ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

October 20, 2021

HOW CHINA IS PLANNING FOR A TECH DECOUPLING

Alex Stone and Peter W. Singer | Defense One | October 12, 2021

Rising tensions between the U.S. and China and the recognition of a new kind of race for technological advantage has led Washington to tighten restrictions on Chinese companies' access to critical technologies and to reevaluate the China-U.S. STEM talent pipeline. China is responding with preparations for a lengthy tech competition and decoupling. A notable set of recommendations by Chinese military strategists sheds light on possible policy countermoves. In July 2021, three PLA analysts presented a research brief that analyzes over 450 policy reports and documents published in the past four years by the U.S. government and the broader policy community and then suggested ways China might respond. The report's authors say they are affiliated with the "National Innovation Research Institute." But the lead author, Maj. Gen. Lu Zhoulai, was in 2018 identified as the political commissar of the National Defense S&T Innovation Institute of the Academy of Military Sciences of the People's Liberation Army. This academy is the Chinese Communist Party's top military research institute; it is believed to formulate "military theory"—doctrine—for the PLA.

Read the full article here.

AAMC SUBMITS JOINT LETTER TO WHITE HOUSE OSTP ON RESEARCH SECURITY

Anurupa Dev and Heather Pierce | Association of American Medical Colleges | October 15, 2021

The AAMC sent a joint letter on Sept. 30 in response to a request for feedback from White House Office of Science and Technology Policy (OSTP) Director Eric Lander, PhD, on implementing the research security guidelines in National Security Presidential Memorandum 33 (NSPM-33). This letter was also signed by the American Council on Education, the Association of American Universities, the Association of Public and Land-grant Universities, and the Council on Governmental Relations. In the letter, the associations stressed the need to safeguard the integrity of federally funded research while also maintaining meaningful international scientific collaboration. The letter provided several recommendations for the OSTP as it implements NSPM-33 and moves to standardize and coordinate federal research security policies. These recommendations included: Building on existing policies created by institutions to address research security, recognizing that the vast majority of university research is open and unrestricted and should not be subject to research standards from the commercial sector, and incorporating the use of pilot programs and continued community engagement as any new policies are implemented.

Read the full article here.

THE ARCHITECTURE OF REPRESSION, UNPACKING XINJIANG'S GOVERNANCE

Vicky Xu, Dr. James Leibold, and Daria Impiombato | Australian Strategic Policy Institute
October 19, 2021

Since the mass internment of Uyghurs and other indigenous groups1 in China was first reported in 2017, there is now a rich body of literature documenting recent human rights abuses in the Xinjiang Uyghur Autonomous Region. However, there is little knowledge of the actual perpetrators inside China's vast and opaque party-state system, and responsibility is often broadly attributed to the Chinese Communist Party, Xinjiang Party Secretary Chen Quanguo, or President Xi Jinping himself. For accountability, it is necessary to investigate how China's campaign against the Uyghurs has been implemented and which offices and individuals have played a leading part. The current knowledge gap has exposed international companies and organisations to inadvertent engagement with Chinese officials who have facilitated the atrocities in Xinjiang. It has also prevented foreign governments from making targeted policy responses.

Read the full article here.

SURVEILLANCE AND PRIVACY SCHOLARS: FOUR THINGS THE GOVERNMENT NEEDS FROM YOU

Adam Klein | Just Security | October 13, 2021

Does government need academia? Do theories matter in the pragmatic, day-to-day grind of national-security policymaking? I think they do. Academics and other independent analysts have advantages that policymakers often lack. These include critical distance and the broader perspective it provides; deeper grounding in theory and conceptual frameworks; and the luxury of time to think about tomorrow's problems and opportunities, not just today's. During my tenure as Chairman of the Privacy and Civil Liberties Oversight Board, my colleagues and I benefited greatly from the contributions of outside experts: think-tank researchers, professors, technologists, legal scholars, civil-society groups, and former officials. Some topics that we reviewed had been well covered by researchers. Surveillance experts have for years debated issues surrounding Sections 702 and 215, two of the main authorities at issue in Snowden leaks.

Read the full article here.

QUANTUM WORKFORCE – NSTC REPORT HIGHLIGHTS NEED FOR INTERNATIONAL TALENT

John Russell | HPCwire | October 13, 2021

Attracting and training the needed quantum workforce to fuel the ongoing quantum information sciences (QIS) revolution is a hot topic these days. Last week, the U.S. National Science and Technology Council issued a report – *The Role of International Talent in Quantum Information Science* – which noted, among other things, there simply isn't enough domestic talent to fill the QIS workforce needs and foreign-born talent will be required. The NSTC report noted that over the last decade, VC funding has "invested more than $2.5 billion USD in over 100 quantum-related startups, and the U.S. Quantum Economic Development Consortium (QED-C) now has a membership of over 160 U.S. companies, universities, and non-profits. Many QED-C members have international offices or employ foreign nationals, and their success is dependent on a competitive and fair global market." While those statistics paint a robust picture of a young industry about to mushroom in size, they also spotlight how important developing an adequate workforce – size and skillsets – will be.

Read the full article here.

FEDERAL RESEARCH: AGENCY ACTIONS NEEDED TO ADDRESS FOREIGN INFLUENCE

United States Government Accountability Office | October 5, 2021

The federal government reported expending about $44.5 billion on university science and engineering research in fiscal year 2019. To protect U.S. investments in scientific research from undue foreign influence, federal agencies should have conflict of interest (COI) policies and require researchers to disclose foreign interests. The Government Accountability Office (GAO) has testified that the National Science Foundation (NSF) has an agency-wide financial conflict of interest policy, but it doesn't define non-financial conflicts (e.g., for researchers with multiple professional appointments). The policy does require researchers to disclose some non-financial interests in grant proposals—like foreign-provided lab space. In a December 2020 report, GAO reviewed five agencies, including NSF, which together accounted for almost 90 percent of all federal research and development expenditures at universities in fiscal year 2018. GAO found that three of the agencies it reviewed have agency-wide COI policies and two do not. The three agencies with existing COI policies focus on financial interests and do not specifically address or define non-financial interests, which may include multiple professional appointments.

Read the full article here.

U.S. RESEARCH AND DEVELOPMENT FUNDING AND PERFORMANCE: FACT SHEET

John F. Sargent Jr. | Congressional Research Service | October 4, 2021

Research and development (R&D) in the United States is funded and performed by a number of sectors—including the federal government, state governments, businesses, academia, and nonprofit organizations—for a variety of purposes. This fact sheet begins by providing a profile of the U.S. R&D enterprise, including historical trends and current funding by sector and by whether the R&D is basic research, applied research, or development. The final section of this fact sheet includes data on R&D performance by sector. The United States became a global leader in R&D in the 20th century, funding as much as 69% of annual global R&D in the period following World War II. 1 Figure 1 shows the growth in total U.S. R&D expenditures from 1955 to 2019 in current dollars. 2 U.S. R&D in 2019 was 105 times higher than it was in 1955 in current dollars, and more than 13 times higher in constant dollars.3 By sector, business-funded R&D grew the most during this period.

Read the full article here.

FOREIGN INTERFERENCE ACT IS A RISK FOR ACADEMIC FREEDOM

Cherian George, Chong Ja Ian, Linda Lim and Teo You Yenn | University World News | October 5, 2021

The government has for decades proclaimed higher education and research as vital to Singapore's development as a knowledge economy. But its proposed Foreign Interference (Countermeasures) Act or FICA – without watertight assurances against overreach in the text of the law – could represent the single biggest threat to academia in Singapore and its chances of realising that vision. This is not because academia is full of the kinds of malign, clandestine foreign manipulation that any government has a responsibility to counteract. Rather, the bill casts a broad shadow over activities that academics consider not only legitimate but also necessary: activities involving cross-border collaboration, wide online dissemination and strong social impact. While academia is not the main target of FICA, in an environment already rampant with second-guessing by university administrators nervous about what might earn official displeasure, there is every chance that it will suffer collateral damage.

Read the full article here.

NATIONAL STRATEGIC OVERVIEW FOR RESEARCH AND DEVELOPMENT INFRASTRUCTURE

National Science and Technology Council | October 2021

Federal investments in world-class basic and applied research and development infrastructure (RDI) after World War II marked a new era for scientific and technological innovation in the United States. Federal investments in the Nation's RDIs have stimulated the development of transformative technologies, such as the internet and the Global Positioning System (GPS), leading to the creation of new industries and markets, including our aerospace and semiconductor industries. Over the past 75 years, our Nation's RDI investments have led to capabilities that have significantly increased human lifespans; eradicated smallpox and helped to control several widespread diseases; expanded understanding of the nature of matter at the nanoscale; and enabled exploration of our universe. The capabilities provided by our Nation's RDIs have historically bolstered America's leadership position in the global research and development (R&D) enterprise.

Read the full article here.

CURRENT US POLICY ON CHINA: THE RISK TO OPEN SCIENCE

Philip H. Bucksbaum, S. James Gates Jr., Robert Rosner, Frances Hellman, James Hollenhorst, Baha Balantekin, and Jonathan Bagger | American Physical Society | October 2021

We are writing to share with you our concerns about our federal government's current approach to research security. Free information exchange between research groups worldwide is essential for progress in science. Yet the US government is placing new restrictions on Chinese contact based on recent concerns that China is stealing knowledge and technology developed in US research labs. There are real threats to national security posed by unauthorized transfer of knowledge and technical expertise. But a response that chokes off legitimate scientific contacts only compounds the problem it seeks to solve. This will inevitably lead to the loss of US competitiveness and international prestige and threaten our future economic progress. A more effective approach to research security balances the responsibilities of the government and the scientists to address the problem. We scientists need to strengthen our partnership with the federal government to ensure that fundamental research remains open to all.

Read the full article here.

RESEARCH SECURITY POLICIES & THEIR IMPACTS: KEY RESULTS OF APS MEMBER SURVEY

American Physical Society | October 2021

New data from a September 2021 survey by the American Physical Society of more than 3,200 physics professionals and students shows that the US federal government's current approach to addressing research security concerns is weakening, not strengthening, the US scientific enterprise. The following survey results highlight the urgent need for a new approach that thoughtfully protects our nation against evident security risks, welcomes international talent and promotes beneficial international collaborations. Nearly one in five physics professionals in the United States (non-student APS members) have either chosen – or been directed – to withdraw from opportunities to engage in professional activities with colleagues based outside the United States due to current research security guidelines. More than 43% of international physics graduate students and early career scientists – i.e., PhD graduates with fewer than five years of experience – perceive that the United States is an unwelcoming country for international students and scholars.

Read the full article here.

CYBERSECURITY AWARENESS FRAMEWORK FOR ACADEMIA

Mohammed Khader, Marcel Karam, and Hanna Fares | MDPI | October 12, 2021

Cybersecurity is a multifaceted global phenomenon representing complex socio-technical challenges for governments and private sectors. With technology constantly evolving, the types and numbers of cyberattacks affect different users in different ways. The majority of recorded cyberattacks can be traced to human errors. Despite being both knowledge- and environment-dependent, studies show that increasing users' cybersecurity awareness is found to be one of the most effective protective approaches. However, the intangible nature, socio-technical dependencies, constant technological evolutions, and ambiguous impact make it challenging to offer comprehensive strategies for better communicating and combatting cyberattacks. Research in the industrial sector focused on creating institutional proprietary risk-aware cultures. In contrast, in academia, where cybersecurity awareness should be at the core of an academic institution's mission to ensure all graduates are equipped with the skills to combat cyberattacks, most of the research focused on understanding students' attitudes and behaviors after infusing cybersecurity awareness topics into some courses in a program.

Read the full article here.

GLOBAL RESEARCH AND DEVELOPMENT EXPENDITURES: FACT SHEET

John F. Sargent Jr. | Congressional Research Service | September 27, 2021

Research and development (R&D) plays a central role in advanced economies in areas such as economic growth and job creation, industrial competitiveness, national security, energy, agriculture, transportation, public health and well-being, environmental protection, and expanding the frontiers of human knowledge understanding. Accordingly, companies, governments, universities, nonprofit organizations, and others around the world have made substantial investments in R&D. Since 2000, total global R&D expenditures have more than tripled in current dollars, from $677 billion to $2.2 trillion in 2019. The United States emerged as a global leader in science and technology in the second half of the 20th century. During this period, U.S. public and private investments in R&D grew rapidly and helped to propel the United States to a position of global economic leadership. By 1960, the United States accounted for approximately 69% of the world's R&D funding. By 2019, however, the U.S. share of global R&D expenditures2 had fallen to about 30%.

Read the full article here.

SECURITY DEMANDS CHALLENGE AIR FORCE, DEFENSE CONTRACTOR COLLABORATION WITH ACADEMIA

Shaun Waterman | Air Force Magazine | September 27, 2021

Deeper partnerships outside the traditional defense industrial base are needed to help the Air Force deliver cutting-edge technology to the warfighter, but relationships with academia can be challenging, according to panelists at AFA's Air, Space, & Cyber Conference. Both the military services and the traditional defense contractors that serve them are going to have to learn to work with a much broader spectrum of partners if they are to "meet the requirements of the Air Force's core missions in fulfilling the interim national security strategy … in a very challenging budgetary environment," said Brig. Gen. Robert K. Lyman, the assistant deputy chief of staff for cyber effects operations, who moderated the conference's closing session. Partnerships with academia were among the issues at the forefront of panelists' concerns, highlighted by the rare presence of an academic among them.

Read the full article here.

TENSIONS SPIKE OVER NEW RESEARCH-SECURITY PROPOSALS TARGETING CHINA

Brendan Bordelon | Center for Security and Emerging Technology | September 16, 2021

In an era of escalating partisanship in Washington, the effort to boost American research institutions and beat China to key discoveries has proven a rare point of cooperation. But as the Biden administration and some lawmakers look to tighten rules governing collaborations between U.S. and Chinese researchers, cracks in that united front are starting to appear—and a fight over the future of the international R&D ecosystem may be on the horizon. “This is a new cold war, basically,” Texas GOP Rep. Brian Babin said at last week’s markup of the House Science Committee’s slice of the budget reconciliation bill. “We’re losing proprietary information, we’re losing valuable learning and research, to these people. They’re inside of our research facilities, they’re inside of our colleges and universities.” Babin was speaking in support of a GOP-led amendment to prohibit federal funds from being used to conduct research in China, or to support any research entity determined to be owned or controlled “directly or indirectly” by the Chinese government.

Read the full article here.

DEFINING ORGANISATIONAL INFORMATION SECURITY CULTURE—PERSPECTIVES FROM ACADEMIA AND INDUSTRY

Adéleda Veiga, Liudmila V. Astakhova, Adéle Botha, and Marlien Herselman | ScienceDirect | May 2020

The ideal or strong information security culture can aid in minimising the threat of humans to information protection and thereby aid in reducing data breaches or incidents in organisations. This research sets out to understand how information security culture is defined from an academic and industry perspective using a mixed-method approach. The definition, factors necessary to instil the ideal information security culture and the potential impact of the ideal information security culture were investigated from both perspectives. A survey approach was implemented to obtain the views from industry and 512 respondents from organisations, many of which operate at an international level, participated in the survey. The research presents a description of information security culture, integrating the existing literature and expanding on it with the views of industry, thereby giving clarity to the concept. The ideal information security culture was identified with the top traits relating to aspects such as an aware and knowledgeable workforce implementing conscientious, caring behaviour to comply with policies as guided by management.

Read the full article here.