RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE
THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary

October 24, 2024

ACHIEVING RESEARCH SECURITY WHILE PURSUING SCIENCE DIPLOMACY: CONSIDERING INTENTIONALITY

Jonathan Dawes, Karen Salt, and Christopher Smith | AAAS Science & Diplomacy | October 17, 2024

In the context of the search for national strategic advantage, "research security" is a broad term that describes the protection of intellectual property, sensitive research, people, and infrastructure from potential theft, misuse, and exploitation. Given its protectionist nature, is research security purely a constraint that inhibits science diplomacy, particularly the facilitation of international science cooperation ("diplomacy for science") and the use of science cooperation to improve international relations between countries ("science for diplomacy")? Or is it an enabling force that clarifies how science diplomacy works and why it is important? We outline an approach ("security by intentionality") that embeds the latter in a world fifteen years on from New Frontiers.[1] At the height of the Cold War, a five-fold controls system (information classification, export controls, terms and conditions for public funders, voluntary restrictions on the private sector, and controls on visitors and visas) was set out to describe the tools deployed to achieve security in the context of open fundamental research.[2] It still holds today. But a new approach to research security is needed: one that emerges from considering issues of intentionality.

Read the full article here.

PF 2025-04 (FAL 2025-02) RESEARCH SECURITY TRAINING REQUIREMENTS FOR ALL R&D FINANCIAL ASSISTANCE AWARDS

U.S. Department of Energy (Office of Management) | October 07, 2024

Provides information and guidance regarding the Department of Energy's (DOE's) implementation for research security training requirements for covered individuals listed on financial assistance applications and for the organizations applying for such an award, per Section 10634 of the CHIPS and Science Act. Attached for your information is guidance and implementation for Research Security Training Requirements for Research and Development in Financial Assistance.

Read the full article here.

EXCLUSIVE: ACT ON 'PROBLEMATIC' CHINESE ARCTIC RESEARCH, US OFFICIALS URGED

Didi Kirsten Tatlow | Newsweek | October 17, 2024

U.S. lawmakers from both sides of the aisle have asked the government to do more to address scientific research by China in the territory of America's Arctic allies that has potential military applications, Newsweek has learned. In a letter sent on Wednesday to Secretary of State Antony Blinken and Secretary of Defense Lloyd Austin, a bipartisan congressional committee said the People's Republic of China was seeking influence and access in the strategically important Arctic region, and that it was expanding its "dual-use"—mixed military and civilian—research, including in NATO allies Norway and Iceland, in ways that may challenge U.S. security. Newsweek reported in July that a Chinese institute in Svalbard archipelago in the Norwegian Arctic was carrying out potential dual-use research including in the areas of radar and missile tracking, that the institute was using a name that masked its role in China's military industry, and that it was undertaking classified research and working with the Chinese People's Liberation Army (PLA).

Read the full article here.

MAPPING CHINA-IN-GERMANY

Didi Kirsten Tatlow | SINOPSIS | October 02, 2019

"What else is there to say"? A decade after Xi Jinping's acerbic comment in Mexico, it turns out quite a lot. China may not be exporting revolution in the commonly-understood sense of the word, but it is exporting major change. Most visibly this is afoot via the geo-economic and strategic "Belt and Road Initiative", but also via a revival, since 2015, of the united front, a 100-year-old project launched by the Third Communist International in Europe in 1921 and later brought to China, where it went through several iterations. Potentially significantly, there are efforts underway to "sinify" the united front and justify it within the context of "traditional Chinese culture", even connecting it to the philosophical worldview of "tianxia 天下", or "all under heaven".[3]

Read the full article here.

FIVE WAYS STUDENT CAPS WILL DAMAGE NATIONAL SECURITY

Craig Jeffrey and Michael Wesley | FINANCIAL REVIW | October 16, 2024

The federal government's proposed caps on international student numbers are at odds with the needs of the economy. International education is one of Australia's top exports. At a time when the government is seeking to grow exports, drive Australia up the value chain, and remove impediments to trade, the caps would be deeply harmful. They could well plunge Australia into recession. It has been well documented that international education is Australia's biggest export outside of mining and agriculture. We've seen that these markets are particularly volatile, while China's economy is slowing and becoming less minerals-dependent. Since these debates started in mid-winter, iron ore prices have plummeted. The planet's transition to renewable energy doesn't chart a growth trajectory for our coal exports, either.

Read the full article here.

