RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE

THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary

May 2, 2024

HUAWEI SECRETLY BACKS US RESEARCH, AWARDING MILLIONS IN PRIZES

Kate O'Keeffe | Bloomberg | May 2, 2024

Huawei Technologies Co., the Chinese telecommunications giant blacklisted by the US, is secretly funding cutting-edge research at American universities including Harvard through an independent Washington-based foundation. Huawei is the sole funder of a research competition that has awarded millions of dollars since its inception in 2022 and attracted hundreds of proposals from scientists around the world, including those at top US universities that have banned their researchers from working with the company, according to documents and people familiar with the matter. The competition is administered by the Optica Foundation, an arm of the nonprofit professional society Optica, whose members' research on light underpins technologies such as communications, biomedical diagnostics and lasers. The foundation "shall not be required to designate Huawei as the funding source or program sponsor" of the competition and "the existence and content of this Agreement and the relationship between the Parties shall also be considered Confidential Information," says a nonpublic document reviewed by Bloomberg.

Read the full article here.

REPUBLICAN DEMANDS INVESTIGATION INTO 'DANGEROUS DOLLARS' SENT TO CHINA

Nick Mordowanec | Newsweek | April 26, 2024

Republican Senator Joni Ernst has called for the expansion of an audit of the Department of Defense (DOD) into the extent of funding sent to Chinese research laboratories, including into work on advanced artificial intelligence that was exposed by Newsweek. The audit by the Office of the Inspector General was spurred by a January 25 letter written by the Iowa lawmaker and former Wisconsin Representative Mike Gallagher. They requested information from the DOD on any funding provided to the People's Republic of China or its affiliates for research activities relevant to the reporting requirement of the National Defense Authorization Act (NDAA). That included funding for COVID-19 research. In January, lawmakers also called for answers from the DOD after a Newsweek investigation showed that a top Chinese AI scientist had received more than $30 million in U.S. grants, including from the Pentagon. "The Department of Defense should defend the nation, not support research with the potential to do us harm," Ernst told Newsweek on Wednesday.

Read the full article here.

AS BIS PREPARES TO ISSUE UPDATED EXPORT CONTROLS, A NEW REPORT FROM JAMES MULVENON HIGHLIGHTS SMIC'S TIES TO CHINESE MILITARY

China Tech Threat | October 16, 2023

In 2020, a report by cybersecurity expert James Mulvenon on Chinese chipmaker SMIC's ties to the Chinese military undergirded the Commerce Department's export controls targeting the company. Those controls (purportedly) cut off SMIC's access to certain leading edge American technologies. But as Mulvenon and Joseph McReynolds write in a new report released in October 2023, "U.S. sanctions efforts to date have not been sufficient to deter SMIC; the firm has even opened a new Southern California office in recent months with public celebrations and fanfare." The title of the authors' work says it all: "SMIC Races Over BIS Speed Bump to Fulfill China's Strategic Ambitions: Continued Troubling Activities Even After 2020's Entity List Designation." In sum, Mulvenon and Reynolds write, "Between SMIC's progress at 7nm production and China's robust industrial practices continuing apace, there is little evidence that would suggest the current export control regime has successfully eased the threat that SMIC poses to U.S. national security interests."

Read the full article here.

THE FATES OF NATIONS

Michael J. Mazarr, Alexis Dale-Huang, John Deak, Gregory Weider Fauerbach, Stacie Goddard, Timothy R. Heath, and Joshua Shifrinson | RAND | April 10, 2024

The United States, according to official U.S. national security statements and an avalanche of commentary since about 2016, is engaged in a long-term strategic rivalry with China and a lesser — but still critical — rivalry for influence with Russia. Many U.S. strategy documents refer to the concept of strategic competition, but the core idea — and increasingly the reality — of these relationships matches the classic historical concept of a great power rivalry. These rivalries, especially with China, promise to define U.S. foreign policy and national security challenges for decades. Yet most assessments of these rivalries tend to ignore the critical question of outcomes. This report is part of a larger project on the societal sources of national dynamism and competitive advantage.

Read the full article here.

SECURITY REVELATIONS: MESSAGES BETWEEN CHINESE HACKERS SHOW AUSTRALIAN STRATEGIC POLICY INSTITUTE IS A TARGET

James King | The Nightly | April 10, 2024

Chinese spymasters have identified Australia's top security research institute as a priority target in their cyber-attack operations, with an investigation by The Nightly for the first time able to reveal messages between hackers that refer to our nation. The group chat exchanges also offer a remarkable insight into the daily lives and frustrations of state-sponsored hackers working for China, including their dismay at being told they're working too slowly while being tasked with disrupting "a big asset in two days". The Nightly investigation can reveal hackers working for the Chinese Government have been directed to target the Australian Strategic Policy Institute. Withdrawing funding for the institute was among 14 demands to the Australian Government released by the Chinese embassy in 2020.

Read the full article here.

CHINA'S INTELLIGENCE SHAKEUP BOOSTS INFORMATION WARFARE

Matt Brazil | SpyTalk | April 25, 2024

In A Major Shakeup at the top of China's intelligence and security apparatus, President Xi Jinping last Friday unexpectedly abolished its key eavesdropping and codebreaking agency, the Strategic Support Force (SSF) and replaced it with three new agencies put directly under the Chinese Communist Party's military oversight body, the Central Military Commission. It's the rough political equivalent of President Biden abolishing the NSA and creating three new powerful spy agencies under the direct purview of the White House National Security Council. Analysts told SpyTalk that rumors of an intelligence shakeup have been floating around for at least several weeks, but the creation of three separate "forces," as China calls them, from the SSF, including a new information warfare agency, was a surprise. It reflected Xi's dissatisfaction with the rate of progress in the development of China's "intelligentized warfare," or what the U.S. calls Joint Doctrine, the fusing of ground, air, space, cyber and naval forces operations through digital networks bolstered by artificial intelligence.

Read the full article here.

CHINA'S ALTERNATIVE ORDER AND WHAT AMERICA SHOULD LEARN FROM IT

Elizabeth Economy | Foreign Affairs | April 23, 2024

By now, Chinese President Xi Jinping's ambition to remake the world is undeniable. He wants to dissolve Washington's network of alliances and purge what he dismisses as "Western" values from international bodies. He wants to knock the U.S. dollar off its pedestal and eliminate Washington's chokehold over critical technology. In his new multipolar order, global institutions and norms will be underpinned by Chinese notions of common security and economic development, Chinese values of state-determined political rights, and Chinese technology. China will no longer have to fight for leadership. Its centrality will be guaranteed.

Read the full article here.

ON WORLD IP DAY, LET'S REMEMBER ALL THE STOLEN INNOVATION

Urmika Deb, Gatra Priyandita and Bart Hogeveen | Australian Strategic Policy Institute | April 26, 2024

As we celebrate World Intellectual Property Day today on 26 April, let's remember all the innovation that has been stolen. While innovators have had their intellectual property stolen for centuries, in modern times they face an avalanche of cyber-enabled attempts at theft of their knowhow. Hacking groups, typically operating with consent from state authorities, exploit vulnerabilities in information and communication technology to grab copious amounts of trade secrets and other business information for commercial gain. These attacks are increasing in scale. Between 30 and 40 identified state-sponsored espionage campaigns affected or targeted private entities globally in 2021–22. They involve sectors of the economy across commercial value chains and industrial development priorities. And they're affecting IP-intensive businesses in advanced economies and emerging economies alike. In 2020, 56 percent of cases struck economies in Southeast Asia, Middle East, Africa, South Asia and Latin America.

Read the full article here.

THE XI FILES: HOW CHINA SPIES

Nigel Inkster | The Spectator | April 27, 2024

Most states spy. In principle there's nothing to stop them. But China's demand for intelligence on the rest of the world goes far beyond anything western intelligence agencies would typically gather. It encompasses masses of commercial data and intellectual property and has been described by Keith Alexander, a former head of America's National Security Agency, as 'the greatest transfer of wealth in history'. As well as collecting data from government websites, parliamentarians, universities, thinktanks and human rights organisations, China also targets diaspora groups and individuals. Chinese cyber intrusions have targeted British MPs and stolen population-level data from the UK Electoral Commission database. In the US, meanwhile, Congress has just cracked down on the Chinese-owned TikTok, which has admitted that some of its employees had been spying on American journalists.

Read the full article here.

OSHIT: SEVEN DEADLY SINS OF BAD OPEN SOURCE RESEARCH

Tristan Lee, Kolina Koltai and Giancarlo Fiiorella | Bellingcat | April 25, 2024

Universities and research institutes in China have been able to buy high-end Nvidia artificial intelligence chips via resellers, despite stronger US curbs imposed by Washington late last year. A review of hundreds of tender documents by Reuters shows 10 Chinese entities acquired advanced Nvidia chips embedded in server products made by Super Micro Computer, Dell Technologies and Taiwan's Gigabyte Technology after the US on November 17 expanded the embargo to subject more chips and countries to licensing rules. Specifically, the servers contained some of Nvidia's most advanced chips, according to the previously unreported tenders fulfilled between November 20 and February. 28. While the US bars Nvidia and its partners from selling advanced chips to China, including via third parties, the sale and purchase of the chips are not illegal in China.

Read the full article here.

SECURITY VETTING PLAN FOR RESEARCHERS OF SENSITIVE TECHNOLOGIES

Chris Havergal | Times Higher Education | April 26, 2024

Academics with access to sensitive research in UK universities could be required to undergo security vetting, ministers have said. The proposal is one of several set to be consulted on after the director general of MI5 warned vice-chancellors that hostile states were targeting sensitive research being conducted in British higher education institutions "to deliver their own authoritarian, military and commercial priorities". Twenty-four vice-chancellors, including the heads of the universities of Oxford and Cambridge and Imperial College London, attended the briefing with MI5's Ken McCallum and Felicity Oswald, interim chief executive of the National Cyber Security Centre (NCSC). It was convened after Oliver Dowden, the deputy prime minister, said that foreign powers' access to sensitive research being conducted in UK universities could "become a chink in our armoury" in an era of heightened geopolitical tension, and warned that institutions' reliance on overseas funding raised the risk that they could be "influenced, exploited or even coerced".

Read the full article here.

UK GOVERNMENT CONSULTS ON PROTECTION MEASURES FOR UNIVERSITIES

Viggo Stacey | The Pie News | April 26, 2024

UK universities are well aware of the threats of malign actors and the current government approach to foreign interference has been "genuinely helpful" to mitigate further risk, the head of organisation representing over 140 universities has said. CEO of Universities UK, Vivienne Stern, was speaking following a meeting of vice chancellors from 24 universities with MI5 head Ken McCallum and National Cyber Security Centre chief Felicity Oswald this week. The UK government is beginning consultations on security with the higher education sector, which will focus on protecting sensitive research, intellectual property theft and dependency on foreign investment. Authorities are said to be looking into requiring key university personnel to undergo additional security clearance, seeking greater transparency about funding and its origins and enhancing security around research in universities.

Read the full article here.

WHY FAKE RESEARCH IS RAMPANT IN CHINA

The Economist | April 24, 2024

Huang Feiruo was once a respected scientist who studied ways to make pigs gain weight more quickly. He ran government-funded research projects at Huazhong Agricultural University in the central city of Wuhan. But last month 11 of his graduate students accused him of plagiarising the work of other academics and fabricating data. He had also, they said, put pressure on them to fake their own research. On February 6th the university announced that it had fired Mr. Huang and retracted some of his work. Scientific fraud is all too common in China. Bad incentives are a big part of the problem. Chinese universities typically reward researchers with promotions and funding based on the quantity of papers they publish, not the quality. That has got results. In 2017, for the first time, China published more scientific papers than any other country.

Read the full article here.

ALMOST EVERY CHINESE KEYBOARD APP HAS A SECURITY FLAW THAT REVEALS WHAT USERS TYPE

Zeyi Yang | MIT Technology Review | April 24, 2024

An encryption loophole in these apps leaves nearly a billion people vulnerable to eavesdropping. Almost all keyboard apps used by Chinese people around the world share a security loophole that makes it possible to spy on what users are typing. The vulnerability, which allows the keystroke data that these apps send to the cloud to be intercepted, has existed for years and could have been exploited by cybercriminals and state surveillance groups, according to researchers at the Citizen Lab, a technology and security research lab affiliated with the University of Toronto.

Read the full article here.

USEFUL RESOURCES

POLICY REGARDING USE OF COMMON DISCLOSURE FORMS FOR THE "BIOGRAPHICAL SKETCH" AND THE "CURRENT AND PENDING (OTHER) SUPPORT" SECTIONS OF APPLICATIONS BY FEDERAL RESEARCH FUNDING AGENCIES

Executive Office of the President of the United States | Office of Science and Technology Policy
February 14, 2024

This policy requires federal research funding agencies to use harmonized common disclosure forms for the Biographical Sketch and the Current and Pending (Other) Support portions of funding application packages for grants and cooperative agreements (i.e., the Common Forms), except as otherwise provided below. The National Science and Technology Council (NSTC) Research Security Subcommittee has worked to develop consistent disclosure requirements, as directed under section 4(b) of National Security Presidential Memorandum 33 (NSPM-33)1, including with resolution of comments submitted through the Paperwork Reduction Act (PRA) notice published in the Federal Register. The Common Forms also provide general standards for agencies to develop forms for use in their own research and development (R&D) programs.

Read the full article here.

DAVID ZWEIG SPEAKS ON THE WAR FOR CHINESE TALENT IN THE UNITED STATES

University of Southern California Annenberg | April 24, 2024

David Zweig is a renowned scholar who focused on China's efforts to build its talent. His insight into the War For Chinese Talent provides us with a different way to look at policy implications for Chinese scholars. Prof. Zweig draws on decades of research to document China's "over-the-top" effort to gain the help of immensely talented Chinese who were living and working in the US, as well as the US government's harsh counterattack, and its strategy to limit and disrupt the transfer of US technology to China. He offers case studies which include stories of several victims of that campaign whose cases were never made public. Zweig highlights the harm this war has done to Sino-American scientific collaboration and the education of Chinese students in America. Prof. Zweig's book on the talent war will be published this summer.

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute