ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

JULY 29, 2020

SINGAPOREAN NATIONAL PLEADS GUILTY TO ACTING IN THE UNITED STATES AS AN ILLEGAL AGENT OF CHINESE INTELLIGENCE

U.S. Department of Justice Federal Bureau of Investigation | July 24, 2020

Jun Wei Yeo, also known as Dickson Yeo, entered a plea of guilty today to one count of acting within the United States as an illegal agent of a foreign power without first notifying the Attorney General, in violation of 18 U.S.C. § 951. Yeo's plea was entered via videoconference before the Honorable Tanya S. Chutkan in the U.S. District Court for the District of Columbia. The announcement was made by John G. Demers, Assistant Attorney General; Michael R. Sherwin, Acting U.S. Attorney for the District of Columbia; Timothy R. Slater, Assistant Director in Charge of the Federal Bureau of Investigation's (FBI) Washington Field Office; and Alan E. Kohler, Jr., Assistant Director of the FBI's Counterintelligence Division.

Read the full article here.

FBI DEPUTY DIRECTOR DAVID BOWDICH'S REMARKS AT PRESS CONFERENCE ANNOUNCING CHARGES AGAINST CHINESE HACKERS

U.S. Department of Justice Federal Bureau of Investigation | July 21, 2020

FBI Deputy Director David Bowdich delivered the following remarks during a virtual press conference at the Department of Justice announcing charges against two Chinese hackers for their roles in a global computer intrusion campaign targeting intellectual property and confidential business information, including COVID-19 research. The indictment alleges that Li Xiaoyu and Dong Jiazh worked with the Guangdong State Security Department (GSSD) of the Ministry of State Security (MSS) while also targeting victims worldwide for personal profit. (Remarks prepared for delivery.)

Read the full remarks here.

‘A BASE FOR SPYING IN HOUSTON’: SEN. CRUZ SAYS MORE CHINESE CONSULATES MAY CLOSE IN WAKE OF ALLEGATIONS

Matt Dougherty | KHOU 11 | July 26, 2020

The United States consulate in Chengdu, China officially closed Sunday. China's decision to shut down the consulate was made in retaliation for last week's eviction of diplomats from the China Consulate General in Houston. Friday was the move-out day for the consul general and staff who are accused of participating in foreign espionage at the Houston location. The U.S. Department of State claimed the consulate in Houston was a hub for Chinese spies. Officials alleged the spies stole medical research from M.D. Anderson Cancer Center and the Texas A&M medical system. Chinese officials denied the claims. During a Sunday morning interview with CBS's Face the Nation, Sen. Ted Cruz said there may be more Chinese consulates closing in the future. "They may well be closed," Cruz said. "That consulate was closed, because that consulate, they used it as a base for spying in Houston and throughout the Southwest.”

Read the full article here.

VIRGINIANS ASKED NOT TO PLANT UNSOLICITED SEEDS MAILED FROM CHINA

Jose Umana | WTOP | July 25, 2020

Residents living in Virginia have been receiving unsolicited seeds that appear to have originated from China. State officials are now asking residents who receive packages with the unidentified seeds not to plant them in their gardens, urging caution as they could be from a non-native or invasive plant species. “Invasive species wreak havoc on the environment, displace or destroy native plants and insects and severely damage crops,” the Virginia Department of Agriculture and Consumer Services said in a news release. “Taking steps to prevent their introduction is the most effective method of reducing both the risk of invasive species infestations and the cost to control and mitigate those infestations.” Virginians said they received the seeds through mailed packages containing Chinese writing.

Read the full article here.

HARVARD PROFESSOR ACCUSED OF LYING ABOUT CHINA TIES FACES U.S. TAX CHARGES

U.S. News | July 28, 2020

U.S. prosecutors brought tax charges on Tuesday against a Harvard University professor accused of lying to authorities about his ties to a China-run recruitment program and funding he allegedly received from the Chinese government for research. Charles Lieber, the former chair of Harvard's chemistry and chemical biology department, was charged in an indictment filed in federal court in Boston with failing to report income he received from Wuhan University of Technology in China. The four tax-related counts are in addition to two counts of making false statements to federal authorities that Lieber, 61, pleaded not guilty to in June. Marc Mukasey, his lawyer, said in a statement that Lieber was innocent. "He didn't hide anything, and he didn't get paid as the government alleges," he said. Lieber's case is one of the highest-profile to emerge from a U.S. Justice Department crackdown on Chinese influence within universities amid concerns about spying and intellectual property theft by the Chinese government.

Read the full article here.

SINGAPOREAN NATIONAL PLEADS GUILTY TO ACTING IN THE UNITED HOW TO SAFEGUARD AMERICAN SCIENCE

M. Peter McPherson | Forbes | July 22, 2020

As scientists across the globe embarked on a race to develop vaccines and treatments for Covid-19, the FBI revealed hackers sponsored by the Chinese government were mounting a cyber assault to gain critical information from U.S.-led medical research trials. Yesterday, the Department of Justice charged two hackers for their work on behalf of the Chinese government. In conjunction with their U.S. and Canadian counterparts, British intelligence officials announced last Thursday that Russian hackers had also launched attacks seeking vaccine data. These malign efforts are stunning in their brazenness. But they're hardly surprising. China has stepped up efforts to exploit American intellectual property in recent years, joining other state actors such as Russia and Iran. To address the challenge, we need a multifaceted approach to safeguard our science and preserve our position as the world's most innovative economy. Universities must continue and enhance their safeguards to protect sensitive research, the intelligence community must share actionable information on risks to science, and the U.S. must redouble public investment in research to match our competitors' increased research investments. This can and must be achieved while advancing sensible immigration policies and the appropriate international scientific collaboration that has been a hallmark of a large share of U.S. research for decades.

Read the full article here.

POPULAR CHINESE-MADE DRONE IS FOUND TO HAVE SECURITY WEAKNESS

Paul Mozur, Julian E. Barnes, and Aaron Krolik | The New York Times | July 23, 2020

Cybersecurity researchers revealed on Thursday a newfound vulnerability in an app that controls the world's most popular consumer drones, threatening to intensify the growing tensions between China and the United States. In two reports, the researchers contended that an app on Google's Android operating system that powers drones made by China-based Da Jiang Innovations, or DJI, collects large amounts of personal information that could be exploited by the Beijing government. Hundreds of thousands of customers across the world use the app to pilot their rotor-powered, camera-mounted aircraft. The world's largest maker of commercial drones, DJI has found itself increasingly in the cross hairs of the United States government, as have other successful Chinese companies.

Read the full article here.

CHINESE MILITARY SPY HIDING IN SAN FRANCISCO CONSULATE PART OF BIGGER THREAT

Paul Crespo | American Defense News | July 23, 2020

As part of the FBI's ongoing crackdown on the overwhelming number of Chinese spies in the U.S., Tang Juan, a Chinese scientist at UC-Davis was identified as tied to Chinese military intelligence. She is accused of lying on her research visa by concealing her ties to the Chinese military, according to court filings reported by Time. After she was interviewed by the FBI she fled to the consulate where she is now hiding. Axios earlier reported that "Tang Juan came to the U.S. on a J-1 visa and was a researcher at the University of California, Davis." It further explained that on her visa application as part of her academic exchange program, Tang stated that she did not have any affiliation with the People's Liberation Army (PLA).

Read the full article here.

GOVERNMENT CLAMPS DOWN ON FOREIGN RESEARCH 'LEAKS'

Suvendrini Kakuchi | University World News | July 23, 2020

Against the backdrop of mounting tensions between Western nations and China, Japan is taking new steps to safeguard its own advanced research, including tightening the screening of foreign students and researchers to prevent leaks to foreign countries of advanced technologies, particularly those with possible military applications. Visas for foreign researchers will be more closely reviewed. The Japanese government has stated that financial aid will not be granted for university research if there are concerns or risks of technology outflow. Under proposed new rules, domestic researchers will be required to disclose foreign funding sources when applying for Japanese research subsidies. This was not required in the past.

Read the full article here.

IS TIKTOK SPYING ON YOU FOR CHINA?

Zak Doffman | Forbes | July 25, 2020

The relentless pressure on TikTok ramped up further this week, with U.S. Secretary of State Mike Pompeo again claiming user data is sent to China. "It's not possible to have your personal information flow across a Chinese server," he warned during a British media interview, suggesting that data would "end up in the hands of the Chinese Communist Party," which he characterized as an "evil empire." TikTok is firmly in the sights of the Trump administration, and they're not letting up. But now, as TikTok continues to deny U.S. accusations of data mishandling, of it bowing to pressure from Beijing, a new report from the cyber experts at ProtonMail has called those denials into question. "Beware," it warns, "the social media giant not only collects troves of personal data on you, but also cooperates with the CCP, extending China's surveillance and censorship reach beyond its borders."

Read the full article here.

ROMNEY CALLS FOR U.S. TO 'TAKE ACTION COLLECTIVELY' WITH OTHER NATIONS AGAINST CHINA

Henry Ren | Market Watch | July 22, 2020

Sen. Mitt Romney is calling for the U.S. to lead a coalition of countries that embrace fair trade to push China to stop its predatory pricing and theft of intellectual property. "There's no other nation that can provide the leadership that's necessary to develop a global approach to China's ambition, and to tell them that ambition cannot be realized in the way you're pursuing it," the Utah Republican said Tuesday during a Center for Strategic and International Studies webinar. "We have to be the nation that does that. We have not done that today." In January, President Donald Trump signed a "Phase 1" trade deal with China, imposing harsher punishments to deter Chinese firms from stealing intellectual property, a practice that Beijing has long denied. However, Romney said China continues to drive Western companies out of business by subsidizing technologies or selling products massively below costs while enjoying unfettered access to foreign markets.

Read the full article here.

LIE, CHEAT & STEAL: CHINA BUILDING 'WORLD-CLASS MILITARY' BY EXPLOITING OUR OPENNESS, SAYS US

Sidharth Shekhar | Times Now | July 22, 2020

The Chinese Communist Party (CCP) is planning to develop the People's Liberation Army (PLA) into a "world-class military" by 2049 and to achieve this it is acquiring the intellectual property, key research, and technological advances of the world's citizens, researchers, scholars, and private industry, said the United States. In order to advance the CCP's military aims, China under its Military-Civil Fusion strategy is acquiring and the world's cutting-edge technologies – including through theft – in order to achieve military dominance, said the US Department of State in its report. The report further says that the MCF is eliminating barriers between China's civilian research and commercial sectors, and it's military and defense industrial sectors.

Read the full article here.

AS FBI CRACKS DOWN ON CHINESE SPIES IN ACADEMIA, ONE RESEARCHER IS REPORTEDLY HIDING OUT AT CONSULATE IN SF

Jay Barmann | SFist | July 23, 2020

Earlier this week, the U.S. Department of Justice filed charges against a visiting Chinese researcher at Stanford who allegedly lied on her visa application to conceal her active status in the Chinese military. And as part of the court filing supporting the need to detain her, the FBI detailed a separate case in which another supposed researcher with ties to the People's Liberation Army who had been at UC Davis has disappeared, likely into the Chinese consulate in San Francisco, where they say she is being harbored. The case of Chen Song was reported earlier this week by the SF Chronicle and others, after visa fraud charges were filed against her. Chen, 38, is a neurologist who entered the U.S. on a work-study visa in December 2018, and had been working at Stanford on research into a brain disease known as myasthenia gravis. Investigators have no identified her through photographs and other evidence as an active member of the Chinese military who had been studying the disease at a Chinese Air Force hospital prior to coming to the U.S. — and she allegedly lied to U.S. Customs and Border Control on her visa application, stating she had only been active in the military until 2011 and her current employer was a civilian hospital.

Read the full article here.

HOW A CHINESE AGENT USED LINKEDIN TO HUNT FOR TARGETS

Kevin Ponniah | BBC News | July 26, 2020

His doctorate research was about Chinese foreign policy and he was about to discover firsthand how the rising superpower seeks to attain influence. After his presentation, Jun Wei, also known as Dickson, was, according to US court documents, approached by several people who said they worked for Chinese think tanks. They said they wanted to pay him to provide "political reports and information". They would later specify exactly what they wanted: "scuttlebutt" - rumours and insider knowledge. He soon realised they were Chinese intelligence agents but remained in contact with them, a sworn statement says. He was first asked to focus on countries in South East Asia but later, their interest turned to the US government. That was how Dickson Yeo set off on a path to becoming a Chinese agent - one who would end up using the professional networking website LinkedIn, a fake consulting company and cover as a curious academic to lure in American targets.

Read the full article here.

UNIVERSITY 'NAIVE' TO PARTNER WITH CHINESE INSTITUTE, SECURITY EXPERT SAYS

Eleisha Foon | RNZ | July 27, 2020

In April 2018, the University of Canterbury signed an agreement with Harbin Institute of Technology to collaborate on teaching and research. China has been accused of stealing sensitive technologies and intellectual property through academic exchanges and some experts warn the university could be putting the country's national security at risk for jumping into a partnership before doing its homework. Experts have called the University of Canterbury "naive" to enter into an agreement in April 2018 with Harbin Institute of Technology (HIT), which is widely known to have links to the Chinese military. UC's Deputy Vice-Chancellor Professor Ian Wright said no inquiries about HIT's defence links were made at the time, but said New Zealand's university sector had been increasingly aware of the sensitivity of some specific areas of research and technology.

Read the full article here.

INDIA BANS 47 CHINESE APPS; OVER 250 MORE UNDER SCANNER FOR USER PRIVACY VIOLATION

Rahul Shrivastava and Kamaljit Kaur Sandhu | India Today | July 27, 2020

India has banned 47 apps of Chinese origin in the country, nearly a month after banning 59 Chinese applications. Sources have told India Today TV that the 47 banned Chinese apps were operating as clones of the earlier banned apps. The list of the 47 Chinese applications banned by the Ministry of Electronics and Information Technology will be released soon. The Ministry of Electronics and Information Technology has banned 47 apps which were variants and cloned copies of the 59 Chinese apps that were banned in June. These 47 banned app clones include Tiktok Lite, Helo Lite, SHAREit Lite, BIGO LIVE Lite, and VFY Lite, news agency ANI reported. India has also prepared a list of over 250 Chinese apps, including apps linked to Alibaba, that it will examine for any user privacy or national security violations, government sources told India Today TV. The list also includes Tencent-backed gaming app PUBG. Some top gaming Chinese applications are also expected to be banned in the new list that is being drawn up, sources said. The Chinese applications, that are being reviewed, have allegedly been sharing data with the Chinese agencies.

Read the full article here.

SAFEGUARDING OUR FUTURE

The National Counterintelligence and Security Center Office of the Director of National Intelligence | July 23, 2020

These unclassified, one-page "Safeguarding Our Future " bulletins provide a brief overview of a specific foreign intelligence threat, as well as impacts of that threat and steps for mitigation.

Read the full article here.

EXCLUSIVE: HARVARD CENTER HYPES CHINESE COMMUNIST PARTY POPULARITY WHILE RECEIVING MILLIONS FROM CHINESE GOVT AND CCP-LINKED COMPANIES

Natalie Winters | The National Pulse | July 23, 2020

The July 2020 report "Understanding CCP Resilience: Surveying Chinese Public Opinion Through Time" contends that the Chinese Communist Party (CCP) is "as strong as ever" and "under no imminent threat of popular upheaval." "Chinese citizen satisfaction with government has increased virtually across the board," the Harvard Kennedy School Ash Center for Democratic Governance and Innovation paper continues. But the 18-page report omits references to events countering this narrative: ongoing Hong Kong protests, oppression of Uyghurs in Xinjiang, or even the party's mishandling of coronavirus.

Read the full article here.

THE HEAD OF U.S. COUNTERINTELLIGENCE HOISTS THE RED FLAG

Lynn Mattice | Security Info Watch | March 9, 2020

During the Opening Session at the November 2019 Executive Summit Series forum in Washington D.C., one of the government officials I interviewed was William Evanina, Director of the National Counterintelligence and Security Center. The focus of the interview was on the threat landscape facing companies operating around the world. No one was surprised that a significant portion of the time was spent on the threat posed by China. A portion of the interview focused on the aggressive nature China has taken in its stated goal in its Made in China 2025 doctrine of global domination in virtually every category of products and services. It also touched upon the other stated goal of the Made in China 2025 doctrine of supplying domestic markets predominately from local Chinese suppliers.

Read the full article here.

WARNING—APPLE SUDDENLY CATCHES TIKTOK SECRETLY SPYING ON MILLIONS OF IPHONE USERS

Zak Doffman | Forbes | June 26, 2020

As I reported on June 23, Apple has fixed a serious problem in iOS 14, due in the fall, where apps can secretly access the clipboard on users' devices. Once the new OS is released, users will be warned whenever an app reads the last thing copied to the clipboard. As I warned earlier this year, this is more than a theoretical risk for users, with countless apps already caught abusing their privacy in this way. Worryingly, one of the apps caught snooping by security researchers Talal Haj Bakry and Tommy Mysk was China's TikTok. Given other security concerns raised about the app, as well as broader worries given its Chinese origins, this became a headline issue. At the time, TikTok owner Bytedance told me the problem related to the use of an outdated Google advertising SDK that was being replaced.

Read the full article here.

WORKING FROM HOME ON YOUR OWN PC? SECURITY IS STILL A CONFUSING MESS FOR MANY

Steve Ranger | ZD Net | June 23, 2020

Many companies have spent the last couple of months scrambling to deploy new systems to manage the security risks surrounding remote working. And with working from home likely to become much more prevalent, it seems there's still plenty more work to do. For most staff, remote working has been a new experience: more than 80% of respondents said they either rarely worked from home or not at all prior to the pandemic, according to research by IBM.

Read the full article here.

JUST IN: PENTAGON EXPECTS 7,500 COMPANIES CMMC CERTIFIED BY 2021

Mandy Mayfield | National Defense | July 23, 2020

The Defense Department anticipates that by next year 7,500 companies in its industrial base will hold certifications that they meet new cybersecurity requirements, a senior official said July 22. The Cybersecurity Maturity Model Certification version 1.0 requirements are part of the Pentagon's push to protect industrial base networks and controlled unclassified information from cyber attacks. The CMMC rules will require contractors to be certified by third-party auditors, which will ensure that contractors are adhering to certain standards. Organizations will be required to meet different levels of security requirements depending on the type of work they are doing, with level 1 being the least burdensome and level 5 the most stringent. An "estimated 7,500 companies will be certified in 2021," Katie Arrington, chief information security officer in the office of the undersecretary of defense for acquisition and sustainment, said during a webinar hosted by cybersecurity company Celeruim "That doesn't seem like a lot but if you think about the interconnectivity of the [defense industrial base] it's a certification that's good for all DoD contracts for three years." By 2026, all solicitations are expected to include CMMC standards that companies must meet if they want to do business with the Pentagon.

Read the full article here.

U.S. ORDERS CHINA TO CLOSE HOUSTON CONSULATE

Kate O'Keeffe, Aruna Viswanatha, and Chun Han Wong | The Wall Street Journal | July 22, 2020

The U.S. ordered China to shut its consulate in Houston, with officials accusing it and other Chinese diplomatic missions of economic espionage and visa fraud, an unprecedented escalation in a rapidly deteriorating relationship. U.S. officials said Wednesday that the Houston consulate has been a focus of rising concern and has until 4 p.m. Friday to close. Assistant Secretary of State David Stilwell in an interview called the order to close the Houston consulate "long overdue" and said it followed a series of malign activities.

Read the full article here.

PROSECUTORS SAY S.F. CONSULATE IS HARBORING CHINESE MILITARY RESEARCHER WANTED BY FB

Bethany Allen-Ebrahimian | Axios | July 22, 2020

A researcher who lied about her affiliation with a Chinese military university entered the Chinese consulate in San Francisco after being interviewed by the FBI on June 20 about alleged visa fraud and has remained there, according to an FBI assessment in court filings dated July 20. Why it matters: Using a diplomatic facility to shelter someone charged with a federal crime could cause serious tension between the U.S. and China, especially as the U.S. is seeking to crack down on Chinese espionage and research theft. "It is highly unusual for a Chinese diplomatic post to associate so closely with a suspect in an intellectual property theft-related case," said Minyao Wang, a New York-based lawyer who has worked on IP theft cases related to China.

Read the full article here.

CHINESE CONSULATE IN HOUSTON CLOSED FOLLOWING US ORDER

Nicole Gaouette and Jennifer Hansler | CNN | July 25, 2020

The Chinese Consulate General in Houston has closed following Tuesday's order to do so after US officials alleged it was part of a larger Chinese espionage effort using diplomatic facilities around the US, a State Department spokesperson confirmed to CNN late Friday. US federal agents and local law enforcement entered the Chinese consulate compound in Houston earlier Friday in a series of black SUVs, trucks, two white vans and a locksmith's van as a crowd of observers and news cameras observed from the edge of the diplomatic compound. US officials speaking to reporters Friday said the consulate had been implicated in a fraud investigation at a Texas research institution and that Chinese consulate officials "were directly involved in communications with researchers and guided them on what information to collect."

Read the full article here.

PROTECTING YOUR BUSINESS FROM CYBERSECURITY THREATS DURING COVID-19

Mike Kelleher | Industry Week | July 13, 2020

COVID-19 has changed how manufacturers work. Many employees began to work remotely when the pandemic hit the United States in earnest — and many continue to do so, even after businesses in some states have tried to reopen their facilities with modified working conditions. While this forced move toward a distributed workforce has prompted many changes in how businesses operate, one that should be of particular concern is the way corporate data is now being trafficked across home networks, which businesses don't control and manage — and which don't necessarily conform to company cybersecurity standards. This inevitable outcome of working from home means that all manufacturers need to revisit and heighten their cybersecurity protocols to account for remote working conditions. Not doing so could leave them vulnerable to forms of cyberattack that are already emerging in response to the changing landscape of how we work.

Read the full article here.

CHINA'S COUNTERINTELLIGENCE "TRINITY" AND FOREIGN BUSINESS

Matthew Brazil | The Jamestown Foundation | March 26, 2018

As the Chinese Communist Party (CCP) pursues a domestic anti-spy campaign and new espionage laws, PRC national security concerns and greater suspicion of foreigners may trump foreign business complaints about unfavorable treatment, rising trade barriers, and feeling unwelcomed. Foreign firms in China should not ignore these warning signs, but instead plan for a period of higher business risk and harsher conditions, especially since strong historical parallels indicate that this period may not pass quickly.

Read the full article here.

THINK BEFORE YOU LINK

Centre for the Protection of National Infrastructure

Criminals and hostile actors may act anonymously or dishonestly online in an attempt to connect with people who have access to valuable and sensitive information. They often do this by posing as recruiters or talent agents who will approach individuals with enticing opportunities, when their real intent is to gather as much information as possible from the target. The consequences of engaging with these profiles can damage individual careers, as well as the interests of your organisation, and the interests of UK national security and prosperity. This guidance provides practical advice on how to identify them, how to respond, and how to minimise the risk of being targeted in the first instance.

Read the full article here.

THINKING THE UNTHINKABLE: ARE AMERICAN ORGANIZATIONS IN CHINA READY FOR A SERIOUS CRISIS?

Matthew Brazil | The Jamestown Foundation | May 11, 2017

Since the 2016 General Election, American relations with the People's Republic of China (PRC) have followed a rollercoaster-like trajectory. Days before his inauguration, President Trump briefly reversed decades of predictable American conduct in a telephone conversation with Taiwan President Tsai Ing-wen and hinted a departure from the "one China policy," (CNA.com.tw, December 3, 2016; Reuters, January 12). During his confirmation hearings, Secretary of State Rex Tillerson proposed blocking access to China's artificial islands in the South China Sea and triggered an outraged response from Beijing (C-SPAN, January 11, Global Times, January 13). Then came the public reversals. With little explanation, Trump endorsed "One China" during his call with Chinese President Xi Jinping in early February (Xinhuanet, February 10).

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