ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE

MEDIA SUMMARY

March 3, 2021

CHINA HAS ALREADY INFILTRATED AMERICA'S INSTITUTIONS

Mike Rogers | The Hill | March 2, 2021

Most Americans probably don't realize that one of the greatest threats to our national and economic security has already infiltrated nearly every aspect of our society — the influence of the Chinese Communist Party (CCP). Backed by considerable financial largesse and run through harmless-sounding front organizations, the CCP is aggressively limiting free speech on American college campuses, co-opting and corrupting American politicians and businesses, stealing invaluable American research and development, and undermining the very foundations of our democratic republic. Ensuring prosperity and sovereignty in the next century demands that we recognize and confront the CCP's propaganda, influence and subversion wherever it is found, and it is found nearly everywhere one looks. This is not mere hyperbole or speculation; it is very real, and it is happening right now. In 2020, FBI Director Christopher Wray warned, "We've now reached the point where the FBI is opening a new China-related counterintelligence case about every 10 hours." Think about that — a new case every 10 hours. That's nearly 17 a week, 17 complex counterintelligence cases resulting from China's activities in the United States.

Read the full article here.

TAIWAN FINES RESEARCHER FOR ALLEGEDLY MANAGING PROJECTS ON CHINESE MAINLAND

Andrew Silver | Nature | March 2, 2021

Taiwan's education ministry has fined prominent chemical engineer Lee Duu-Jong for allegedly managing research projects funded by the Chinese mainland without approval from the island's authorities. But Lee says he was not involved in the projects and was listed as the person in charge without his knowledge. The fine, which China's central government has criticized as politically motivated, could affect how other researchers approach collaborations between Taiwan and the Chinese mainland. Lee is considering appealing against the fine of 300,000 Taiwan dollars (US$11,000). A researcher who was involved in the projects backs up Lee's account. Scientists in Taiwan frequently collaborate with colleagues on the Chinese mainland — but participating in major mainland research programmes without permission is against the island's laws. In 2018, Taiwan's science and education ministries sent out letters reminding researchers about the rule — a move understood to reflect growing concerns that the island might be losing talent and intellectual property to the mainland.

Read the full article here.

MICROSOFT SAYS CHINESE HACKERS HAVE EXPLOITED BUG TO TARGET U.S. COMPANIES

Market Watch | March 2, 2021

China-based government hackers have exploited a bug in Microsoft's email server software to target U.S. organizations, the company said Tuesday. Microsoft MSFT said that a "highly skilled and sophisticated" state-sponsored group operating from China has been trying to steal information from a number of American targets, including universities, defense contractors, law firms and infectious-disease researchers. Microsoft said it has released security upgrades to fix the vulnerabilities to its Exchange Server software, which is used for work email and calendar services, mostly for larger organizations that have their own in-person email servers. It doesn't affect personal email accounts or Microsoft's cloud-based services. The company said the hacking group it calls Hafnium was able to trick Exchange servers into allowing it to gain access. The hackers then masqueraded as someone who should have access and created a way to control the server remotely so that they could steal data from an organization's network.

Read the full article here.

U.S. DOUBLES DOWN ON PROTECTING UNIVERSITY RESEARCH FROM CHINA

Jane Lanhee Lee and Daphne Psaledakis | Reuters | February 28, 2021

A U.S. national security commission is recommending that American universities take steps to prevent sensitive technology from being stolen by the Chinese military, a sign of growing concerns over the security of academic research. The National Security Commission on Artificial Intelligence (NSCAI), led by former Google chairman Eric Schmidt, is set to vote Monday on its final report to Congress. A new section on university research was added to a recently published final draft, which also features numerous recommendations in areas including competition in artificial intelligence and the semiconductor supply chain. The fresh recommendations come as the United States pushes ahead with the prosecution of at least five Chinese researchers arrested last year in various cities across the U.S. on charges of visa fraud for not disclosing ties to the Chinese military. Among those arrested was Chen Song, a former Stanford University visiting scholar in neurology who faces charges including obstruction of justice, destruction of records, and making false statements to a government agency. She pleaded not guilty at an arraignment last week in the United States District Court Northern District of California.

Read the full article here.

DESANTIS & FLORIDA LAWMAKERS TAKE AIM AT CHINA

Jake Stofan | News 4 Jax | March 1, 2021

Gov. Ron DeSantis and state lawmakers are adding China to the growing list of targets for the 2021 Florida legislative session, which gets underway on Tuesday. Newly filed bills include measures that aim to limit intellectual property theft by the communist regime and crack down on Chinese influence at American colleges and universities. "The growing presence of the Chinese communist party influence in domestic and international affairs is one of the most pervasive threats to American security and prosperity," DeSantis said during a Monday news conference. The governor and House Speaker Chris Sprowls are backing two proposals. The first seeks to curb Chinese influence in the academic field by requiring transparency for donations from foreign governments over $50,000 and punishing institutions that don't comply. "Florida is known for our sunshine and transparency," Sprowls said. "No longer will foreign interests be able to hide payments through subsidiaries and front companies."

Read the full article here.

U.S. ENLISTS ALLIES TO COUNTER CHINA'S TECHNOLOGY PUSH

Bob Davis | The Wall Street Journal | February 28, 2021

President Biden portrays U.S. relations with China as a clash of values: democracy vs. autocracy. But his rhetoric obscures the administration's more pragmatic approach of cobbling together groups of countries to work jointly on technology. The goal is to stay ahead of China in semiconductors, artificial intelligence and other advances that are expected to define the economy and military of the future. Preliminary conversations with U.S. allies have begun, though the effort is expected to take months, said senior administration officials. The strategy has both offensive and defensive components. By combining efforts, the U.S. and its allies can vastly outspend China, whose research-and-development budget now nearly matches the U.S. The alliances can also coordinate policies to deny China the technologies it needs to try to become a global leader.

Read the full article here.

THE BIDEN ADMINISTRATION WITHDREW A TRUMP-ERA ORDER TO TRACK CHINA'S INFLUENCE ON U.S. UNIVERSITIES. HERE'S WHY IT MATTERS.

Isa Ryan | Falkirk Center for Faith and Liberty | February 25, 2021

The Biden administration has quietly withdrawn a pending executive order from former President Donald Trump to track the influence of the Chinese Communist Party-linked Confucius Institute at universities and colleges across the U.S., which many are concerned will pave the way for further influence in these institutions from this major global adversary. Quick Facts: Under the Trump proposal, schools would have been required to disclose their ties to the Confucius Institute, as critics of the educational program say its primary aim is to disseminate Chinese Communist Party (CCP) propaganda in U.S. schools. The Biden administration affirms that they mean to address concerns surrounding the Confucius Institute. Foreign influence in U.S. universities is a growing concern in the globalized West, as the Biden administration is expected to take a softer approach to China than Trump did. The order was reversed along with 65 pending Trump executive orders the day he took office, many of which, the Washington Free Beacon noted, "deal with key national security and immigration matters."

Read the full article here.

THE OPEN UNIVERSITY
UNIVERSITIES TO U.S. GOVERNMENT: WHEN IT COMES TO CHINA, HELP US HELP YOU.

Richard Lester | The Wire China | February 21, 2021

The ongoing deterioration in the U.S.-China relationship has left America's research universities scrambling to adjust. After decades of building ties with China, universities are unsure how to deal with the growing calls to decouple the U.S. and Chinese economies, especially in science and technology. If they fail to respond to anxieties in government and industry over technology leakage to China, and to American concerns over President Xi Jinping's increasingly repressive regime, its human rights violations in Xinjiang, Tibet, and Hong Kong, and the Chinese military buildup in East Asia, public support for the universities' key role in the U.S. research and innovation system will erode. But the wrong response could end up badly damaging the roots of American scientific and technological strength, including the openness of our universities to dynamic young researchers from China and elsewhere.

Read the full article here.

WHY AMERICA WOULD NOT SURVIVE A REAL FIRST STRIKE CYBERATTACK TODAY

Mike Rogers | The Hill | February 22, 2021

If a full on "turn the lights off" cyber war were to happen today, we would lose. Think about that. We would lose a cyber war. With a few clicks of the mouse, and in just a few seconds, hackers in Beijing or Moscow could turn off our electricity, millions would lose heat, groceries would spoil, banking machines would not work, and people could not get gasoline. It would be what we have seen down in Texas, but on national scale and with no end in sight. That we have escaped a digital catastrophe thus far is not due to skill. It is due to blind luck and restraint from our adversaries. Just a few weeks ago, hackers attacked a water treatment plant in Florida, trying to increase the amount of lye in the water to toxic levels. A worker was able to prevent the contamination. Luck was all that stood between hackers and a potentially deadly cyber incident. If that were not enough, we are still uncovering the full scale of the Solar Winds hack nearly three months on from its first disclosure. At least nine federal departments or agencies and over 100 companies were compromised and, as the probe continues, it remains likely that more targets are identified.

Read the full article here.

STEFANIK PROPOSES LEGISLATION TO LIMIT FEDERAL FUNDING FOR COLLEGES, UNIVERSITIES WITH CHINESE PARTNERSHIPS

Brooke Singman | Fox News | February 23, 2021

Rep. Elise Stefanik on Tuesday rolled out legislation that would limit federal funding for institutions of higher education that have partnerships with the People's Republic of China as Republicans take aim at taxpayer money for so-called Confucius Institutes. The bill, first obtained by Fox News, is titled the "End College Chinese Communist Partnerships Act" or the "End College CCP Act." The legislation would block any institution of higher education or postsecondary educational institution from receiving federal funds if it has "a contractual partnership in effect with an entity that is owned or controlled, directly or indirectly, by the Government of the People's Republic of China, or organized under the laws of the People's Republic of China." Department of Education funds that are provided directly to students are exempt from Stefanik's legislation.

Read the full article here.

U.S. TO IMPOSE SWEEPING RULE AIMED AT CHINA TECHNOLOGY THREATS

John D. McKinnon | The Wall Street Journal | February 26, 2021

The Biden administration plans to allow a sweeping Trump-era rule aimed at combating Chinese technology threats to take effect next month, over objections from U.S. businesses, according to people familiar with the matter. The rule, initially proposed in November, enables the Commerce Department to ban technology-related business transactions that it determines pose a national security threat, part of an effort to secure U.S. supply chains. Companies in technology, telecommunications, finance and other industries say the rule could stifle innovation and hurt competitiveness, and had expected it to be delayed as the administration undertakes a broad review of U.S. policy on Chinese technology. Now the administration is planning to go forward with the rule, the people said.

Read the full article here.

FINAL REPORT: NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

National Security Commission on Artificial Intelligence | February 19, 2021

Americans have not yet grappled with just how profoundly the artificial intelligence (AI) revolution will impact our economy, national security, and welfare. Much remains to be learned about the power and limits of AI technologies. Nevertheless, big decisions need to be made now to accelerate AI innovation to benefit the United States and to defend against the malign uses of AI. When considering these decisions, our leaders confront the classic dilemma of statecraft identified by Henry Kissinger: "When your scope for action is greatest, the knowledge on which you can base this action is always at a minimum. When your knowledge is greatest, the scope for action has often disappeared." The scope for action remains, but America's room for maneuver is shrinking. As a bipartisan commission of 15 technologists, national security professionals, business executives, and academic leaders, the National Security Commission on Artificial Intelligence (NSCAI) is delivering an uncomfortable message: America is not prepared to defend or compete in the AI era. This is the tough reality we must face. And it is this reality that demands comprehensive, whole-of-nation action.

Read the full article here.

EMBRACING A ZERO TRUST SECURITY MODEL

National Security Agency Cybersecurity Information | February 2021

As cybersecurity professionals defend increasingly dispersed and complex enterprise networks from sophisticated cyber threats, embracing a Zero Trust security model and the mindset necessary to deploy and operate a system engineered according to Zero Trust principles can better position them to secure sensitive data, systems, and services. Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access and other system responses.

Read the full article here.

EXCLUSIVE: HACKERS BREAK INTO 'BIOCHEMICAL SYSTEMS' AT OXFORD UNIVERSITY LAB STUDYING COVID-19

Thomas Brewster | Forbes | February 25, 2021

One of the world's top biology labs—one whose renowned professors have been researching how to counter the Covid-19 pandemic—has been hacked. Oxford University confirmed on Thursday it had detected and isolated an incident at the Division of Structural Biology (known as "Strubi") after Forbes disclosed that hackers were showing off access to a number of systems. These included machines used to prepare biochemical samples, though the university said it couldn't comment further on the scale of the breach. It has contacted the National Cyber Security Center (NCSC), a branch of the British intelligence agency GCHQ, which will now investigate the attack. "We have identified and contained the problem and are now investigating further," an Oxford University spokesperson said. "There has been no impact on any clinical research, as this is not conducted in the affected area. As is standard with such incidents, we have notified the National Cyber Security Center and are working with them."

Read the full article here.

KLOBUCHAR, REED, PETERS URGE NATIONAL SECURITY OFFICIALS TO TAKE STEPS TO COUNTER FOREIGN INFLUENCE CAMPAIGNS

Amy Klobuchar, United States Senator | February 25, 2021

U.S. Senator Amy Klobuchar (D-MN), Chairwoman of the Senate Rules Committee with oversight over federal elections, with Senator Jack Reed (D-RI), Chairman of the Committee on Armed Services, and Senator Gary Peters (D-MI), Chairman of the Homeland Security and Governmental Affairs Committee, urged national security officials to take steps to counter foreign influence campaigns. In the letter to Secretary of Homeland Security Alejandro Mayorkas, Director of National Intelligence Avril Haines, and National Security Advisor Jake Sullivan, the senators highlighted warnings of ongoing malign influence campaigns from Russia, China, and Iran, and other foreign adversaries seeking to undermine the U.S. and our allies from U.S. intelligence officials and independent researchers. The senators urged the implementation of three congressionally authorized initiatives designed to counter foreign malign influence campaigns that were not implemented by the Trump administration: the establishment of the Foreign Malign Influence Response Center at the Office of the Director of National Intelligence; the establishment of a social media threat and analysis center (in the form of an Information Sharing and Analysis Center (ISAC); and the creation of a Foreign Malign Influence Coordinator position on the White House National Security Council staff.

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