ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

October 26, 2022

DOJ CHARGES ALLEGED CHINESE INTELLIGENCE OFFICERS WITH TRYING TO INTERFERE WITH HUAWEI PROSECUTION

Alison Durkee | Forbes | October 24, 2022

The Justice Department announced charges Monday against 13 people allegedly involved in attempts by the Chinese government to influence U.S. operations, including two Chinese nationals who were accused of trying to obstruct a government investigation into Chinese telecommunications giant Huawei. The DOJ charged Guochun He and Zheng Wang with attempting to obstruct a criminal prosecution into an unnamed global telecommunications company—which multiple outlets have identified as Huawei—and He with additional money laundering charges after he allegedly paid $61,000 in Bitcoin to a U.S. government employee. The defendants, who were allegedly intelligence officers working on behalf of the Chinese government, allegedly "orchestrated" a scheme starting in 2019 to steal information from the U.S. Attorney for the Eastern District of New York, which indicted Huawei and its subsidiaries for fraud and racketeering in 2019 and 2020. He and Wang allegedly paid an employee working for a U.S. law enforcement agency to steal information that would help them obstruct the FBI's investigation, but the U.S. employee was actually a double agent working with the FBI, thwarting their efforts.

Read the full article here.

CHINESE-LINKED HACKERS TARGETED U.S. STATE LEGISLATURE, RESEARCHERS SAY

AJ Vicens | CyberScoop | October 13, 2022

A long-running Chinese-linked cyberespionage group targeted a U.S. state legislature's network in July, marking the outfit's first confirmed attack against the U.S. in years, according to analysis published Thursday. The findings from the Symantec Threat Hunter Team point to a group the company refers to as Budworm. Other researchers call the group Bronze Union, APT27, Emissary Panda, Lucky Mouse and Temp.Hippo. The group has operated since at least 2013 and is known for targeting a wide range of industries "in support of its political and military intelligence-collection objectives." The outfit has attacked "a number of strategically significant targets" over the last six months, Symantec said, including the government of a Middle Eastern country, a multinational electronics manufacturer as well as the unnamed U.S. state legislature. Dick O'Brien, principal intelligence analyst for the Symantec Threat Hunter Team, declined to share additional details related to the attack, other than to say that it was an attack on its network, "which presumably both legislators and employees had access to."

Read the full article here.

WHAT NEXT FOR SCIENTIFIC COLLABORATION AS STAND-OFF BETWEEN CHINA AND THE WEST HEATS UP?

Maria Burke | Royal Society of Chemistry | October 18, 2022

Governments around the world – led by the US – are moving to restrict and control academic collaborations with China. What will this mean for research groups and universities on both sides? The latest in the clampdown on links with China is the closure of two major research centres involving Imperial College London and Chinese companies linked to the nation's defence industry after the UK government denied permission for work to continue. The move follows warnings from the FBI and MI5 in July that China was involved in economic espionage and presented 'the biggest long-term threat' to economic and national security. How times have changed. Back in 2012, Chinese investment in UK universities was encouraged and welcomed. Now, academic partnerships particularly those involving 'dual-use' technologies – which have civilian uses, but also potential military applications – have fallen from favour.

Read the full article here.

JUST A PROFESSOR OR A NATIONAL SECURITY THREAT FROM CHINA? THE CASE OF FRANKLIN TAO

Joe Jabara | ClearanceJobs | October 19, 2022

The subject of professors as a national security threat has continued to stay in the news. The prosecutions were part of the previous administrations China Initiative policy, in which failing to disclose a relationship with China on United States academic research paperwork. Make no mistake: these cases are different than someone specifically caught engaging in espionage, which are not nearly as common. The most recent court ruling involves Franklin Tao, a University of Kansas professor who specialized in renewable energy research. Tao was born in China, but he became a U.S. Citizen and a permanent resident. He has lived in the United States since 2002, as either a student or faculty. In 2020, Tao was charged with seven counts of wire fraud and three counts of false statements by the Department of Justice (eventually the charges at the beginning of trial were six counts of wire fraud and two counts of making false statements. The predominate basis of those charges, which has become common in similar professor cases, was a failure to disclose foreign activity, while applying for or participating in a National Science Foundation-funded research grant.

Read the full article here.

HOW CHINA'S SPYING OPERATIONS ARE FOOLING THE WORLD

Patricia R. Blanco | EL PAÍS | October 17, 2022

It is April 2001. Lin Di, secretary general of a key Chinese cultural exchange organization, is giving a talk to a select audience gathered at the National Press Club in Washington, one of America's premier conference centers. Chas Freeman, a diplomatic expert on the Asian giant, introduces him. But Lin, a well-known figure among the US elite at the time, needed no introduction: he had already met dozens of the officials, academics and diplomats who now greeted him warmly. "China is deepening its reforms to build a more open, prosperous, democratic and modernized nation," Lin said. He then expressed his "sincerest hope" that in the century that was just beginning, China and the US would work "together to build a healthy and stable relationship for the noble cause of world peace and the progress of human civilization." It was all a lie. Lin was, in fact, a spy; the "head of the Social Investigation Bureau of China's premier intelligence agency, the Ministry of State Security [MSS]," according to Alex Joske, author of Spies and Lies: How China's Greatest Covert Operations Fooled the World, and a senior analyst at the Australian Strategic Policy Institute.

Read the full article here.

REASONABLE MEASURES TO PROTECT TRADE SECRETS

R. Mark Halligan | Reuters | October 10, 2022

Protecting confidential business information dates back to Roman law which afforded relief against a person who induced another's servant to divulge secrets relating to the master's commercial affairs. The law of trade secrets evolved in England in the early 19th century and in the United States by the middle of the 19th century. One of the earliest issues in trade secret law was the degree of secrecy required to qualify as a trade secret. There were two common law doctrines: absolute secrecy and relative secrecy. The courts held that absolute secrecy was not required because absolute secrecy would prohibit the trade secret owner from exploiting the economic value of the trade secret with employees, agents, licensees, and others. In addition, absolute secrecy would encourage unproductive hoarding of useful information. The majority view became relative secrecy. Courts do not require extreme and unduly expensive procedures to be taken to protect trade secrets.

Read the full article here.

LOUISIANA'S HIGHER EDUCATION FOREIGN SECURITY ACT OF 2022 SIGNALS CONTINUED SCRUTINY OF FOREIGN INFLUENCE IN AMERICAN ACADEMIA

Mark Barnes, Laura G. Hoey, Brendan C. Hanifin, Samantha Barrett Badlam, Emerson Siegle, Kurt Fowler, and Francis Liesman | Ropes & Gray | October 18, 2022

On June 18, Louisiana Governor John Bel Edwards signed into law the Higher Education Foreign Security Act of 2022 (the "Act"), imposing new policy requirements on Louisiana postsecondary education institutions. The Act takes effect July 1, 2023, and requires covered institutions to establish policies governing foreign gift reporting, screening of foreign researchers, and international travel approval and monitoring. Although the Act is limited in scope to institutions of higher education in Louisiana, it shares some features with a gubernatorial executive order in Florida applicable to institutions there, and moreover, may presage similar actions by other state legislatures and governors. We could well have, over the next few years, a state-by-state patchwork of regulatory requirements applicable to researchers, students, and faculty from outside the U.S., as well as to scholarly activities and collaborations with researchers outside the U.S.

Read the full article here.

CHINESE COMMUNIST CELLS IN WESTERN FIRMS?

Dennis Kwok and Sam Goodman | The Wall Street Journal | July 11, 2022

The legal and regulatory risk of doing business in China may be about to get a lot higher. The China Securities Regulatory Commission is implementing changes to its rules governing publicly offered securities investment funds. These rules include requiring foreign-owned fund managers such as BlackRock and Fidelity to create Communist Party cells when operating in China. Many foreign investors have assumed these rules would apply only to Chinese businesses and state-owned enterprises. China analysts, however, have been warning since 2018 that these laws could soon apply to foreign-owned companies operating through Chinese joint ventures. Since 2016, Xi Jinping has pushed for state-run companies and subsidiaries of foreign-owned companies to establish cells through the provisions of the Chinese Communist Party's Articles of Association. In September 2020, the General Office of the Communist Party's Central Committee issued the "Opinion on Strengthening the United Front Work of the Private Economy in the New Era," which called on the nation's United Front Work Departments to strengthen their involvement in corporate governance.

Read the full article here.

CHINESE FIRMS EXPORTING SURVEILLANCE TOOLS ACROSS THE GLOBE, REPORT SAYS

Edward Graham | Nextgov | October 18, 2022

The Chinese government is using its investments in surveillance technologies to advance "both its ambitions of becoming a global technology leader as well as its means of domestic social control," according to a report released by the Atlantic Council on Monday. The report, authored by Bulelani Jili—a non-resident fellow at the Atlantic Council's Cyber Statecraft Initiative—noted that Beijing's domestic surveillance system "is confined to its national borders," but said that the Chinese companies that "make its surveillance state possible are now actively selling their tools abroad." These technologies—produced almost exclusively by companies funded by and tied to the Chinese government—enable Beijing to monitor its citizens through the collection of a vast array of personal data.

Read the full article here.

SECURITY FEARS AS THOUSANDS OF BRITISH ACADEMICS WORK WITH CHINESE MILITARY SCIENTISTS ON RESEARCH

Robert Mendick and Sophia Yan | The Telegraph | MSN | October 16, 2022

British academics have collaborated on thousands of research papers with Chinese military scientists according to a government-funded report that universities sought to suppress. The paper, a summary of which was published yesterday by the Henry Jackson Society, detailed publications in which British academics had partnered with those at 'very high risk' universities in China. It also detailed links to universities in Russia and Iran with military ties. The research by the foreign policy and national security think tank claims to have uncovered 13,415 collaborative partnerships. It is alleged that 11,611 of these were between British and Chinese academics. It comes as Xi Jinping, the Chinese president, on Sunday renewed his threat to invade Taiwan in a speech at the 20th Communist Party Congress in Beijing.

Read the full article here.

AMERICAN TECHNOLOGY BOOSTS CHINA'S HYPERSONIC MISSILE PROGRAM

Cate Cadell and Ellen Nakashima | The Washington Post | October 17, 2022

Military research groups at the leading edge of China's hypersonics and missile programs — many on a U.S. export blacklist — are purchasing a range of specialized American technology, including products developed by firms that have received millions of dollars in grants and contracts from the Pentagon, a Washington Post investigation has found. The advanced software products are acquired by these military organizations through private Chinese firms that sell them on despite U.S. export controls designed to prevent sales or resales to foreign entities deemed a threat to U.S. national security, the investigation shows. Scientists who work in the sprawling network of Chinese military research academies and the companies that aid them said in interviews that American technology — such as highly specialized aeronautical engineering software — fills critical gaps in domestic technology and is key to advances in Chinese weaponry.

Read the full article here.