RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE

THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary

July 3, 2024

GEOPOLITICAL TENSIONS DIM PROSPECTS FOR US-CHINA EXCHANGES

Yojana Sharma | University World News | June 28, 2024

Reports of Chinese students being turned back at United States airports despite having valid student visas, and recent remarks by senior US administration officials on the need to move away from over-reliance on Chinese researchers have signalled what some academics see as a "ratcheting up" of the science and technology rivalry between China and the US. Wider geopolitical tensions are leading to a cooling of academic and student exchanges between the two countries, which both sides have said they want to restore after they came to a virtual halt during the COVID-19 pandemic. In January this year *China Science Daily*, a newspaper run by the Chinese Academy of Sciences, posted on its WeChat blog a detailed story written by a fifth-year PhD student at Yale University writing under the pseudonym of Meng Fei who was detained by US customs at Washington Dulles Airport upon her return in December to further her research in cell biology. The blog described interrogations in what was referred to as "a little dark room" as well as body searches. The student said she was held for at least 12 hours in solitary confinement before being sent back to China and barred from entering the US for five years.

Read the full article here.

HUAWEI'S SECRET ALLY IN THE US-CHINA TECH WAR: A SCIENCE NONPROFIT BASED IN DC

Kate O'Keeffe | Bloomberg | June 25, 2024

When Optica Chief Executive Officer Elizabeth Rogan traveled to China in November, the prestigious US scientific society she runs promoted the trip internally and on social media. But it omitted a key stop: her visit to Huawei Technologies Co.'s headquarters, according to communications and documents reviewed by Bloomberg News. By April, Rogan's under-the-radar meetings at Huawei had become part of a whistleblower complaint about her nonprofit's growing partnership with a Chinese telecommunications giant that's in the crosshairs of US national-security officials. A review of internal Optica corporate records shows the alliance ran far deeper than publicly known, blossoming over decades even as US-China tensions over technology soared. The findings expand on a Bloomberg News report in May that Huawei was secretly sponsoring a research competition run by Optica's foundation. That arrangement enabled Huawei to fund millions of dollars worth of cutting-edge studies at US universities without their knowledge, including at schools that ban their researchers from taking Huawei money.

Read the full article here.

CHINA'S HACKING NETWORK: TALENT COMPETITIONS FUEL STATE ESPIONAGE

Val Dockrell | National Security News | June 18, 2024

China is recruiting talented citizens through local "hacking competitions" and weaponising their talents to attack Western governments, according to a report by ETH Zurich University's Centre for Security Studies. The revelation, coupled with recent admissions by Dutch officials about the wide scope of Chinese hacking efforts, has amplified fears about China's growing "hack-for-hire" programme. The report titled "From Vegas to Chengdu", uncovers a two part hacker system:

- **Competition Stars** – The elite teams and researchers who dominate prestigious competitions with their expertise in finding system weaknesses (vulnerabilities). They often target software used by Western governments and companies, including Apple, Android, and Microsoft.
- **Government-Contracted Hackers** – Operating under the radar, these private contracted hackers do not compete publicly. Instead, they focus on exploiting weaknesses uncovered by the "stars" to conduct cyber espionage and steal intellectual property. The competition hackers also start businesses that develop security tools, which can then be used by the contracted hackers to complete their mission faster.

Read the full article here.

DEPARTMENT OF DEFENSE CONRACTORS AND EFFORTS TO MITIGATE FOREIGN INFLUENCE

Congressional Research Service | June 24, 2024

Some U.S. firms, including some Department of Defense (DOD) contractors, receive foreign investment or have other ties to foreign entities, including foreign firms and foreign governments. Some DOD contractors' foreign connections could include connections such as ownership, investment, supplier or producer relationships, or production overseas. These ties may pose a risk to U.S. national security, especially when firms performing work of a sensitive or classified nature have relationships with adversarial countries. DOD's Defense Counterintelligence and Security Agency (DCSA) is responsible for mitigating potential risks that may arise from foreign investment or foreign ties to DOD contractors. Foreign Ownership, Control, or Influence (FOCI) is a term that DOD uses to describe a condition in which a U.S. entity's foreign connections are believed to pose a risk of compromise of or unauthorized access to classified U.S. national security information.

Read the full article here.

NEW INTERNATIONALISATION STRATEGY AIMS TO BUILD RESILIENCE

Michael Gardner | University World News | June 27, 2024

Germany's federal and state governments have presented a new internationalisation strategy to strengthen the country's universities and make them more resilient in times of new technological and political developments as well as rising global risks. The strategy, announced by the *Kultusministerkonferenz* (KMK – Conference of State Ministers of Cultural Affairs) and supported by the federal government, comprises four fields of activity. It centres on universities as drivers of international mobility, improving the legal and structural framework of higher education, viewing international cooperation in a global context and benefiting from digital transformation.

Read the full article here.

SECURING KNOWLEDGE, PROTECTING VALUES IN A PERILOUS WORLD

Mihone Kerolli, Paulina Polko and Vilius Sadauskas | University World News | June 17, 2024

The world is entering a new era of uncertainty with an unprecedented series of threats, risks and challenges that are hard to predict. Security concerns have become a predominant factor, determining daily life in societies at large and at all levels. Health and climate threats are compounded by the risk and reality of armed conflict across the globe. Universities and their networks are increasingly aware that security issues are an integral part of academia, be they aggressive behaviour by individuals, cyberattacks or outright war. Security challenges may also concern soft aspects, such as the cross-cultural diversity of academic society, which might cause tensions and conflicts that can easily turn into serious problems. Our experience shows that integrating a security component successfully into university missions requires the close involvement of a variety of stakeholders along the value chain: other educational providers, civil society, companies, public authorities, the health sector, the police and even the military

Read the full article here.

HICKS ESTABLISHES SBIR/STTR DUE DILIGENCE POLICY AND IMPLEMENTION GUIDANCE

U.S. Department of Defense | May 23, 2024

Deputy Secretary of Defense Kathleen Hicks signed a memorandum to establish policy and provide implementation guidance for the Defense Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) Due Diligence Program May 13. In accordance with the SBIR and STTR Extension Act of 2022, the goal of the Due Diligence Program is to mitigate security risks when small business concerns (SBCs) with ties from any foreign country of concern seek SBIR/STTR funding. Under Department of Defense policy, the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) ensures consistent application of common minimum standards across all DoD services and components making SBIR/STTR awards to small businesses. The Defense SBIR/STTR Program, oversees DoD services' and components' establishment and implementation of their SBIR/STTR Due Diligence Programs. "We value the innovations and technologies derived from SBCs that enhance warfighter capabilities to support the DoD mission," said Gina Sims, Defense SBIR/STTR Program director.

Read the full article here.

NIST SEEKS PUBLIC INPUT ON DRAFT ROADMA FOR USG NATIONAL STANDARDS STRATEGY FOR CET

National Institute of Standards and Technology (NIST) | June 26, 2024

In response to the stakeholder feedback received, United States Government (USG) departments and agencies worked to generate a draft Implementation Roadmap. The roadmap sets forth actions and outcomes for the USG to increase investment in pre-standards development activities for critical and emerging technologies (CETs), broaden CET standards participation, grow a CET standards-savvy workforce, and ensure inclusivity and integrity in developing CET standards. The Implementation Roadmap is intended to guide USG actions. Actual implementation of the roadmap will require extensive coordination and engagement with variety of stakeholders. NIST requests public review and comment to further support the development and application of the USG NSSCET Implementation Roadmap.

Read the full article here.

THE TIK TOK DEBACLE: DISTINGUISHING BETWEEN FOREIGN INFLUENCE AND INTERFERENCE

Diana Fu and Emile Dirks | Brookings | June 24, 2024

Washington is afraid of TikTok. More precisely, it is afraid of Beijing's influence over TikTok via the platform's China-based parent company ByteDance. Critics allege TikTok, where a third of U.S. adults under 30 get their news, is used to "silence free speech," "undermine democracy," and "promote propaganda." Through China's National Intelligence Law, ByteDance could gain access to the personal data of its 170 million U.S. users. These fears drove President Joe Biden to sign into law a bill forcing TikTok to find a new owner in one year or be banned in the United States. TikTok has attempted to rebut these accusations by storing U.S. user data on American soil through "Project Texas" and limiting the reach of Chinese state-backed accounts. However, the company has been forced to contend with its own record. Interviews with TikTok employees indicate the company is ultimately "answerable to ByteDance rather than its international leadership." TikTok has misrepresented the work of researchers at the Citizen Lab to downplay privacy concerns about the app. Chinese engineers have reportedly accessed U.S. user data, despite TikTok's claims to the contrary.

Read the full article here.

BIDEN ADMINISTRATION BANS KASPERSKY SOFTWARE OVER SECURITY CONCERNS

Vikki Davies | MES Computing | June 21, 2024

The Biden administration has announced plans to prohibit the sale of Kaspersky Lab's antivirus software in the U.S. The significant move to bolster national security, it said, highlights concern over potential Russian government influence on the company, which could lead to cybersecurity vulnerabilities. Commerce secretary Gina Raimondo highlighted the heightened security risks posed by Kaspersky software, which has deep access to users' computer systems. This access could be exploited to steal sensitive information, install malware, or withhold critical updates. These concerns are particularly acute given that Kaspersky's customer base includes critical infrastructure providers and various state and local government entities. "Russia has shown it has the capacity and the intent to exploit Russian companies like Kaspersky to collect and weaponize the personal information of Americans and that is why we are compelled to take the action that we are taking today," Raimondo stated during a briefing with reporters.

Read the full article here.

USEFUL RESOURCES

CHINA REGIONAL SNAPSHOT: EXPOSING THE CCP'S MALIGN INFLUENCE

House Foreign Affairs Committee Republicans

An in-depth assessment led by House Foreign Affairs Committee Lead Republican Michael McCaul (TX-10), found that global investment and commercial efforts by the People's Republic of China (PRC), mainly through its predatory Belt and Road Initiative (BRI), are negatively affecting many countries and their citizens around the world. Launched by the Secretary General of the Chinese Communist Party (CCP) Xi Jinping in 2013, the BRI is falsely presented as a global development and investment initiative. In reality, it is an effort to expand the CCP's heavy-handed influence around the world while also laying the groundwork for their global military power projection. In the process of expanding their control, the CCP is creating economic dependencies via their familiar "debt trap" diplomacy. They are also creating technological dependencies around the world by exporting intrusive and dangerous technology.

View the full resource here.

SAFEGUARDING OUR MILITARY EXPERTISE

DNI

THREAT: China's (PRC) People's Liberation Army (PLA) continues to target current and former military personnel from North Atlantic Treaty Organization (NATO) nations and other Western countries to help bolster the PLA's capabilities. The PLA is using private companies in South Africa and China to hire former fighter pilots from Canada, France, Germany, the United Kingdom, Australia, the United States, and other Western nations to train PLA Air Force and Navy aviators. The PLA wants the skills and expertise of these individuals to make its own military air operations more capable while gaining insight into Western air tactics, techniques, and procedures. The insight the PLA gains from Western military talent threatens the safety of the targeted recruits, their fellow service members, and U.S. and allied security.

View the full resource here.

ENHANCING THE SECURITY AND INTEGRITY OF AMERICA'S RESEARCH ENTERPRISE

The White House Office of Science and Technology Policy-Trump Whitehouse Archives

Clarivate Plc (NYSE:CLVT), a leading global provider of transformative intelligence, today released the 2024 update to the Journal Citation Reports™ (JCR™). The reports provide an essential and comprehensive resource of high-quality journals, ranked by field to enable academic institutions, researchers and publishers to gauge the significance of journals in the global research landscape. Changes to journal rankings include the addition of the Emerging Sources Citation Index. Only journals that have met the rigorous quality standards for inclusion in the Web of Science Core Collection™ are featured within the Journal Citation Reports, to ensure that users can confidently rely on the information and descriptive data provided.

View the full resource here.

VIDEO: THE STATE OF THE SCIENCE ADDRESS

National Academies | June 25, 2024

The first State of the Science address will explore how U.S. science and innovation are positioned to respond to rising global competition and shifting priorities for the nation's economy, security, public health, and well-being. The event is intended to bring together leaders in science and research, technology and innovation, policymaking, government, industry, and philanthropy to explore what actions may be needed to chart a course toward a more nimble, more robust U.S. science and technology enterprise that is ready to meet the nation's current challenges and make vital advances in the future.

View the full resource here.

UPCOMING RESEARCH SECURITY EVENTS

PUBLIC SAFETY CANADA RESEARCH SECURITY WEBINAR: MODULE 1 - SAFEGUARDING SCIENCE (JULY)

Safeguarding Science: Raising awareness of security risks and mitigation tools in the research ecosystem

The purpose of the Safeguarding Science workshop is to raise awareness within Canada's scientific and academic communities about research security-related issues. The primary objective of this workshop is to explain the potential for misuse of dual-use research, technology and materials, along with possible risk indicators and mitigation tools to protect Canadian research assets.

- July 9, 2024
- Online Event

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute