ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

March 8, 2023

UNIVERSITIES 'MUST BALANCE OPENNESS WITH SECURITY'

Jenny Sinclair | Research Professional News | March 6, 2023

Universities are being caught in a "race" between powers for technological dominance, a national conference has heard. However, it is a "terrible message" to send to researchers that they should not work with others, particularly China, according to Catriona Jackson, chief executive of the vice-chancellors' group Universities Australia. She said that "if you can't see that we are in a period of extraordinary geopolitical flux, you are not looking very hard", and that the threats of foreign interference and cybercrime were being added to the threat of terrorism. But Australian universities "all work, and we have to work, across national boundaries…and we don't find them dangerous, threatening, alien and hostile". Speaking at Universities Australia's annual conference on 22 February, Jackson said that universities have to grapple with "how we continue that fundamental free and open exchange". The University Foreign Interference Taskforce, a collaboration between universities and government, is the main tool for that and has arisen in a period when national security forces are "terrifying" universities with the risks. "We have got a very, very delicate balance here," she said.

Read the full article here.

CHINA HAS A 'STUNNING LEAD' OVER THE US IN THE RESEARCH OF 37 OUT OF 44 CRITICAL AND EMERGING TECHNOLOGIES, NEW STUDY FINDS

Huileng Tan | Insider | March 3, 2023

China has a "stunning lead" ahead of the US in high-impact research across critical and emerging technologies, according to Canberra-based independent think tank Australian Strategic Policy Institute, or ASPI. The world's second-largest economy is leading the US in researching 37 out of 44 critical and emerging technologies across the defense, space, energy, and biotechnology sectors — including research of advanced aircraft engines, drones, and electric batteries — the ASPI said in its Thursday report. The US State Department partly funded the study. The ASPI found that for a few fields, all of the world's top 10 research institutions are in China, and they collectively generate nine times more high-impact research papers than the second-ranked country — which is the US in many cases. In particular, China has the edge in defense and space-related technologies, the ASPI said. "Western democracies are losing the global technological competition, including the race for scientific and research breakthroughs," the report, led by the institute's senior analyst Jamie Gaida, said.

Read the full article here.

REQUEST FOR INFORMATION; NSPM 33 RESEARCH SECURITY PROGRAMS STANDARD REQUIREMENT

Office of Science and Technology Policy (OSTP) | Federal Register | March 7, 2023

The Office of Science and Technology Policy (OSTP) requests comments from the public on draft Research Security Programs Standard Requirement developed in response to National Security Presidential Memorandum 33 on National Security Strategy for United States Government-Supported Research and Development (R&D). The draft Standard Requirement has been created by OSTP, together with Federal agencies and the Office of Management and Budget, to ensure that there is uniformity across Federal research agencies in implementing this requirement. Interested persons and organizations are invited to submit comments on or before 5 p.m. ET June 5, 2023.

Read the full article here.

DRAFT RESEARCH SECURITY PROGRAMS STANDARD REQUIREMENT

Prepared by the Interagency Working Group on Research Security Programs, Subcommittee on Research Security, National Science and Technology Council | Office of Science and Technology Policy | February 2023

After more than a year of productive partnership among Federal agencies, together with engagement with the external research community, the National Science and Technology Council of the Office of Science and Technology Policy (OSTP) released Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development, on January 4, 2022. NSPM-33 charges OSTP with "coordina[ting] activities to protect Federally funded R&D from foreign government interference, and outreach to the United States scientific and academic communities to enhance awareness of risks to research security and Federal Government actions to address these risks." A similar charge is captured in the National Defense Authorization Act of 2020.[1] The Guidance, called for by the Director of the Office of Science and Technology Policy, delivers on three key priorities, consistent with the values of the Biden-Harris Administration, in the areas of research security and integrity: (1) protecting America's security and openness; (2) being clear in our delivery of guidance and information to impacted communities, so that compliance with NSPM-33 is easy, straightforward, and minimally burdensome; and (3) ensuring that our policies do not fuel xenophobia or prejudice.

Read the full article here.

U.S. UNIVERSITIES EXIT ACADEMIC PARTNERSHIPS WITH RUSSIA OVER UKRAINE WAR

Susan Fourtané | Fierce Education | March 9, 2022

Following Massachusetts Institute of Technology (MIT) decision to end over a decade-long academic partnership with Russia, several colleges and universities have recently announced plans to cut ties with the country over military actions in Ukraine, with more expected to follow suit. In October 2011, MIT and the Russian government began a partnership which led to the creation of the Skolkovo Institute of Science and Technology in Moscow. The high-tech campus was a joint effort between MIT and Russia to "build a unique and pioneering academic center in Russia." MIT notified Skoltech it was terminating the collaboration with the graduate research Russian institution on February 25. MIT President L. Rafael Reif in agreement with senior leadership decided to end the collaboration "in light of the unacceptable military actions against Ukraine by the Russian government."

Read the full article here.

UNDERSTANDING CONNECTIONS BETWEEN CHINA AND U.S. ACADEMIA

Michael Lammbrau | Newsweek | March 3, 2023

Current concerns regarding China's influence and intellectual property theft related to U.S. academia, government, and industry have driven debate across the country. U.S. responses have varied, from the China Initiative (focused on Chinese influence in academia and industry) to broad-scale economic sanctions against the Chinese Communist Party (CCP). For stakeholders in academia, the risk of influence is high due to the connections to China through funding. A recent internal report by Internet 2.0 has revealed that the Chinese government has implemented a comprehensive strategy to infiltrate and influence U.S. academic institutions and technology research programs. It's important for stakeholders throughout academia to better understand the context of funding from China as well as the potential for threats on national security. Considering the recent focus on endowments and foreign funding, we analyzed data on foreign gifts and contracts from the People's Republic of China (PRC) reported to the U.S. Department of Education.

Read the full article here.

WHY CYBERATTACKS HIT HIGHER ED AND WHAT YOU CAN DO TO STOP THEM

Shannon Flynn | MUO (MakeUseOf) | March 3, 2023

If you've considered going to college, maybe you looked at available degree programs, a school's reputation, and the quality of its professors. Perhaps you also researched the chances of securing a job in your field after graduation. Those are all important, but there's another factor to add to the list—how seriously an institution treats cybersecurity. With thousands of students and staff, universities make for tantalizing targets. Administrators, educators, students, and staff members must work together to strengthen their school's defenses against cyberattacks. Let's consider why and what you can do to help. The higher education sector is a frequent cyberattack target. That's due to several factors, including the amount and type of sensitive information stored at educational institutions. A Check Point Research report revealed a 44% jump in cyberattacks against the education and research sectors in the first half of 2022 compared to all of 2021. That change represented 2,297 more attacks per week in the studied period.

Read the full article here.

CHINA LEADS US IN GLOBAL COMPETITION FOR KEY EMERGING TECHNOLOGY, STUDY SAYS

Kirsty Needham and Edmund Klamann | Reuters | March 1, 2023

China has a "stunning lead" in 37 out of 44 critical and emerging technologies as Western democracies lose a global competition for research output, a security think tank said on Thursday after tracking defence, space, energy and biotechnology. The Australian Strategic Policy Institute (ASPI) said its study showed that, in some fields, all of the world's top 10 research institutions are based in China. The study, funded by the United States State Department, found the United States was often second-ranked, although it led global research in high-performance computing, quantum computing, small satellites and vaccines. "Western democracies are losing the global technological competition, including the race for scientific and research breakthroughs," the report said, urging greater research investment by governments. China had established a "stunning lead in high-impact research" under government programs.

Read the full article here.

MIT TAKES STEPS TO STOP FOREIGN ESPIONAGE, BUT SOME FACULTY SAY IT GOES TOO FAR

Kirk Carapezza | GBH | March 1, 2023

MIT materials researcher Yoel Fink said he had never seen anything like it in his nearly 30 years as a scientist at one of the world's premiere engineering universities. In a small MIT conference room with the blackout shades pulled down, FBI agents told him and other researchers in the fall that rogue nations like China, Russia and India were sending secret agents to steal intellectual property from university labs and asked them to take steps to stop it, including vetting their staff. "I've never had a formal threat briefing by law enforcement here," Fink said, saying the experience left him shaken. "Law enforcement should come onto campus only when there is clear evidence of a crime." Campus administrators at MIT are following new national security guidelines first announced under Trump and enacted by the Biden administration that are supposed to protect research labs from spying and international espionage. At MIT, that has meant not only on-campus briefings by the FBI, but a new requirement asking professors who receive federal funding to sign a disclosure form certifying that their students are not participating in suspicious activities.

Read the full article here.

LEAKING CHIP SECRETS TO CHINA RESULTS IN JAIL TERMS FOR EX-SAMSUNG EMPLOYEES

Jiyoung Sohn | The Wall Street Journal | February 21, 2023

A court in South Korea found seven ex-employees of a Samsung Electronics Co. SSNHZ 0.00% increase; green up pointing triangle subsidiary guilty of illegally obtaining and transferring semiconductor-related technology to Chinese companies, a case that underscores the intensifying efforts countries are making to protect their chip technologies. Details of the accusations, which were released on Monday, emerged as the U.S. has pushed sweeping restrictions on exports of advanced chips and chip-making equipment to China to prevent American technology from advancing Beijing's military power. Countries have long treated semiconductors and companies integral to the global chip supply-chain as matters of national security, and the efforts have taken on greater significance as the U.S. pushes allies to join its effort. Allegations of theft involving major chip-industry players have also emerged in the Netherlands and Taiwan.

Read the full article here.

WAR IN UKRAINE PROMPTS SHIFTS IN THINKING ABOUT INTERNATIONAL COOPERATION IN SCIENCE

Goda Naujokaitytė | Science Business | March 2, 2023

A year ago, Russia's full-scale invasion of Ukraine redefined geopolitics in a shockwave that is still reverberating through the science world. The EU research community was quick to cut ties with Russia and lend Ukraine a helping hand – but now it is grappling with resulting instability and uncertainty as the war climbs into its second year. Lucian Brujan, programme director for international relations and science diplomacy at the German National Academy of Sciences Leopoldina, says it's too early to say what the long-term impact will be on research and innovation - and urges patience. "I think many in the community are waiting to see how the political problems will be solved and how this war will end; and after that, we'll need to have a discussion," Brujan says. "We have to be honest with ourselves in the scientific community. We are dealing with political and security uncertainty." But what is clear already is the shift in discourse on international cooperation.

Read the full article here.

U.S. VISA AND IMMIGRATION POLICY CHALLENGES: EXPLANATIONS FOR FACULTY PERCEPTIONS AND INTENT TO LEAVE

Mary K. Feeney, Heyjie Jung, Timothy P. Johnson, and Eric W. Welch | Research in Higher Education | Springer | March 6, 2023

United States (US) immigration policies have increasingly focused on national security resulting in universities experiencing declines in international student applications, constraints on international scholar employment, and complications facilitating international research collaborations. The COVID-19 pandemic brought additional travel restrictions, embassy closures, and health and safety concerns that exacerbated these challenges. Science mobility is critical for science education, training, competitiveness, and innovation. Using a representative sample of US and foreign-born scientists in three STEM fields, we explore how recent visa and immigration policies have shaped research collaborations, work with students and postdoctoral scholars, and intentions to leave.

Read the full article here.

NSA GIVES GUIDANCE ON WORKING REMOTELY AND SECURING HOME NETWORKS

Jillian Hamilton | ClearanceJobs | March 2, 2023

The National Security Agency (NSA) shared a guide for teleworkers on making sure your home network is secure. As cybersecurity experts, NSA is keenly aware of the dangers of the remote work life. While the NSA may not be looking to take advantage of remote work for their own staff, they are interested in making sure others stay safe out there. Their "Best Practices for Securing Your Home Network" Cybersecurity Information Sheet (CSI) is aimed at helping teleworkers to protect their home networks from malicious cyber actors. That's something that LastPass wishes they had followed. Want to be remote? Reduce risk. NSA Cybersecurity, Technical Director, Neal Ziring, shares, "In the age of telework, your home network can be used as an access point for nation-state actors and cybercriminals to steal sensitive information.

Read the full article here.

BEST PRACTICES FOR SECURING YOUR HOME NETWORK

National Security Agency | February 2023

Don't be a victim! Malicious cyber actors may leverage your home network to gain access to personal, private, and confidential information. Help protect yourself, your family, and your work by practicing cybersecurity-aware behaviors, observing some basic configuration guidelines, and implementing the following mitigations on your home network, including: Upgrade and update all equipment and software regularly, including routing devices; Exercise secure habits by backing up your data and disconnecting devices when connections are not needed; Limit administration to the internal network only. Electronic computing devices, including computers, laptops, printers, mobile phones, tablets, security cameras, home appliances, cars, and other "Internet of Things" (IoT) devices must all be secured to reduce the risk of compromise.

Read the full article here.