HOW TO FIGHT BACK AGAINST CHINA CORPORATE ESPIONAGE

Dan Harris | Harris Sliwoski | October 16, 2024

Reports of intellectual property (IP) theft and corporate espionage involving China are nothing new. For those familiar with China's business practices, these stories come as no surprise. However, recent insights from U.S. intelligence highlight how China's tactics are evolving, creating new challenges for foreign companies. To nobody's surprise, Michael C. Casey, Director of the National Counterintelligence and Security Center, recently warned that China remains the most prolific threat actor in corporate espionage. Casey emphasized that China's strategy goes beyond high-tech hacking, increasingly relying on "human assets"—employees recruited to steal data, trade secrets, or proprietary information This updated playbook builds on long-standing patterns: insiders are key to IP theft. Casey stressed that targeting employees with financial or personal difficulties has become a primary tactic. While media often focuses on high-tech cyberattacks, the most common form of IP theft remains low-tech—perpetrated by trusted insiders. Firewalls and cybersecurity systems are necessary but won't prevent insiders from downloading sensitive information and sharing it with competitors.

Read the full article here.

RANSOMWARE ATTACK ON UNIVERSITÉ PARIS-SACLAY IMPACTED SERVERS AND DIGITAL SERVICES

TEISS | October 11, 2024

Located in the south of Paris, Université Paris-Saclay runs a network of five faculties, three university technical institutes, five schools, two associate member universities and seven national research organisations. The university has about 50,000 students, over 8,000 researchers and academic staff and a network of 220 laboratories. In a data security incident notice posted on its website on 10th October, the leading French educational institution said that on August 11, it was a victim of a significant cyber attack that affected its entire internal network. "A number of services such as the intranet and certain business applications were unavailable. Since that date, the teams of the Information Systems Department (DSI), supported in particular by the National Agency for the Security of Information Systems (ANSSI), have been working to gradually restore these services," reads the notice.

Read the full article here.

CHINA SETS OUT ROADMAP TO BECOME 'LEADING EDUCATION POWER'

Amber Wang | University World News | October 8, 2024

China has set out a new action plan for educators in its bid to become a "leading education power", with universities set to play a more strategic role, according to the country's education minister who said the intention is to build China into an "important education centre with global influence". International exchanges and high level cooperation, including joint degree programmes, with leading international universities, especially in science and engineering, will be strengthened. Minister of Education Huai Jinpeng said, during a rare press conference in Beijing last month, that the education blueprint outlined by Chinese President Xi Jinping to be achieved by 2035 is "our grand goal and direction for the next 11 years", while acknowledging there were still "many difficulties and challenges" ahead. The government first said in 2010 the nation needed to grow from "a major power" to "a strong power" in education, as a 'precursor' to becoming a strong nation in all aspects.

Read the full article here.

DEBUNKING HYPE: CHINA HASN'T BROKEN MILITARY ENCRYPTION WITH QUANTUM

Craig Smith | Forbes | October 16, 2024

Recent headlines have proclaimed that Chinese scientists have hacked "military-grade encryption" using quantum computers, sparking concern and speculation about the future of cybersecurity. The claims, largely stemming from a recent South China Morning Post article about a Chinese academic paper published in May, was picked up by many more serious publications. However, a closer examination reveals that while Chinese researchers have made incremental advances in quantum computing, the news reports are a huge overstatement. "Factoring a 50-bit number using a hybrid quantum-classical approach is a far cry from breaking 'military-grade encryption'," said Dr. Erik Garcell, Head of Technical Marketing at Classiq, a quantum algorithm design company. While advancements have indeed been made, the progress represents incremental steps rather than a paradigm-shifting breakthrough that renders current cryptographic systems obsolete.

Read the full article here.

A US-CHINA SCIENCE PACT HAS EXPIRED AFTER 45 YEARS. HOW IS THE WORLD POORER FOR IT?

Lee Gim Siong | Chinese News Asia (CNA) | October 18, 2024

A scientific slowdown - not just between the United States and China, but the wider world - is on the cards, warn analysts, as the two superpowers let a landmark science and technology treaty slip away without renewal for the first time in 45 years. Climate research and public health are at particular risk from the recent expiry of the longstanding bilateral pact which yielded breakthroughs across the decades, experts note, potentially hurting the global fight against existential threats to humanity. "These areas rely heavily on international collaboration to address global challenges like climate change and pandemics," said Associate Professor Jonathan Ping from Bond University, who specialises in China studies. "The loss of joint efforts could slow progress in developing solutions and sharing critical data," he told CNA.

Read the full article here.

TOWARD A COHERENT FRAMEWORK FOR US-CHINA TECH COMPETITION IN THE GLOBAL SOUTH

Peter Engelke and Samantha Wong | Atlantic Council | October 18, 2024

The Atlantic Council's Scowcroft Center for Strategy and Security and the Global China Hub are embarking on a three-year project to assess the technological competition in the Global South between the United States, its allies and partners, and China. This memo is intended to provide strategists and policymakers in the United States and elsewhere with a coherent framework for understanding the nature of this competition with respect to the Global South and the stakes involved. Since 1945, the international system led by the United States and its allies and partners has generated widespread prosperity and economic development.[1] The rules-based international system that the United States and its allies and partners built during the postwar era created historic levels of global growth and equally historic reductions in poverty around the world.[2]

Read the full article here.

CHINA'S RISE IN RESEARCH PAPERS HAS AN UNFAIR 'HOME BIAS', SAY US, JAPAN STUDIES

Sandhya Ramesh | The Print | October 18, 2024

An upsurge in recent media coverage of China's ascent in research and academia has brought large attention to Chinese investment in different fields of science. As the country advances in domestic work, the influx of Chinese researchers into academia has had many Western scientists take notice China has been flexing its scientific muscles in recent years to beat the United States with the most number of cited papers in the world as well as the largest contributor to natural science research by 2022. But, according to some, this could be because of home bias and citation loop. Findings seem to indicate that Chinese researchers have a tendency to cite papers published within the country more than those published in English academic journals. At least two new papers, from the US and Japan, concluded that Chinese academia is rife with a "home bias" problem. The findings have raised "concerns" that it could skew global research rankings.

Read the full article here.

DEAR COLLEAGUE LETTER: MULTIFACTOR AUTHENTICATION IMPLEMENTATION FOR RESEARCH.GOV

Terry L. Carpenter | U.S. National Science Foundation | October 11, 2024

As part of our ongoing commitment to enhancing security and safeguarding NSF's IT systems, user accounts, personal and scientific data, and the integrity of the merit review process, effective on October 27, 2024, the U.S. National Science Foundation (NSF) is implementing multifactor authentication (MFA) for Research.gov. With the growing number of cyber threats, traditional password-only security is no longer sufficient. MFA provides an added layer of security and helps to ensure that only authorized users can access Federal resources online.

Read the full article here.

FUELING CHINA'S INNOVATION: THE CHINESE ACADEMY OF SCIENCES AND ITS ROLE IN THE PRC'S S&T ECOSYSTEM

Cole McFaul, Hanna Dohmen, Sam Bresnick, and Emily S. Weinstein | Center for Security and Emerging Technology | October 2024

The Chinese Academy of Sciences is among the most important S&T organizations in the world and plays a key role in advancing Beijing's S&T objectives. This report provides an in-depth look into the organization and its various functions within China's S&T ecosystem, including advancing S&T research, fostering the commercialization of critical and emerging technologies, and contributing to S&T policymaking.

Read the full article here.

USEFUL RESOURCES

PRODUCT SECURITY BAD PRACTICES

Cybersecurity and Infrastructure Security Agency | Federal Bureau of Investigation | October 2024

As outlined in CISA's Secure by Design initiative, software manufacturers should ensure that security is a core consideration from the onset of software development. This voluntary guidance provides an overview of product security bad practices that are deemed exceptionally risky, particularly for software manufacturers who produce software used in service of critical infrastructure or national critical functions (NCFs) and provides recommendations for software manufacturers to mitigate these risks. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) (hereafter referred to as the authoring organizations) developed this guidance to urge software manufacturers to reduce customer risk by prioritizing security throughout the product development process.

Read the full article here.

14 STEPS TO SAFEGUARD YOUR DIGITAL FOOTPRINT

Insider Threat Program | U.S. Department of State | October 2024

The Diplomatic Security Service manages/administers the Department of State's Insider Threat program to protect the department, its people, property, and information from threats within the department. The goal of the Insider Threat Program is to:

- Prevent the unauthorized disclosure of sensitive and classified material
- Eliminate workplace violence
- Identify employees on the critical path
-

View the full resource here.

NSA CYBERSECURITY COLLABORATION CENTER

National Security Agency/Central Security Service

The NSA Cybersecurity Collaboration Center (CCC) is how NSA scales intel-driven cybersecurity through open, collaborative partnerships. The CCC works with industry, interagency, and international partners to harden the U.S. Defense Industrial Base, operationalize NSA's unique insights on nation-state cyber threats, jointly create mitigations guidance for emerging activity and chronic cybersecurity challenges, and secure emerging technologies.

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute