chief declared.

Read the full article here.

DELIVER UNCOMPROMISED: SECURING CRITICAL SOFTWARE SUPPLY CHAINS

Dr. Charles Clancy, Joe Ferraro, Robert A. Martin, Adam G. Pennington, Christopher L. Sledjeski, and Dr. Craig J. Wiener | Mitre | January 2021

A series of actions, if taken by the software development community and the larger information technology ecosystem, can significantly reduce the risk of compromise, exploitation, exfiltration, or sabotage from software supply chain attacks. While no silver bullet exists, establishing and implementing an end-to-end framework for software supply chain integrity will reduce risks from too-big-to-fail applications that are central to private sector enterprises, governments, and the critical capabilities they rely upon each day. The current state of practice in software supply chain security lacks systematic integrity. There are insufficient interoperable tools for preventing, detecting, or remediating software supply chain attacks that go beyond tools available for general cybersecurity threats. Given the potential impacts from software supply chain attacks, we cannot treat them as just another cybersecurity breach.

Read the full article here.

MITRE RELEASES "DELIVER UNCOMPROMISED" STUDY ON CONFRONTING NEW ASYMMETRIC THREATS

Jeremy Singer | Mitre | August 13, 2018

Just as U.S. supply convoys faced sniper fire as they moved through Iraq and Afghanistan, our entire national security supply chain, from conception to retirement, provides opportunities for adversaries to target critical warfighting capabilities and undermine the confidence of mission owners. MITRE has released "Deliver Uncompromised," a report that makes recommendations on how the U.S. government and private sector can address growing asymmetric threats like counterfeit parts that pass ordinary inspection but fail operationally and malware that exploits latent vulnerabilities in firmware or software and threaten unintended or unexpected physical results. "Make no mistake, our adversaries are working right now to steal intellectual property, compromise technical information, and degrade, deny, or potentially destroy, critical infrastructure, assets, and capabilities," said Dr. Jason Providakes, MITRE president and CEO. "In the same way we have taken advantage of technology offsets to stay ahead of our adversaries, we must ensure they don't flip the script and target our critical areas, which are often part of the supply chain."

Read the full article here.