ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

August 19, 2020

U.S. WARNS COLLEGES TO DIVEST CHINA STOCKS ON DELISTING RISK

Kevin Cirilli and Shelly Banjo | Bloomberg | August 18, 2020

The U.S. State Department is asking colleges and universities to divest from Chinese holdings in their endowments, warning schools in a letter Tuesday to get ahead of potentially more onerous measures on holding the shares. “Boards of U.S. university endowments would be prudent to divest from People’s Republic of China firms’ stocks in the likely outcome that enhanced listing standards lead to a wholesale de-listing of PRC firms from U.S. exchanges by the end of next year,” Keith Krach, undersecretary for economic growth, energy and the environment, wrote in the letter addressed to the board of directors of American universities and colleges, and viewed by Bloomberg. “Holding these stocks also runs the high risks associated with PRC companies having to restate financials,” he said. The warning to endowments opens a new front in the Trump administration’s multipronged campaign against China’s government, businesses and individuals. The college and university funds represent billions of investment in Chinese companies, according to a 2019 investigation by Bloomberg, driven by the prospect of better returns.

Read the full report here.

DESIGNATION OF THE CONFUCIUS INSTITUTE U.S. CENTER AS A FOREIGN MISSION OF THE PRC

Michael R. Pompeo, Secretary of State | U.S. Department of State | August 13, 2020

The Trump Administration has made it a priority to seek fair and reciprocal treatment from the People’s Republic of China. For more than four decades, Beijing has enjoyed free and open access to U.S. society, while denying that same access to Americans and other foreigners in China. Furthermore, the PRC has taken advantage of America’s openness to undertake large scale and well-funded propaganda efforts and influence operations in this country. Today, the Department of State designated the Confucius Institute U.S. Center as a foreign mission of the PRC, recognizing CIUS for what it is: an entity advancing Beijing’s global propaganda and malign influence campaign on U.S. campuses and K-12 classrooms. Confucius Institutes are funded by the PRC and part of the Chinese Communist Party’s global influence and propaganda apparatus.

Read the full report here.

COMMERCE DEPARTMENT FURTHER RESTRICTS HUAWEI ACCESS TO U.S. TECHNOLOGY AND ADDS ANOTHER 38 AFFILIATES TO THE ENTITY LIST

U.S. Department of Commerce | August 17, 2020

The Bureau of Industry and Security (BIS) in the Department of Commerce (Commerce) today further restricted access by Huawei Technologies (Huawei) and its non-U.S. affiliates on the Entity List to items produced domestically and abroad from U.S. technology and software. In addition, BIS added another 38 Huawei affiliates to the Entity List, which imposes a license requirement for all items subject to the Export Administration Regulations (EAR) and modified four existing Huawei Entity List entries. BIS also imposed license requirements on any transaction involving items subject to Commerce export control jurisdiction where a party on the Entity List is involved, such as when Huawei (or other Entity List entities) acts as a purchaser, intermediate, or end user. These actions, effective immediately, prevent Huawei's attempts to circumvent U.S. export controls to obtain electronic components developed or produced using U.S. technology.

Read the full report here.

FY21 NDAA: NATIONAL SECURITY INNOVATION BASE AND RESEARCH SECURITY PROPOSALS

Will Thomas | American Institute of Physics | August 18, 2020

This bulletin reviews provisions proposed for inclusion in Congress' annual defense policy update that are focused on bolstering the "national security innovation base" and protecting federally funded research from exploitation by rival governments. The National Defense Authorization Act (NDAA) is the only major policy bill that Congress commits to passing annually and comprises a sprawling array of provisions that are crafted by the House and Senate Armed Services Committees, supplemented with amendments introduced by individual lawmakers. These provisions touch on all aspects of national security, with many aiming to strengthen the defense R&D enterprise, promote specific military technologies, and bolster U.S. nuclear security. The House and Senate approved their separate versions of this year's NDAA at the end of July on votes of 295 to 125 and 86 to 14, respectively. A conference committee is expected to convene this fall to hammer out a final version.

Read the full report here.

GLOBAL ENGAGEMENT: RETHINKING RISK IN THE RESEARCH ENTERPRISE

Glenn Tiffert, Jeffrey Stoff, and Kevin Gamache | Hoover Institution

The final version of Global Engagement: Rethinking Risk in the Research Enterprise is now available.

Neither the US government nor the universities and national laboratories in the US research enterprise are adequately managing the risks posed by research engagements with foreign entities. The task is quite simply falling through the cracks. Data with which to assess the performance of current frameworks for managing foreign engagement risk, to identify their defects, and to devise proportionate fixes is consequently in short supply. Dueling narratives have filled this evidentiary vacuum, pitting some who propose incremental adjustments against others who call for far-reaching change. Without a common set of facts to anchor the debate, consensus has proven elusive.

Read the full report here.

DOD’S IT SUPPLY CHAIN HAS DOZENS OF SUPPLIERS FROM CHINA, REPORT FINDS

Jackson Barnett | FedScoop | August 14, 2020

A report from data analytics firm Govini shows that the Department of Defense‘s IT supply chains has dozens of Chinese companies in it. It is unclear how much work, products or services come from these companies and in what way, but it still is a significant risk, according to Govini’s CEO. “The volume alone is important because it just amplifies the risk,” Tara Murphy Dougherty, a former DOD official and CEO of Govini, said in an interview. The report found several dozen Chinese suppliers from the IT, software and telecommunications equipment industries in a sample of more than 1,000 prime defense contractors’ supply chains. Govini’s findings come as the federal government, including the DOD, has been required by law to remove certain Chinese-owned technology firms from it its supply chains as of Aug. 13. The law, Section 889, Part B of the National Defense Authorization Act of 2019, goes as far as to bar the government from doing business with any contractor that “uses” the technology from Chinese companies like Huawei, ZTE and others.

Read the full report here.

CHINA AND THE UNITED STATES ARE IN A RACE TO LOSE POWER

Stephen M. Walt | Foreign Policy | August 17, 2020

Back in the bad old days of the Cold War, I recall hearing a well-known academic (and former diplomat) remark that the United States and the Soviet Union were engaged in “a relentless competition to see which one could lose influence fastest.” Assuming my memory is accurate, he then added, “Fortunately, the Soviets are winning.” I’m wary of facile analogies to that earlier period of great-power rivalry, but that observation seems to be an apt description of the current state of Chinese and American foreign policy. Beijing and Washington can each point to a few successes over the past year or two, but for the most part both seem to be perfecting the art of the own goal. Citizens of both countries have reason to be grateful; given how poorly their leaders have performed, it’s a small miracle the other side hasn’t taken better advantage.

Read the full report here.

TRUMP ORDERS TIKTOK'S CHINESE-OWNED PARENT COMPANY TO DIVEST INTEREST IN US OPERATIONS

Paul LeBlanc and Maegan Vazquez | CNN Politics | August 14, 2020

President Donald Trump issued an executive order Friday evening directing ByteDance, the Chinese-owned parent company of TikTok, to divest interest in the app's US operations within the next 90 days. Trump explained in the order that he believes there is "credible evidence" that ByteDance "might take action that threatens to impair the national security of the United States" following the company's acquisition of the social media app Musical.ly. The step marks just the latest twist in the dramatic back and forth between the popular video app and the President after he declared last month that he would ban TikTok from operating in the US. Trump issued an executive order last week that would ban the app from operating in the US in 45 days if it is not sold.

Read the full report here.

CHINESE ACADEMIC DISCIPLINED AFTER CRITICISING XI AND COMMUNIST PARTY

Yew Lun Tian | U.S. News and World Report | August 17, 2020

A retired Chinese professor who called President Xi Jinping a "mafia boss" and the ruling Communist Party a "political zombie" has been disciplined, according to her former employer, the latest such critic to face punishment in recent months. Cai Xia, who had taught democratic politics at the Central Party School of the Chinese Communist Party before retiring, is the third prominent figure in recent months to be disciplined after criticising the party and its leader. The school, which trains rising officials destined for promotion, announced on Monday that it had rescinded Cai's Communist Party membership and retirement benefits for making remarks that "had serious political problems and damaged the country's reputation". The notice on the school's website did not specify the remarks. Two Chinese political watchers, however, pointed to comments she made in a recording leaked online in June arguing that replacing Xi as party chief would be the first step to saving the party from itself.

Read the full report here.

NSA AND FBI EXPOSE RUSSIAN PREVIOUSLY UNDISCLOSED MALWARE "DROVORUB" IN CYBERSECURITY ADVISORY

National Security Agency | August 13, 2020

The National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) released a new Cybersecurity Advisory about previously undisclosed Russian malware. The Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165, whose activity is sometimes identified by the private sector as Fancy Bear, Strontium, or APT 28, is deploying malware called Drovorub, designed for Linux systems as part of its cyber espionage operations. Further details on Drovorub, to include detection techniques and mitigations, can be found in the joint NSA and FBI Cybersecurity Advisory. "This Cybersecurity Advisory represents an important dimension of our cybersecurity mission, the release of extensive, technical analysis on specific threats," NSA Cybersecurity Director Anne Neuberger said. "By deconstructing this capability and providing attribution, analysis, and mitigations, we hope to empower our customers, partners, and allies to take action.

Read the full report here.

US ARMY REPORT SAYS MANY NORTH KOREAN HACKERS OPERATE FROM ABROAD

Catalin Cimpanu | ZD Net | August 18, 2020

North Korea has at least 6,000 hackers and electronic warfare specialists working in its ranks, and many of these are operating abroad in countries such as Belarus, China, India, Malaysia, and Russia, the US Army said in a report published last month. Named "North Korean Tactics," the report a tactical manual that the US Army uses to train troops and military leaders, and which the Army has made public for the first time last month. The 332-page report contains a treasure trove of information about the Korean People's Army (KPA), such as military tactics, weapons arsenal, leadership structure, troop types, logistics, and electronic warfare capabilities. While the vast majority of the report deals with classic military tactics and capabilities, the report also shines a light into North Korea's secretive hacking units. "Most EW [electronic warfare] and cyberspace warfare operations take place within the Cyber Warfare Guidance Unit, more commonly known as Bureau 121," the US Army said.

Read the full report here.

DISMISSING CYBER CATASTROPHE

James Andrew Lewis | Center for Strategic and International Studies | August 17, 2020

A catastrophic cyberattack was first predicted in the mid-1990s. Since then, predictions of a catastrophe have appeared regularly and have entered the popular consciousness. As a trope, a cyber catastrophe captures our imagination, but as analysis, it remains entirely imaginary and is of dubious value as a basis for policymaking. There has never been a catastrophic cyberattack. To qualify as a catastrophe, an event must produce damaging mass effect, including casualties and destruction. The fires that swept across California last summer were a catastrophe. Covid-19 has been a catastrophe, especially in countries with inadequate responses. With man-made actions, however, a catastrophe is harder to produce than it may seem, and for cyberattacks a catastrophe requires organizational and technical skills most actors still do not possess. It requires planning, reconnaissance to find vulnerabilities, and then acquiring or building attack tools—things that require resources and experience.

Read the full report here.

COGNITIVE HACKING AS THE NEW DISINFORMATION FRONTIER

Izabella Kaminska | Financial Times | August 17, 2020

Persuasion doesn't need to influence the majority of the public to be effective. It's enough to convince just one per cent of a population to destabilise a democracy pretty effectively with protests, rioting and a collapse in institutional trust. So the question that really needs asking is: how hard is it to radicalise one per cent of the public with modern, weaponised forms of persuasion? The answer, experts say, is dangerously easy. Those who specialise in the field of the persuasive arts told FT Alphaville that in 2020 new cognitive hacking technology means digitally-crafted propaganda has power like never before and the biggest risk to cognitive security is now AI-driven influence hiding behind "secret" algorithms on social media platforms. For a moment, remove from the equation whether the social movements erupting across western democracies in 2020 are justified or not. The intention of this post is not to analyse the tenets of these movements, but rather to consider if it's possible, whether by propaganda, social conditioning or amplified feedback loops, to radicalise well-intentioned people to turn against their own interests.

Read the full report here.

FORMER CIA OFFICER CHARGED WITH SPYING FOR CHINA

Pete Williams | NBC News | August 17, 2020

A 15-year veteran of the CIA was charged Monday with selling U.S. secrets to China then unwittingly admitting his spying to the FBI. The method prosecutors said they used to get him to reveal the nature of his espionage was worthy of a spy novel itself. Court documents said 67-year-old Alexander Yuk Ching Ma of Honolulu was charged with violating U.S. espionage laws. Prosecutors said he joined the CIA in 1967 then served as a CIA officer until he retired from the agency in 1989. For part of that time he was assigned to work overseas in the East-Asia and Pacific region. Twelve years after he retired, prosecutors said Monday that Ma met with at least five officers of China's Ministry of State Security in a Hong Kong hotel room, where he "disclosed a substantial amount of highly classified national defense information," including facts about the CIA's internal organization, methods for communicating covertly, and the identities of CIA officers and human assets. "The trail of Chinese espionage is long and, sadly, strewn with former American intelligence officers who betrayed their colleagues, their country and its liberal democratic values to support an authoritarian communist regime," said John Demers, assistant attorney general for national security.

Read the full article here.

SECURITY NEWS THIS WEEK: THE NSA AND FBI EXPOSE FANCY BEAR'S SNEAKY HACKING TOOL

Brian Barrett | Wired | August 15, 2020

Last weekend, during and in the aftermath of a contentious presidential election, the country of Belarus effectively shut off access to most of the internet for its 9.5 million citizens. It's a tactic that has become increasingly popular among authoritarian regimes, whether it's a total blackout like Belarus' or more targeted censorship of specific apps like Telegram and WhatsApp. The outage lasted around three days, although some sites remain blocked. Elsewhere, we took a look at an Alexa bug that could have let a hacker access your entire voice history.

Read the full report here.

U.S. LABELS CHINESE LANGUAGE EDUCATION GROUP A DIPLOMATIC MISSION

Edward Wong | The New York Times | August 13, 2020

The State Department announced on Thursday that it was designating the U.S. headquarters of a Chinese government educational organization as a diplomatic mission, in the latest action by the Trump administration to limit official operations by China in the United States. The headquarters, called the Confucius Institute U.S. Center, in Washington, manages and provides funding for Chinese-language teachers and classes across the country. The university-level classes are operated out of 75 entities called Confucius Institutes, and the kindergarten through 12th-grade classes are run out of 500 entities called Confucius Classrooms.

Read the full report here.

U.S. AIR FORCE INTERNATIONAL SCIENCE DIVISION, TRI-SERVICE PARTNERS JOIN TECHNOLOGY TRANSITION ECOSYSTEM

Molly Lachance | Air Force Office of Scientific Research | August 6, 2020

The Air Force, Army and Navy international research offices jointly became the newest tenants last month at the Translation and Innovation Hub (I-HUB) at Imperial College London’s expansive White City Campus — a move expected to enhance partnerships with academics, industry, non-traditional innovators, and the UK Ministry of Defence, under the coordination of the Institute for Security Science and Technology (ISST) Innovation Ecosystem. “It’s all about relationships and tapping in and leveraging international talent,” explained Col. D. Brent Morris, the International Science Division Director at the Air Force Research Laboratory’s Air Force Office of Scientific Research (AFRL/AFOSR).

Read the full report 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

ASCE
ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM