ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

July 21, 2021

BIDEN ADMINISTRATION BLAMES HACKERS TIED TO CHINA FOR MICROSOFT CYBERATTACK SPREE

Dustin Volz and Aruna Viswanatha | The Wall Street Journal | July 19, 2021

The Biden administration Monday publicly blamed hackers affiliated with China's main intelligence service for a far-reaching cyberattack on Microsoft Corp. email software this year, part of a global effort to condemn Beijing's malicious cyber activities. In addition, four Chinese nationals, including three intelligence officers, were indicted over separate hacking activity. The U.S. government has "high confidence" that hackers tied to the Ministry of State Security, or MSS, carried out the unusually indiscriminate hack of Microsoft Exchange Server software that emerged in March, senior officials said. "The United States and countries around the world are holding the People's Republic of China (PRC) accountable for its pattern of irresponsible, disruptive, and destabilizing behavior in cyberspace, which poses a major threat to our economic and national security," Secretary of State Antony Blinken said. The MSS, he added, had "fostered an ecosystem of criminal contract hackers who carry out both state-sponsored activities and cybercrime for their own financial gain."

Read the full article here.

IRANIAN HACKERS IMPERSONATED ACADEMICS AT LONDON UNIVERSITY

University World News | July 17, 2021

Iranian hackers impersonated academics at London's School of Oriental and African Studies to conduct an online espionage campaign targeting experts on the Middle East, according to the cyber security company Proofpoint, writes Helen Warrell for Financial Times. The hacking attempt was carried out by a group called Charming Kitten, also known as 'Phosphorus' and APT35, which is widely thought by regional experts to carry out intelligence efforts on behalf of Iran's elite Revolutionary Guard. Iran – alongside Russia, China and North Korea – is one of the most potent cyber aggressors facing the United Kingdom and its allies. Lindy Cameron, chief executive of the National Cyber Security Centre, a branch of signals intelligence agency GCHQ, warned last month that Iran was using digital technology to "sabotage and steal" from a range of British organisations.

Read the full article here.

WHY IS CHINA FALLING BEHIND ON BREAKTHROUGH INNOVATION?

Qiang Zha | University World News | July 17, 2021

This past year witnessed not only a global health crisis, but also a dramatic hit on China's academic profession. There has been a U-turn with respect to academic appraisal exercises in Chinese universities. In the past decade, enormous weight was placed on publications in journals sourced by the Science Citation Index (SCI), a commercial citation index that records citations of articles published in its indexed science, medicine and technology journals. Those journals are thus considered to be leading, and publishing in those journals would not only lead to merit pay but also preference in appraisal exercises, leading to professional promotion and talent programme opportunities, in turn bringing increased personal income and research resources. For example, a paper published in a top SCI-indexed journal could earn a bonus of up to US$85,000. Consequently, China's annual outputs of papers published in SCI-indexed journals soared from 120,000 in 2009 to 450,000 in 2019.

Read the full article here.

AN AUSTRALIAN DARPA? UNIVERSITY RESEARCH VITAL TO NATIONAL SECURITY

Brendan Nicholson | Australian Strategic Policy Institute | July 14, 2021

Providing significant amounts of Defence funding to Australia's universities could drive urgent national security research while ensuring the survival of the institutions and reducing their dependence on large numbers of students from China. A new ASPI paper urges the establishment of a formal partnership involving the Defence Department, defence industry and Australian universities via the creation of an Australian Defence Advanced Research Projects Agency, or Australian DARPA—based on the highly successful American model. In An Australian DARPA to turbocharge universities' national security research: securely managed Defence-funded research partnerships in Five-Eyes universities, authors Robert Clark, a former chief defence scientist, and ASPI's executive director, Peter Jennings, say there is a significant opportunity to boost international defence scientific and technical research cooperation with 'Five Eyes' partners the United States, Britain, Canada and New Zealand.

Read the full article here.

HOW CAN I ASSESS RISKS IN PARTNERSHIPS?

Government of Canada | July 12, 2021

Domestic and international partnerships are an essential component of Canada's open and collaborative academic research, guided by the principles of academic freedom and institutional autonomy. The majority of research partnerships have transparent intentions that provide mutual benefits to all research partners. However, some activities by foreign governments, militaries and other actors pose real risks to Canada's national security and the integrity of its research ecosystem. To address these risks, researchers, research institutions, federal granting agencies, and the Government of Canada have a shared responsibility to identify and mitigate any potential national security risks related to research partnerships. To ensure the Canadian research ecosystem is as open as possible and as secure as necessary, the Government of Canada is introducing the National Security Guidelines for Research Partnerships. The purpose of the guidelines is to integrate national security considerations into the development, evaluation, and funding of research partnerships.

Read the full article here.

CHINESE NATIONAL GETS 3 1/2 YEARS IN JAIL FOR SCHEME TO BUY U.S. COMMANDO CRAFT

Bill Gertz | The Washington Times | July 16, 2021

A Chinese national was sentenced to 3 ½ years in prison on Friday as part of what U.S. officials said was a plot to illegally export inflatable military boats that are used by special operations commandos to China. Ge Songtao, 51, of Nanjing, China, pleaded guilty in federal court in Florida last fall to charges of conspiracy to submit false export information to the federal government. Analysts said the case reveals how China's military has gone through Hong Kong to obtain embargoed goods. U.S. District Judge Harvey Schlesinger, during a hearing in Jacksonville federal court, said Ge intended to reverse-engineer the special military-grade engines and sell a knock-off version to Beijing's military. The boats were described in court as "maritime raiding craft." According to court papers in the case, Ge and an associate, Yang, worked for a Shanghai company that sought to buy seven inflatable boats equipped with engines capable of using either gasoline, diesel or jet fuel. The boats are designed to covertly dispatch special operations commandos from submarines or aircraft and are not available in China.

Read the full article here.

U.S. SENATE PASSES BILL TO BAN ALL PRODUCTS FROM CHINA'S XINJIANG

Michael Martina | Reuters | July 15, 2021

The U.S. Senate passed legislation on Wednesday to ban the import of products from China's Xinjiang region, the latest effort in Washington to punish Beijing for what U.S. officials say is an ongoing genocide against Uyghurs and other Muslim groups. The Uyghur Forced Labor Prevention Act would create a "rebuttable presumption" assuming goods manufactured in Xinjiang are made with forced labor and therefore banned under the 1930 Tariff Act, unless otherwise certified by U.S. authorities. Passed by unanimous consent, the bipartisan measure would shift the burden of proof to importers. The current rule bans goods if there is reasonable evidence of forced labor. The bill must also pass the House of Representatives before it can be sent to the White House for President Joe Biden to sign into law. It was not immediately clear when that might take place. Republican Senator Marco Rubio, who introduced the legislation with Democrat Jeff Merkley, called on the House to act quickly.

Read the full article here.

DECOUPLING IN SCIENCE AND EDUCATION: A COLLATERAL DAMAGE BEYOND DETERIORATING US–CHINA RELATIONS

Li Tang, Cong Cao, Zheng Wang, and Zhuo Zhou | Science and Public Policy | July 16, 2021

The world's two largest scientific communities are now witnessing unprecedented yet escalating tensions ever since the Cold War. Since 2018, dozens of prominent scientists in the US, most of Chinese origin, have been fired or investigated for undisclosed ties with China (Hao and Guo, 2021; Mervis 2020). These, combined with continuing shuttering of Confucius Institutes on US university campuses, strict limits on Chinese nationals studying or conducting research in science, technology, engineering, and mathematics (STEM) fields, revocations of visas for Chinese scholars who are already studying in the US, the closures of Chinese Consulate in Houston and the US Consulate in Chengdu in succession, and the recent The United States Innovation and Competition Act of 2021 (USICA), are casting long shadows on the US–China scientific relationship.

Read the full article here.

TWO DECADES AFTER 9/11, BRITISH SPIES TURN FOCUS BACK TO RUSSIA AND CHINA

Guy Faulconbridge | Reuters | July 14, 2021

Britain's top domestic spymaster cautioned citizens on Wednesday to treat the threat of spying from Russia, China and Iran with as much vigilance as terrorism, in a shift of focus back to counter-espionage nearly two decades after the 9/11 attacks. The Sept. 11, 2001 attacks on the United States made tackling terrorism the biggest priority for Western intelligence agencies, with vast resources being focused on the threat from home-grown and foreign-based militants. But the growing assertiveness of post-Soviet Russia, the rise of China, and Iran's sometimes daring espionage has forced the West's spies to return their focus to counter-intelligence, or spies tracking, countering and tackling other spies. Security Service (MI5) Director General Ken McCallum said foreign spies killed, stole technology, sought to corrupt public figures, sow discord and attack infrastructure with potentially devastating cyberattacks.

Read the full article here.

THREAT TO UK FROM HOSTILE STATES COULD BE AS BAD AS TERRORISM, SAYS MI5 CHIEF

Dan Sabbagh | The Guardian | July 14, 2021

The chief of MI5 is to warn that the activities of China, Russia and other hostile states could have as large an impact on the public as terrorism, marking a significant shift in emphasis from the UK's domestic spy agency. Giving his annual threat update on Wednesday, Ken McCallum is expected to say that the British public will have to "build the same public awareness and resilience to state threats that we have done over the years on terrorism". But while the threat from Russia, as demonstrated by the poisoning of the Skripals in Salisbury, is familiar to the British public – the spy chief will argue that threats that typically come from China are not. McCallum will say that universities and researchers risk "having their discoveries stolen or copied" if they are not vigilant and that businesses could be "hollowed out by the loss of advantage they've worked painstakingly to build". "Given half a chance, hostile actors will short-circuit years of patient British research or investment.

Read the full article here.

CHINA IS KILLING ITS TECH GOLDEN GOOSE

Minxin Pei | Australian Strategic Policy Institute | July 13, 2021

US politicians from both congressional parties are worried that China is overtaking America as the global leader in science and technology. In a rare display of bipartisanship, the normally gridlocked Senate passed a bill in early June to spend close to US$250 billion in the next decade to promote cutting-edge research. But lawmakers may be fretting unnecessarily, because the Chinese government seems to be doing everything possible to lose its tech race with America. The latest example of China's penchant for self-harm is the sudden and arbitrary regulatory action taken by the Cyberspace Administration of China (CAC) against Didi Chuxing, a ride-hailing company that recently raised US$4.4 billion in an IPO on the New York Stock Exchange. On 2 July, just two days after Didi's successful offering, which valued the firm at more than US$70 billion, the CAC, a department of the ruling Chinese Communist Party masquerading as a state agency, announced a data-security review of the company. Two days later, the CAC abruptly ordered the removal of Didi from app stores, a move that wiped out nearly a quarter of the firm's market value. The CCP's crackdown against Didi under the pretext of data security seems to be just the beginning of a wider campaign to assert control over China's thriving tech sector.

Read the full article here.

REPUTATION LAUNDERING IN THE UNIVERSITY SECTOR OF OPEN SOCIETIES: AN INTERNATIONAL FORUM WORKING PAPER

Alexander Cooley, Tena Prelec, John Heathershaw, and Tom Mayne | National Endowment for Democracy
May 25, 2021

Modern kleptocracy thrives on the ability of kleptocrats and their associates to use their ill-gotten gains in open settings. This often takes the form of investing in high-end real estate or other luxury goods, which serves to both obscure the corrupt origin of the money and to protect it for future use. But there is also a subtler dynamic at play. The use of kleptocratic-linked funding or other forms of engagement in open societies to blur the illicit nature and source of the donation serves to launder kleptocrats' reputations, as well as their cash. This careful cultivation of positive publicity and influence empowers autocrats and their cronies. It also entrenches kleptocrats—and the regimes with which they are associated—in positions of power. Universities and think tanks in open settings are prime targets for reputation laundering.

Read the full article here.

THE FEDERAL GOVERNMENT CAN'T COUNTER CHINA ON ITS OWN

Alexander B. Gray | National Review | July 12, 2021

As the Biden administration begins to shape its China policy, from supporting Taiwan against Chinese provocations to strengthening export controls on entities aligned with the People's Liberation Army, it is increasingly clear that it is following in its predecessor's footsteps. Other key players in this conversation, however, are still formulating their respective approaches. Those actors are U.S. states, and they have a significant role to play in the unfolding great-power competition between China and the United States. Take Chinese investment in state pension funds. At the federal level, the Trump administration spoke candidly of the risk posed by investing federal employees' pensions in China through the Thrift Savings Plan (TSP). Such investment "would expose the retirement funds to significant and unnecessary economic risk, and it would channel federal employees' money to companies that present significant national security and humanitarian concerns," wrote then-national-security-adviser Robert O'Brien and then-National Economic Council–director Larry Kudlow in May 2020.

Read the full article here.

TRADE SECRETS LAW IN FLORIDA COLLIDES WITH ACADEMIC CULTURE

Kyle Jahner | Bloomberg Law | July 13, 2021

A Florida law designed to curb theft trade secrets from research institutions by China amps up punishment but doesn't necessarily address a core problem at places like universities: keeping secrets in the first place. The Combating Corporate Espionage in Florida Act, signed into law June 8, enhanced penalties for trade secret theft, particularly theft to benefit a foreign government. It was paired with a law requiring universities and state agencies to disclose foreign grants larger than $50,000, all in the wake of cases of Florida researchers who failed to disclose ties to China. But the law doesn't address the core day-to-day practice of identifying and protecting trade secrets, something that cuts against the collaborative culture of academia, University of Florida trade secrets professor Elizabeth A. Rowe said. She said treating innovations as proprietary information has caught on somewhat in the last two decades as schools look to protect exclusivity on an increasing source of income, although academia remains well behind the private sector.

Read the full article here.

CULTURE OF CONSENSUS STOPPED PUBLIC SERVICE FROM TACKLING CHINA THREAT EARLY: THINK TANKS

Daniel Y. Teng | The Epoch Times | July 12, 2021

A culture of consensus held back the Australian Public Service from recognising, and acting, on the threat posed by the Chinese Communist Party (CCP), leading think tank experts argue. Peter Jennings of the Australian Strategic Policy Institute said there was a "remarkable degree of conformity" within the debate in the public service, particularly around foreign affairs. "There's not a lot of warmth or welcome towards people who challenge that conformity. You could argue that perhaps that's a product of the design of the federal capital, which means that foreign and defence policy is very much a public service business inside the Australian Capital Territory and that, unlike Washington or London, it's not troubled by a broader exposure to a range of views," he told the Senate Standing Committee on Foreign Affairs and Trade.

Read the full article here.

RISK ASSESSMENTS REQUIRED TO APPLY FOR NSERC'S ALLIANCE GRANTS PROGRAM, FEDERAL GOVERNMENT ANNOUNCES

Michel Proulx | University Affairs | July 13, 2021

Researchers applying for funding under the Natural Sciences and Engineering Research Council's Alliance Grants program will now have to complete a security risk assessment as part of their application if the work involves a private sector partner, the federal government announced Monday. In a news release, it said NSERC will conduct the risk assessments on a case-by-case basis in consultation with national security agencies and federal departments. Projects that have identified risks must also include mitigation measures. "Projects that are deemed high risk, or where the risk cannot be mitigated, will not be funded," said François-Philippe Champagne, minister of innovation, science and industry.

Read the full article here.

CANADA TIGHTENS UP SECURITY RULES FOR FOREIGN RESEARCH COLLABORATION

Richard L. Hudson | Science Business | July 13, 2021

The Canadian government joined a push by western governments to tighten up security on research collaborations that could leak secrets to China or other countries deemed a security risk. A new policy, announced 12 July, would require Canadian researchers to start including a security risk-assessment form with certain grant applications involving collaboration with foreign companies. The government said it will reject the application if, "in consultation with" Canadian intelligence services, it finds a security risk. It highlighted as especially sensitive a wide range of emerging technologies including quantum computing, aerospace and artificial intelligence. The government didn't name China as a target; but work on the policy began in 2018 as western concern mounted about incorporating Chinese technology in next-generation 5G mobile phone networks.

Read the full article here.