ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

JULY 8, 2020

THE THREAT POSED BY THE CHINESE GOVERNMENT AND THE CHINESE COMMUNIST PARTY TO THE ECONOMIC AND NATIONAL SECURITY OF THE UNITED STATES

Remarks by Director Christopher Wray | Federal Bureau of Investigation | July 7, 2020

Good morning. I realize it's challenging, particularly under the current circumstances, to put on an event like this, so I'm grateful to the Hudson Institute for hosting us today. The greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China. It's a threat to our economic security—and by extension, to our national security. As National Security Advisor O'Brien said in his recent remarks, we cannot close our eyes and ears to what China is doing—and today, in light of the importance of this threat, I will provide more detail on the Chinese threat than the FBI has ever presented in an open forum. This threat is so significant that the attorney general and secretary of state will also be addressing a lot of these issues in the next few weeks. But if you think these issues are just an intelligence issue, or a government problem, or a nuisance largely just for big corporations who can take care of themselves—you could not be more wrong.

Read the full remarks here.

NDAA COULD REQUIRE CLOSER TRACKING OF DOD RESEARCHERS

Lauren C. Williams | FCW | July 6, 2020

House lawmakers last week passed an amendment to the 2021 National Defense Authorization Act that would allow the Defense Department to track U.S. and foreign student researchers on national security projects, despite privacy concerns. The amendment aims to close a loophole in the 2020 NDAA that excluded basic DOD research at academic institutions from information-sharing requirements. "We have seen numerous incidents from both Americans and foreign nationals involved in the theft of intellectual property, espionage and illicit technology transfer," Rep. Jim Banks (R-Ind.) said of his amendment, adding that the measure was about transparency so taxpayers can understand where DOD funds were going and who was participating in the research.

Read the full article here.

HOW THE U.S. DOJ'S 'CHINA INITIATIVE' IMPACTS CHINESE-AMERICAN SCIENTISTS AND RESEARCHERS

Catherine X. Pan-Giordano | SupChina | July 1, 2020

What is the China Initiative, and why is it important for Chinese and Chinese American businesses and researchers to know? In this sponsored post, SupChina COO Bob Guterma interviewed Pan-Giordano to find out. Bob Guterma: Let's begin with a general policy discussion. What is the Department of Justice's (DOJ) "China Initiative? Pan-Giordano: On November 1, 2018, the Department of Justice launched its "China Initiative" to confront China's national security threats and to protect U.S. technology. Under the China Initiative, the DOJ has been prioritizing U.S. government enforcement actions against Chinese companies and persons doing business in the U.S. or partnering with U.S. companies and universities. The DOJ has also been focusing on individual researchers and scientists with ties to China.

Read the full article here.

AN UNFAIR ADVANTAGE: CONFRONTING ORGANIZED INTELLECTUAL PROPERTY THEFT

Megan Gates | ASIS International | July 1, 2020

Hongjin Tan had a good job. A Chinese national and U.S. legal permanent resident, he was employed as an associate scientist for a U.S. petroleum company to work with a team developing the next generation of battery technologies for stationary energy storage. But after just over two years at the company, Tan contacted his supervisor on 12 December 2018 to give his two weeks' notice. Tan said he wanted to return to China because, as an only child, he needed to be there to care for his aging parents. He did not have a job lined up back home but was in negotiations with a few battery companies about a position.

Read the full article here.

INTERNATIONAL STUDENTS MAY NEED TO LEAVE US IF THEIR UNIVERSITIES TRANSITION TO ONLINE-ONLY LEARNING

Priscilla Alvarez and Catherine E. Shoichet | CNN | July 7, 2020

International students who are pursuing degrees in the United States will have to leave the country or risk deportation if their universities switch to online-only courses, Immigration and Customs Enforcement announced Monday. The move may affect thousands of foreign students who come to the United States to attend universities or participate in training programs, as well as non-academic or vocational studies. Universities nationwide are beginning to make the decision to transition to online courses as a result of the coronavirus pandemic. At Harvard, for example, all course instruction will be delivered online, including for students living on campus. For international students, that opens the door to them having to leave the US.

Read the full article here.

CHINA USES ANDROID MALWARE TO SPY ON ETHNIC MINORITIES WORLDWIDE, NEW RESEARCH SAYS

Simon Chandler | Forbes | July 6, 2020

China-based surveillance campaigns are using Android malware to spy on Uighur Muslims and other ethnic minorities worldwide, according to new research from mobile cybersecurity firm Lookout. The San Francisco-based Lookout discovered that Chinese hacker groups are using four surveillance-ware tools to harvest personal data from Android smartphones. Named SilkBean, DoubleAgent, CarbonSteal and GoldenEagle, these related pieces of malware are previously undocumented. They're part of larger mAPT (mobile advanced persistent threat) campaigns originating in China and stretching back as far as 2013. While they primarily target the Uighur Muslim ethnic minority, Lookout also found evidence that the campaigns target Tibetans and Muslims outside of China.

Read the full article here.

VIRTUAL TELEWORK PLATFORMS – PROTECT YOUR COMPANY INFORMATION

The National Counterintelligence and Security Center Office of the Director of National Intelligence | July 6, 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 bulletin here.

ENHANCED SECURITY REQUIREMENTS FOR PROTECTING CONTROLLED UNCLASSIFIED INFORMATION: A SUPPLEMENT TO NIST SPECIAL PUBLICATION 800-171 (FINAL PUBLIC DRAFT)

National Institute of Standards and Technology | July 1, 2020

Draft NIST Special Publication (SP) 800-172 (formerly Draft NIST SP 800-171B) provides an enhanced security requirements to help protect the confidentiality, integrity, and availability of Controlled Unclassified Information (CUI) associated with critical programs or high value assets in nonfederal systems and organizations from the advanced persistent threat (APT). The APT is an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using both cyber and physical attack vectors. The objectives include establishing and extending footholds within the infrastructure of the targeted organizations for the purposes of exfiltrating information; undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The APT pursues its objectives repeatedly over an extended period, adapts to defenders' efforts to resist it, and is determined to maintain the level of interaction needed to execute its objectives.

Read the full announcement here.

THE DOD WANTS BETTER CYBERSECURITY FOR ITS CONTRACTORS. THE FIRST STEPS HAVEN'T BEEN EASY.

Jackson Barnett | Fed Scoop | July 1, 2020

One of the biggest, most complicated projects in the defense industrial base isn't a new weapons system or cloud computing environment. It's the Cybersecurity Maturity Model Certification (CMMC), which is set to upend how the Department of Defense does business with 300,000 contractors who provide everything from advanced aircraft to the shoelaces in soldiers' boots. The program is the Pentagon's latest response to years of neglect that left the door open to hackers to steal critical defense information, and the second half of 2020 will be a crucial stretch for the new, 15-person volunteer board at the heart of the CMMC process.

Read the full article here.

TRENDS IN U.S. MULTINATIONAL ENTERPRISE ACTIVITY IN CHINA, 2000–2017

U.S. – China Economic and Security Review Commission | July 1, 2020

The report analyzes nearly two decades of data compiled by the Bureau of Economic Analysis to profile U.S. commercial activity in China. It finds that the vast expansion of U.S. multinational enterprise (MNE) activity in China may challenge U.S. industrial competitiveness and long-term tech leadership. Since 2000, U.S. companies' operations in China have been among the fastest growing globally for all foreign subsidiaries, with total U.S. commercial assets in China surging 15-fold. The rapid evolution of U.S. business operations in China away from manufacturing and toward higher value-added activity such as research and development, often coerced by Beijing, increases the risk that U.S. firms are unwittingly enabling China to achieve its industrial policy objectives.

Read the full report here.

CAN CHINA BE STOPPED FROM STEALING TECHNOLOGY FROM U.S. COLLEGES?

Kris Osborn | The National Interest | July 2, 2020

Congress is cracking down on Chinese espionage taking place throughout the U.S. scientific community by requiring researchers to disclose foreign funding sources in federal grant applications. The U.S. House Armed Services Committee has passed two of Representative Michael Waltz's (R-Florida) amendments to the 2021 National Defense Authorization Act to protect federally-funded research from Chinese espionage. "The United States faces the greatest adversary we have ever known in China," Waltz said in a written statement. "For years, the Chinese Communist Party has infiltrated our colleges and universities, using them to steal sensitive scientific research and information. America can no longer be a safe harbor for blatant espionage and intellectual property theft—and I'm glad this is a bipartisan concern across the Armed Services Committee."

Read the full article here.

CHINA'S CONFUCIUS INSTITUTES REBRAND AFTER OVERSEAS PROPAGANDA ROWS

Zhuang Pinghui | South China Morning Post via Yahoo News | July 4, 2020

Beijing is abandoning its Confucius Institute brand after a global backlash over censorship, switching to a new look as a centre for "language exchange and cooperation". In a directive to lower-level agencies, the Ministry of Education said the Confucius Institute Headquarters, or Hanban, had changed its name to the Ministry of Education Centre for Language Education and Cooperation. The directive, which was circulating on social media on Saturday, was confirmed by a source in the education sector who was briefed about the change. There was no response to phone calls to the institute's headquarters or its Asian offices.

Read the full article here.

RED FLAGS RAISED OVER CHINESE RESEARCH PUBLISHED IN GLOBAL JOURNALS

Eva Xiao | The Wall Street Journal | July 5, 2020

Internationally peer-reviewed journals published more than 100 scientific research papers from China-based authors that appear to have reused identical sets of images, raising questions about the proliferation of problematic science as institutions fast-track research during the coronavirus pandemic. The cache of 121 papers, credited to researchers from hospitals and medical universities across roughly 50 cities in China, all shared at least one image with another—a sign that many were likely produced by the same company or "paper mill," said Elisabeth Bik, a California-based microbiologist and image-analysis expert who identified the trove.

Read the full article here.

GUY WHO REVERSE-ENGINEERED TIKTOK REVEALS THE SCARY THINGS HE LEARNED, ADVISES PEOPLE TO STAY AWAY FROM IT

Rokas Laurinavivius and Ilona Baliunaite | Bored Panda | July 4, 2020

Facebook got itself into a sensitive data scandal when it did shady business with Cambridge Analytica, Instagram confirmed a security issue exposing user accounts and phone numbers, but these apps are basically online security havens compared to TikTok, according to one senior software engineer with about 15 years of professional experience. 2 months ago, Reddit user bangorlol made a comment in a discussion about TikTok. Bangorlol claimed to have successfully reverse-engineered it and shared what he learned about the Chinese video-sharing social networking service. Basically, he strongly recommended that people never use the app again, warning about its intrusive user tracking and other issues. Considering that TikTok was the 4th most popular free iPhone app download in 2019, this is quite alarming.

Read the full article here.

RUSSIAN HACKER GROUP EVIL CORP TARGETS US WORKERS AT HOME

Alejandro Serrano | BBC News | June 26, 2020

Evil Corp hackers have tried to access at least 31 organisations' networks in order to cripple systems and demand millions of dollars in ransom. The group's two alleged leaders were indicted by the US Justice Department in December 2019. There are concerns that US voting systems could also be targeted. Last year, US authorities filed charges against Evil Corp's alleged leaders Maksim Yakubets and Igor Turashev, accusing them of using malware to steal millions of dollars from groups including schools and religious organisations in over 40 countries.

Read the full article here.

FBI INVESTIGATING CYBERATTACK THAT LED UCSF TO PAY $1.14 MILLION IN RANSOM

Alejandro Serrano | San Francisco Chronicle | June 30, 2020

The FBI is investigating a cyberattack that led UCSF to pay approximately $1.14 million in ransom so the hackers would unlock data illegally obtained from the school, officials said Tuesday. The university's IT staff detected the incident June 1 as it was taking place "in a limited part of the UCSF School of Medicine's IT environment," school officials said in a statement. Staffers were able to isolate the incident from the core UCSF network. School officials said they don't believe patient medical records were exposed, and the school's patient care delivery operations, as well as the overall campus network and efforts related to the coronavirus outbreak, were not affected.

Read the full article here.

EUROPEAN DEFENSE COMPANIES THE TARGET OF CYBER ESPIONAGE OVER LINKEDIN

Byron Muhlberg | CPO Magazine | July 3, 2020

By posing as recruiters on LinkedIn, a new tactic has emerged by which advanced persistent threat (APT) hackers have been able to commit cyber espionage. This was evidenced by the findings of a recent report, which found that cybercriminals—believed to be affiliated with the North Korean government—posed as recruiters working at the U.S. defense groups Collins Aerospace and General Dynamics in order to break into the networks of European defense companies. According to Slovakia-based cybersecurity firm ESET, the cyber espionage attempts took place between September and December of last year, and were uncovered after a collaborative investigation with two of the affected defense companies in Europe.

Read the full article here.

UNIVERSITY OF TENNESSEE PROFESSOR ACCUSED OF HIDING HIS CHINESE JOB WANTS CASE TOSSED

Travis Dorman | Knox News | July 2, 2020

Under a directive to catch Chinese spies, federal authorities monitored Anming Hu for more than a year, found no evidence of espionage and manufactured a case against the University of Tennessee researcher anyway, his attorney says. "The (U.S. Department of Justice) wanted a feather in its cap with an economic espionage case, so they ignored the facts and the law, destroyed the career of a professor with three PhDs in nanotechnology and now expects the court to follow their narrative," attorney Philip Lomonaco wrote in a brief asking a judge to dismiss the charges against Hu.

Read the full article here.

SENATOR WARNS COLLEAGUES OF RISKS POSED BY CYBERATTACK ON U.S.

Dennis Hoey | Security Info Watch | July 1, 2020

Sen. Angus King of Maine took to the floor of the Senate on Tuesday to urge his colleagues to develop a national cyber-defense program that could fend off a potential "catastrophic cyberattack" that could disrupt millions of lives and throw the country into chaos. King urged his colleagues to consider the inclusion of vital cybersecurity amendments in the 2021 National Defense Authorization Act.

Read the full article here.

NATIONAL SECURITY AGENCY WARNS THAT VPNS COULD BE VULNERABLE TO CYBERATTACKS

Olivia Gazis | CBS News | July 2, 2020

The National Security Agency issued a new cybersecurity advisory on Thursday, warning that virtual private networks, or VPNs, could be vulnerable to attacks if not properly secured. The agency's warning comes amid a surge in telework as organizations adapt to coronavirus-related office closures and other constraints. A VPN allows users to establish private, encrypted connections to another network over the internet. They are used widely by corporations and other organizations to protect proprietary data from hackers while employees work remotely.

Read the full article here.