ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

December 9, 2020

POMPEO SAYS MANY U.S. COLLEGES ARE 'BOUGHT BY BEIJING' FUNDING

David Wainer | Bloomberg | December 9, 2020

Secretary of State Michael Pompeo accused U.S. universities of letting China steal American science and technology and stifle criticism in return for funding from Beijing. "What more bad decisions will schools make because they are hooked on communist cash?" he said Wednesday at the Georgia Institute of Technology in Atlanta. "What professors will they silence? What theft and espionage will they overlook?" Arguing that the Chinese communist party is "poisoning the well" of U.S. higher education, Pompeo called for "rigorous" oversight of students and scholars from China. President Donald Trump and his administration are piling pressure on Chinese's President Xi Jinping and the ruling Communist Party in his final weeks in office before President-elect Joe Biden takes over. Pompeo accused "left-leaning college campuses" of being rife with anti-Americanism, presenting easy "target audiences for their anti-American messaging." "So many of our colleges are basically bought by Beijing," he said.

Read the full article here.

FIREEYE, A TOP CYBERSECURITY FIRM, SAYS IT WAS HACKED BY A NATION-STATE

David E. Sanger and Nicole Perlroth | The New York Times | December 8, 2020

For years, the cybersecurity firm FireEye has been the first call for government agencies and companies around the world who have been hacked by the most sophisticated attackers, or fear they might be. Now it looks like the hackers — in this case, evidence points to Russia's intelligence agencies — may be exacting their revenge. FireEye revealed on Tuesday that its own systems were pierced by what it called "a nation with top-tier offensive capabilities." The company said hackers used "novel techniques" to make off with its own tool kit, which could be useful in mounting new attacks around the world. It was a stunning theft, akin to bank robbers who, having cleaned out local vaults, then turned around and stole the F.B.I.'s investigative tools. In fact, FireEye said on Tuesday, moments after the stock market closed, that it had called in the F.B.I.

Read the full article here.

MORE THAN 1,000 VISITING RESEARCHERS AFFILIATED WITH THE CHINESE MILITARY FLED THE UNITED STATES THIS SUMMER, JUSTICE DEPARTMENT SAYS

Ellen Nakashima | The Washington Post | December 2, 2020

Following an FBI investigation this summer, more than 1,000 researchers who had hidden their affiliation with the Chinese military fled the United States, the Justice Department said Wednesday. The exodus came in the wake of the arrests of six Chinese researchers accused of lying on their visa applications about their ties to the People's Liberation Army and a warning to the Chinese ambassador that individuals who had not disclosed their true status needed to leave or face arrest. The figure is startling, and some experts and former FBI officials said the actual number of researchers who currently work for the PLA is likely far lower. It is plausible, they said, that all had some affiliation to the military at some point and would be vulnerable to pressure to spy for the government. The Chinese Embassy did not respond to a request for comment. In July, the Justice Department announced the indictments of six Chinese individuals accused of concealing their PLA ties.

Read the full article here.

HOW THE BIDEN ADMINISTRATION CAN MAKE THE U.S. A TOP DESTINATION FOR INTERNATIONAL STUDENTS

M. Peter McPherson | Forbes | December 7, 2020

The number of new international students enrolling at U.S. universities fell by 43% this year, according to a new report. A decline in international enrollment — even a significant one — is to be expected in a global pandemic, of course. More worrying is the fact the decline marks the fourth consecutive year of decreased enrollment among new international students. The trend is the result of many factors, but also unmistakably a function of less welcoming federal policies and harsh rhetoric from some policymakers over the past four years. The effect on higher education has been profound. Left unaddressed, diminished international student enrollment will take a toll on our country's economic competitiveness as well. President-elect Biden has already emphasized the importance of immigrants' manifold contributions to our society and economy.

Read the full article here.

OPPORTUNITIES FOR INTERNATIONAL RECRUITMENT POST-PANDEMIC

Adrian Mutton | University World News | December 2, 2020

United States international student enrolments this fall semester dropped by more than 40% amid COVID-19 disruptions, but even before the pandemic, international students were beginning to look elsewhere for an education. We all knew that international student enrolments at US universities would be down this term as a result of the pandemic – the recent Open Doors Report has confirmed this supposition. But what happens after the dust clears? How will US institutions gain traction with students who have been mulling their study abroad plans from the sidelines? The Open Doors Report released by the Institute of International Education contained a 'snapshot' survey of 700 US colleges and universities that indicated a 43% decline in new international enrolments for the current semester, with a 16% fall in international enrolments overall. After a jittery year of travel bans, visa office closures, cancelled standardised test dates and infection spikes across the country, it's not hard to see why this would be the outcome.

Read the full article here.

CHINESE RESEARCHER PLEADS GUILTY TO MAKING FALSE STATEMENTS TO FEDERAL AGENTS

U.S. Department of Justice | December 3, 2020

A Chinese national pleaded guilty today in federal court in Boston to making false statements in connection with his theft of 21 vials of biological research. Zaosong Zheng, 31, pleaded guilty to one count of making false, fictitious or fraudulent statements. U.S. District Court Judge Denise J. Casper scheduled sentencing for January 6, 2021. According to the terms of the plea agreement, Zheng has agreed to a judicial order of removal from the United States after his sentencing hearing. Zheng was arrested on Dec. 10, 2019, at Boston's Logan International Airport and charged by criminal complaint. In August 2018, Zheng entered the United States on a J-1 visa and conducted cancer-cell research at Beth Israel Deaconess Medical Center in Boston from Sept. 4, 2018, to Dec. 9, 2019. On Dec. 9, 2019, Zheng stole 21 vials of biological research, hid them in his luggage, and attempted to take them out of the United States aboard a flight destined for China. Federal officers at Logan Airport discovered the vials hidden in a sock inside one of Zheng's bags, and not properly packaged.

Read the full article here.

CHINA HAS DONE HUMAN TESTING TO CREATE BIOLOGICALLY ENHANCED SUPER SOLDIERS, SAYS TOP U.S. OFFICIAL

Ken Dilanian | NBC News | December 3, 2020

U.S. intelligence shows that China has conducted "human testing" on members of the People's Liberation Army in hope of developing soldiers with "biologically enhanced capabilities," the top U.S. intelligence official said Friday. John Ratcliffe, the director of national intelligence, included the explosive claim in a long Wall Street Journal op-ed in which he made the case that China poses the pre-eminent national security threat to the U.S. "There are no ethical boundaries to Beijing's pursuit of power," wrote Ratcliffe, a Republican former member of Congress from Texas. His office and the CIA did not immediately respond to requests to elaborate on the notion that China sought to create "super soldiers" of the sort depicted in Hollywood films like "Captain America," "Bloodshot" and "Universal Soldier."

Read the full article here.

PHYSICISTS IN CHINA CHALLENGE GOOGLE'S 'QUANTUM ADVANTAGE'

Philip Ball | Nature | December 3, 2020

A team in China claims to have made the first definitive demonstration of 'quantum advantage' — exploiting the counter-intuitive workings of quantum mechanics to perform computations that would be prohibitively slow on classical computers. They have used beams of laser light to perform a computation which had been mathematically proven to be practically impossible on normal computers. The team achieved within a few minutes what would take half the age of Earth on the best existing supercomputers. Contrary to Google's first demonstration of a quantum advantage, performed last year, their version is virtually unassailable by any classical computer. The results appeared in Science on 3 December. "We have shown that we can use photons, the fundamental unit of light, to demonstrate quantum computational power well beyond the classical counterpart," says Jian-Wei Pan at the University of Science and Technology of China in Hefei. He adds that the calculation that they carried out — called the boson-sampling problem — is not just a convenient vehicle for demonstrating quantum advantage, but has potential practical applications in graph theory, quantum chemistry and machine learning.

Read the full article here.

CHINA USING LINKEDIN TO RECRUIT SPIES

Vision Times | December 2, 2020

The Chinese government is using LinkedIn profiles to hire spies, says James Olson, who has spent 30 years working for the CIA and is presently a professor at Texas A&M University. In addition, Chinese agents are also targeting foreign students as potential spies. Social media platforms like LinkedIn provide detailed professional histories and other personal information of individuals. This allows Chinese agents to identify people they should target and convert into spies. Such targets are often people who have access to critical American technologies and innovative research. Olson says that China's information gathering is like a "tidal wave" and that most professionals are completely oblivious that they are being targeted for espionage. According to Olson, such professionals come from a culture where it is okay to collaborate with others and share research. As such, these professionals tend to overlook the fact that there are people who are looking to exploit them because of their background.

Read the full article here.

JAPAN STEPS UP PROTECTION OF RESEARCH FROM ESPIONAGE

Suvendrini Kakuchi | University World News | December 2, 2020

Against a backdrop of growing hostility between China and the United States, Japan is beefing up measures to protect university scientific research from foreign espionage. Experts say this also reflects Tokyo's geopolitical interests in line with the US-Japan security partnership signed in 1960. A news report by Japan's Kyodo News agency on 30 November indicated 45 national, private and public universities in Japan had agreements on academic or student exchange programmes with seven universities in China which have ties to China's People's Liberation Army (PLA) and may involve technology relating to military use. Some of the universities in China are on the US embargo list such as Beihang University (formerly Beijing University of Aeronautics and Astronautics) in Beijing, Harbin Engineering University and Harbin Institute of Technology. While some Japanese universities, including Chiba Institute of Technology, have discontinued joint research with Chinese military-linked institutions, Japan's Hokkaido University and Osaka University, which conduct joint research with PLA-linked counterparts on nanotechnology and nuclear research respectively, will continue with the programme, according to Kyodo.

Read the full article here.

CHINA AIMS ITS INFLUENCE OPERATIONS AT INCOMING BIDEN ADMINISTRATION, TOP INTEL OFFICIAL SAYS

Sean Lyngaas | CyberScoop | December 2, 2020

China has increased its influence operations targeting incoming Biden administration personnel and their associates since the presidential election, the top U.S. counterintelligence official said Wednesday. "We're starting to see that now play [out] across the country, to not only the folks who are in the new administration, but those who are around those folks in the new administration," William Evanina, who heads the National Counterintelligence and Security Center, said at an online event hosted by the Aspen Institute. Evanina did not elaborate on what the Chinese influence activity entailed. But another U.S. intelligence official told CyberScoop it included intelligence collection and efforts to shape U.S. policy. Evanina did say that China had engaged in an "uptick" in influence operations since the Nov. 3 election of Joe Biden that were focused on the president-elect's advisers. Chinese influence activity in the past has included amplification of state-controlled media outlets and other means of reaching a domestic U.S. audience.

Read the full article here.

OFFICIAL: OVER 1,000 CHINESE RESEARCHERS HAVE LEFT US AMID TECH THEFT CRACKDOWN

Reuters | VOA | December 2, 2020

More than 1,000 Chinese researchers have left the United States amid a U.S. crackdown on alleged technology theft, John Demers, the U.S. Justice Department's top national security official, said Wednesday. William Evanina, chief of the counterintelligence branch of the office of the U.S. Director of National Intelligence, told the same Aspen Institute Cyber Summit that Chinese agents already were targeting personnel of the incoming administration of President-elect Joe Biden, as well as "people close" to Biden's team. A Justice Department official said the researchers to which Demers referred were a different group than those mentioned by the State Department in September, when it said the U.S. had revoked visas for more than 1,000 Chinese nationals under a presidential measure denying entry to students and researchers deemed security risks. China described that move as "naked" political persecution and racial discrimination that seriously violated human rights.

Read the full article here.

IBM RELEASES REPORT ON CYBER ACTORS TARGETING THE COVID-19 VACCINE SUPPLY CHAIN

U.S. Cybersecurity & Infrastructure Security Agency | December 3, 2020

IBM X-Force has released a report on malicious cyber actors targeting the COVID-19 cold chain—an integral part of delivering and storing a vaccine at safe temperatures. Impersonating a biomedical company, cyber actors are sending phishing and spearphishing emails to executives and global organizations involved in vaccine storage and transport to harvest account credentials. The emails have been posed as requests for quotations for participation in a vaccine program. The Cybersecurity and Infrastructure Security Agency (CISA) encourages Operation Warp Speed (OWS) organizations and organizations involved in vaccine storage and transport to review the IBM X-Force report Attackers Are Targeting the COVID-19 Vaccine Cold Chain for more information, including indicators of compromise. For tips on avoiding social engineering and phishing attacks, see CISA Insights: Enhance Email & Web Security.

Read the full article here.

CHINESE STEP UP ATTEMPTS TO INFLUENCE BIDEN TEAM - US OFFICIAL

BBC News | December 2, 2020

William Evanina, from the US Office of the Director of National Intelligence, said the Chinese were also focusing on people close to Mr Biden's team. Mr Evanina said it was an influence campaign "on steroids". Separately, a justice department official said more than 1,000 suspected Chinese agents had fled the US. In Wednesday's virtual discussion at the Aspen Institute think tank, Mr Evanina, chief of the Director of National Intelligence's counter-intelligence branch, said China had been attempting to meddle in the US efforts to develop a coronavirus vaccine and recent American elections. He continued: "We've also seen an uptick, which was planned and we predicted, that China would now re-vector their influence campaigns to the new [Biden] administration. "And when I say that, that malign foreign influence, that diplomatic influence plus, or on steroids, we're starting to see that play across the country to not only the folks starting in the new administration, but those who are around those folks in the new administration.

Read the full article here.

CHINA MOVES TO SURPASS US IN ECONOMICS, TECHNOLOGY, DIPLOMACY AND MILITARY, REPORT SAYS

Tom O'Connor | Newsweek | December 1, 2020

China is poised to overtake the United States in key economic and security areas, a development that could forever change the dynamic between the world's two premier powers, according to a report released Tuesday by a congressionally mandated commission. The United States-China Economic and Security Review Commission, founded two decades ago to mark the beginning of "The American Century," produces an annual report to Congress, detailing challenges to the bilateral ties between the two countries. The 2020 report, obtained early by Newsweek, took a definitive turn, even for an already historic year, calling on Congress to take action as the international playing field was redefined based on steps taken by Beijing and Washington.

Read the full article here.

STRATEGICALLY ASSESSING CONTRACTOR IMPLEMENTATION OF NIST SP 800-171

Defense Pricing and Contracting

Strategically Implementing Cybersecurity Contract Clauses, USD(A&S) Memorandum, dated February 5, 2019, directs development of a standard methodology to recognize industry cybersecurity readiness at a strategic level. Assessing Contractor Implementation of Cybersecurity Requirements, USD(A&S) Memorandum, dated November 14, 2019, provides standard DoD-wide methodology for assessing DoD contractor implementation of the security requirements in NIST SP 800-171. NIST SP 800-171 DoD Assessment Methodology rev 1.2.1, dated June 24, 2020, documents a standard methodology that enables a strategic assessment of a contractor's implementation of NIST SP 800-171, a requirement for compliance with DFARS clause 252.204-7012.

Read the full article here.

INDICTING RUSSIA'S MOST DESTRUCTIVE CYBERWAR UNIT: THE IMPLICATIONS OF PUBLIC ATTRIBUTION

Gil Baram | Council on Foreign Relations | November 23, 2020

On October 19, the U.S. Department of Justice unsealed charges accusing six Russian military intelligence officers of an aggressive worldwide hacking campaign. According to the indictment, the officers, who are believed to be members of Unit 74455 of the Russian Main Intelligence Directorate (GRU), were responsible for some of the most high profile cyberattacks of the last few years, including the devastating NotPetya worm in 2017 that cost $10 billion in damages, the targeting of the French presidential election in 2018, the hacking of the 2018 Winter Olympics in South Korea, interfering with electric grid in Ukraine in 2016, and others. Cybersecurity and national security experts [PDF] had long maintained that the attacks were Russia's doing, and along with investigative journalists, were expecting this to become public sooner or later.

Read the full article here.