ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

November 18, 2020

MEETING THE CHINA CHALLENGE

Working Group on Science and Technology in U.S-China Relations, University of San Diego and Asia Society Center on U.S.-China Relations; Peter Cowhey, Chair, and Susan Shirk and Orville Schell, Co-Chairs | November 4, 2020

Innovation in science and technology (S&T) is a core American strength. The United States has been the undisputed global technology leader since the end of World War II, but today, our preeminence faces three major interlinked challenges: The United States has allowed the foundations for its technological leadership to erode. It faces formidable competition from the People's Republic of China (PRC)—a country that has deployed full state power, and sometimes used illegal means, to build an innovation system to gain on the United States. And it has overreacted to the competition challenge from China, and in doing so, is poised to damage its own innovation ecosystem, which flourishes in an environment of global openness. To confront these challenges, the United States needs a clear-eyed strategy for S&T innovation that enhances our national competitiveness and protects our national security. We must do two things, now: make needed investments in and policy adjustments for our S&T base at home; and craft a new approach to global cooperation that minimizes the security risks China poses without unduly sacrificing the benefits of openness.

Read the full article here.

FORMER RAYTHEON ENGINEER SENTENCED FOR EXPORTING SENSITIVE MILITARY RELATED TECHNOLOGY TO CHINA

U.S. Department of Justice | November 18, 2020

Today, Wei Sun, 49, a Chinese national and naturalized citizen of the United States, was sentenced to 38 months in prison by District Court Judge Rosemary Marquez. Sun previously pleaded guilty to one felony count of violating the Arms Export Control Act (AECA). Sun was employed in Tucson for 10 years as an electrical engineer with Raytheon Missiles and Defense. Raytheon Missiles and Defense develops and produces missile systems for use by the United States military. During his employment with the company, Sun had access to information directly related to defense-related technology. Some of this defense technical information constituted what is defined as "defense articles," which are controlled and prohibited from export without a license under the AECA and the International Traffic in Arms Regulations (the ITAR). From December 2018 to January 2019, Sun traveled from the United States to China on a personal trip.

Read the full article here.

UNIVERSITY RESEARCHER PLEADS GUILTY TO LYING ON GRANT APPLICATIONS TO DEVELOP SCIENTIFIC EXPERTISE FOR CHINA

U.S. Department of Justice | November 12, 2020

A rheumatology professor and researcher with strong ties to China pleaded guilty to making false statements to federal authorities as part of an immunology research fraud scheme. Song Guo Zheng, 58, of Hilliard, appeared in federal court today, at which time his guilty plea was accepted by Chief U.S. District Judge Algenon L. Marbley. "Federal research funding is provided by the American tax payers for the benefit of American society — not as a subsidy for the Chinese Government," said Assistant Attorney General for National Security John Demers. "The American people deserve total transparency when federal dollars are being provided for research, and we will continue to hold accountable those who choose to lie about their foreign government affiliations in an attempt to fraudulently gain access to these funds."

Read the full article here.

CHINESE TALENT PROGRAM TRACKER

Emily Weinstein | Center for Security and Emerging Technology

The Chinese Talent Program Tracker is a catalogue of Chinese Party-State-sponsored initiatives aimed at cultivating China's domestic talent pool in support of China's strategic civilian and military goals. Viewed by Beijing as vital to Chinese economic and social development, talent programs aim to recruit everyone from experts to students of both Chinese and non-Chinese citizenship to fill positions across government, industry, defense, and academia to drive the innovation and growth of the Chinese economy. The information in this catalogue, as described in Chinese documents, resulted from analysis of primary Chinese sources publicly available on PRC ministry and government websites, state-owned media sources, and Chinese university websites. It is not meant to provide a comprehensive assessment of individual talent programs. Rather, it aims to make this information more accessible to the general public so they can have a better understanding of the depth and breadth of China's talent initiatives. This version of the catalogue includes national-level talent programs. Further iterations will include provincial, municipal, and sub-municipal-level programs.

Read the full article here.

NORTH KOREAN, RUSSIAN HACKERS TARGET COVID-19 RESEARCHERS: MICROSOFT

Raphael Satter | Reuters | November 13, 2020

Hackers working for the Russian and North Korean governments have targeted more than half a dozen organizations involved in COVID-19 treatment and vaccine research around the globe, Microsoft MSFT.O said on Friday. The software company said a Russian hacking group commonly nicknamed "Fancy Bear" - along with a pair of North Korean actors dubbed "Zinc" and "Cerium" by Microsoft - were implicated in recent attempts to break into the networks of seven pharmaceutical companies and vaccine researchers in Canada, France, India, South Korea, and the United States. Microsoft said the majority of the targets were organizations that were in the process of testing COVID-19 vaccines. Most of the break-in attempts failed but an unspecified number succeeded, it added. Few other details were provided by Microsoft. It declined to name the targeted organizations, say which ones had been hit by which actor, or provide a precise timeline or description of the attempted intrusions.

Read the full article here.

UNIVERSITIES WRESTLE WITH QUESTION OF HOW OPEN TO BE WITH CHINA

Eanna Kelly and Fintan Burke | Science Business | October 15, 2020

Universities around the world are wrestling with what – if anything – to do about the scale of China's influence on strategic industries and research fields. Concerns about China's authoritarian rulers are growing significantly in Europe, in light of what some see as the country's obfuscation of the origins of COVID-19, the treatment of its Uighur Muslim minority, the crackdown in Hong Kong, and more general concerns about industrial espionage. "Academic relations with China are becoming more politicised. Ten years ago, the mood was to extend collaboration with China. Now, while this is still happening, there's pressure to justify it," said Dominic Sachsenmaier, chair of modern China at the University of Göttingen. In a hardening of Brussels' stance towards Beijing, the bloc has recently drawn up rules that may be used to block Chinese entry into EU research programmes.

Read the full article here.

NEW DOD SECURITY CERTIFICATION ON THE HORIZON

Rob Simopoulos | Security Info Watch | November 10, 2020

There is a lot to think about as you run your business, and if you contract with the U.S. Department of Defense (DoD) or its supply chain, there may be even more to think about. In January 2020, the DoD launched a new compliance program called the Cybersecurity Maturity Module Certification (CMMC). This new standard builds on the existing DFARS 252.204-7012 regulation by adding five maturity levels, along with a verification and certification component. Prior to CMMC, organizations only had to self-attest that they met the DFARS requirements without requiring an external audit. It is estimated that there are more than 300,000 companies in the Defense Industrial Base sector, and with such a large number of these organizations interacting with sensitive data in one way or another, the DoD is aiming to address numerous cyber risks through the new program. Contractors who want to bid on DoD projects will need to become CMMC certified, possibly as early as next year, and certainly no later than 2025.

Read the full article here.

BEIJING'S TIGHTENING SUPPLY CHAIN POLICY RAISES RISKS FOR U.S., ALLIES' FIRMS

Pointe Bello | November 2020

The Communist Party of China (CPC) is responding to disruptions in foreign and domestic markets by increasing focus on growth of industrial supply chain clusters in an effort to decrease PRC dependence on foreign firms, increase PRC dominance of east and southeast Asian regional supply chains, and increase its exploitation of international financial and technological resources. Beijing's control and direction of PRC firms' behavior may impact the viability and security of the U.S.' and its allies' firms in and outside of the PRC. U.S. and allied country firms, particularly in the tech industry, should assess the risk that their links to the PRC could be substantially outcompeted or coopted by growing state support of PRC-controlled high-tech industries. They should similarly remain vigilant against the threat of forced technology transfer and industrial espionage that have become integral to the PRC's development strategy.

Read the full article here.

CHINA UNLIKELY TO FIND BIDEN A SOFT TOUCH

David Brunnstrom and Humeyra Pamuk | Reuters | November 7, 2020

In his unsuccessful campaign for re-election, President Donald Trump repeatedly warned that a victory for Joe Biden would be a win for China and that Beijing would "own America." Despite that rhetoric, there is little to suggest Beijing will find Biden a soft alternative to Trump, who dramatically shifted the U.S. narrative to confront the world's second-largest economy in his final year in power. Even before Trump took office, the last Democratic administration of President Barack Obama and then Vice President Biden had significantly hardened its attitude towards China. After initial efforts to engage Beijing, Trump's administration took this further, pushing back forcefully against China's efforts to spread its influence globally, earning some grudging praise from Biden advisers despite a bitterly fought election campaign. Biden has not laid out a detailed China strategy, but all indications are he will continue the tough approach to Beijing. Diplomats, analysts and former officials who advised the Biden campaign do though expect a more measured tone after Trump's hip-fired threats, and an emphasis on "strategic competition" rather than outright confrontation. That said, Biden has at times gone even further than the outgoing president in attacking China.

Read the full article here.

PORTMAN COMMENTS ON FORMER OSU PROFESSOR'S GUILTY PLEA

The Highland County Press | November 12, 2020

Today, U.S. Senator Rob Portman (R-OH) issued the following statement after David M. DeVillers, United States Attorney for the Southern District of Ohio, and FBI Cincinnati Special Agent in Charge Chris Hoffman announced that Song Guo Zheng, a former Ohio State professor, has pled guilty to making false statements to federal authorities related to his affiliation with China's Thousand Talents Program while receiving taxpayer-funded grants. Portman, as chairman of the Permanent Subcommittee on Investigations (PSI), led a year-long investigation into China's talent recruitment programs like the Thousand Talents Program, culminating in a bipartisan report in November 2019 that detailed how China has recruited U.S.-based scientists and researchers since the late 1990s and incentivized them to transfer U.S. taxpayer-funded research and intellectual property (IP) to China for their own military and economic gain.

Read the full article here.

THE LIBERTY TIMES EDITORIAL: CHINA IS INCAPABLE OF INNOVATION

Taipei Times | November 15, 2020

With no end in sight to the US-China trade dispute, Beijing is feeling a noose tighten around its neck, and Chinese President Xi Jinping (習近平) has said that, even though China is a major manufacturing nation, it still has a deficit of talent in crucial core technologies. Given this, the buzzword flying around last month's Fifth Plenary Session of the 19th Chinese Communist Party (CCP) Central Committee was "innovation." There was talk of implementing major breakthroughs in core technologies to propel the country into the leading ranks of innovative nations, of placing innovation at the center of the country's modernization drive, of the importance of scientific and technological self-reliance in the strategic support of national development, of how innovation is the soul of national progress, and of how "grasping innovation is grasping development and seeking innovation is seeking the future." The problem is that innovation is not about mobilizing the workforce, nor is it about pulling out all the stops. The sad truth is that a one-party totalitarian government acts as a straitjacket on innovation.

Read the full article here.

READY OR NOT…GOVERNMENT CONTRACTOR CYBERSECURITY REQUIREMENTS ROLL OUT THIS MONTH

Rose Stern and Jason Vespoli | JD Supra | November 9, 2020

New Department of Defense (DoD) regulations related to government contractor Cybersecurity requirements become effective November 30, 2020. The progressive steps to mandatory contractor Cybersecurity Maturity Model Certification (CMMC) are expected to roll out over the next 5 years. However, certain preliminary actions are required this month to ensure that contractors are eligible for award of new contracts, task orders, delivery orders, or option terms. The new CMMC requirements essentially build on existing regulations. Under DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, contractors are required to comply with National Institute of Standards and Technology (NIST) SP 800-171, in the protection of certain contractor and government information. Defense contractors and subcontractors are required to provide "adequate security" to store, process, or transmit Controlled Unclassified Information (CUI) on information systems or networks, and to report cyber incidents that affect systems or networks.

Read the full article here.

DOJ: UNIVERSITY RESEARCHER PLEADS GUILTY TO DEVELOPING SCIENTIFIC EXPERTISE FOR CHINA

Alexis Berdine | News 4 Tucson KVOA | November 13, 2020

On Thursday, the United States Department of Justice (DOJ) announced a rheumatology professor and researcher with strong ties to China pleaded guilty to making false statements to federal authorities as part of an immunology research fraud scheme. According to the DOJ, Song Guo Zheng, a 58-year old man admitted he lied on applications in order to use approximately $4.1 million in grants from the National Institutes of Health (NIH) to develop China's expertise in the areas of rheumatology and immunology. "Federal research funding is provided by the American tax payers for the benefit of American society—not as a subsidy for the Chinese Government," John Demers, Assistant Attorney General for National Security said. "The American people deserve total transparency when federal dollars are being provided for research, and we will continue to hold accountable those who choose to lie about their foreign government affiliations in an attempt to fraudulently gain access to these funds." The DOJ said Zheng was a professor of internal medicine who led a team conducting autoimmune research at The Ohio State University and Pennsylvania State University.

Read the full article here.

UK PUTS CHINA CORPORATE DEALS IN REGULATORS' CROSSHAIRS

Jet Encila | Business Times | November 11, 2020

The UK will Wednesday step in to prevent takeovers and corporate deals by China and other foreign companies that have the potential to endanger national security, it said. The change is the UK's most sweeping corporate intervention measure for almost 20 years. Set to be published Wednesday, the National Security and Investment Bill will allow ministers to examine and intercede in foreign investments and give them powers to block acquisitions any time within five years following the conclusion of a deal. According to UK Business Minister Alok Sharma, the law will mean "we can continue to welcome job-generating investment to our shores while shutting out those who could threaten the safety of the British people," Reuters quoted the official as saying. The law will allow the UK to address long-standing concerns that some corporate deals could bring disrepute by indiscreet or reckless behavior and compromise security or vital economic infrastructure, Sharma said.

Read the full article here.

TRUMP BARS AMERICANS FROM INVESTING IN FIRMS THAT HELP CHINA'S MILITARY

Gordon Lubold and Dawn Lim | The Wall Street Journal | November 12, 2020

President Trump signed an executive order prohibiting Americans from investing in a group of Chinese companies the U.S. says supply and otherwise support China's military, intelligence and security services. The order blocks American companies and individuals from owning shares directly or through funds that include any of 31 companies identified by the U.S. as aiding the modernization of the People's Liberation Army, or PLA, and China's intelligence and security services.

Read the full article here.

HOW CYBER POLICY WILL EVOLVE UNDER BIDEN

Eric Geller | Politico | November 9, 2020

A presidential election closely monitored for cyberattacks — but surprisingly free of them — reached an apparent conclusion on Saturday morning when Vice President Joe Biden secured the necessary electoral votes to win the White House. Under a President Biden, U.S. cyber policy is likely to see a major evolution. As yours truly reports in a new story, President-elect Biden will elevate cybersecurity issues once he takes office, even as he continues many of the Trump administration's policy initiatives, according to close observers of Biden and the cyber policy landscape. "What you'll see is a recommitment to cyber being an important issue," said Chris Painter, who served as the top U.S. cyber diplomat from 2011 to 2017. "He'll take the good things that have happened, and he'll make them more consistent and strategic." James Lewis, a cyber expert at the Center for Strategic and International Studies, predicted that Biden would marry "a high degree of continuity" with "a lot smoother implementation."

Read the full article here.