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

Open Source Media Summary

September 12, 2024

RESPONSIBLE COLLABORATION THROUGH APPROPRIATE RESEARCH SECURITY

Tam K. Dao, Kenneth M. Evans, Michael D. Shannon, Christopher Bronk Claudia Neuhauser, and Evan Roberts | Rice University's Baker Institute for Public Policy | September 5, 2024

A topic largely forgotten after the Cold War, research security has reemerged as a top national security concern for academia and the government. The renewed attention on research security issues was brought into sharp, public focus in 2018, when the National Institutes of Health raised concerns about foreign governments using systematic programs to compromise the U.S. research ecosystem as part of the Department of Justice's China Initiative. Foreign covert programs aim to illegally acquire U.S. federally funded research, which is built on a tradition of openness, transparency, impartiality, respect, and fairness (Collins 2018). That research is the bedrock of the current and future U.S. economy in which a rules-based order protects against the theft of innovations produced by sponsored research. These concerns were addressed in new research security policies enacted under the United States Government- Supported Research and Development National Security Presidential Memorandum (NSPM-33) as well as the research security provisions of the Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act of 2022.

Read the full article here.

HOW (AND HOW MANY) WESTERN CHIPS ARE GETTING TO RUSSIA?

Max Kossek and Ian Stewart | TradeCompliace.io | August 26, 2024

Lagging domestic microelectronics production has forced Russia to continue to rely on foreign-sourced electronics for its weapon systems. This article examines where Russia imports these electronics from and how this has shifted since the February 2022 invasion of Ukraine. Hong Kong and China have become the main suppliers post-invasion, though the electronics are still predominantly Western-branded electronics. Sources differ over the scale of Russian imports. Several indicators point to the increasing cost and complexity of Russian procurement, demonstrating the effectiveness of sanctions and export controls. Since Russia's full-scale invasion of Ukraine in February 2022, the U.S. and its allies have imposed strict export controls, and a series of sanctions targeting sectors and entities involved in furthering Russia's military aims. The U.S., European Union, Japan, and United Kingdom have also jointly developed a Common High Priority List (CHPL) of Harmonized Digit (HS)—a classification system of descriptors used to signify different sorts of goods for customs purposes —codes that include items at a high risk of illegal diversion by Russia.

Read the full article here.

THE CITATION BLACK MARKET: SCHEMES SELLING FAKE REFERENCES ALARM SCIENTISTS

Dalmeet Singh Chawla | Nature | August 20, 2024

Research-integrity watchers are concerned about the growing ways in which scientists can fake or manipulate the citation counts of their studies. In recent months, increasingly bold practices have surfaced. One approach was revealed through a sting operation in which a group of researchers bought 50 citations to pad the Google Scholar profile of a fake scientist they had created.

Read the full article here.

SECURING INNOVATION IN AN EPOCH OF GEOPOLITICAL COMPETITION

Dr. Neil Ashdown and Natasha Buckley | The Royal United Services Institute for Defence and Security Studies (RUSI) | September 4, 2024

Amid great power competition over technology, states such as the UK are seeking to protect the ecosystems that drive innovation in a growing range of technologies. However, developing security capability and culture within organisations that are unfamiliar with national security concerns is challenging. The announcement of yet another strategic review – the third in just four years – presents an opportunity for the new government to outline a roadmap for securing the UK's innovation ecosystem, a crucial backbone of its economic and national security. The previous strategic reviews outlined the UK government's goal of becoming a technology superpower. Any advances in key areas of emerging and deep technology will undoubtedly require cultivating a thriving innovation ecosystem. This entails promoting research in a higher education sector that is experiencing profound financial challenges, supporting the commercialisation of research, and developing a more informed approach to industrial policy.

Read the full article here.

DEPARTMENT OF COMMERCE IMPLEMENTS CONTROLS ON QUANTUM COMPUTING AND OTHER ADVANCED TECHNOLOGIES ALONGSIDE INTERNATIONAL PARTNERS

The U.S. Commerce Department's Bureau of Industry and Security | September 5, 2024

The U.S. Commerce Department's Bureau of Industry and Security (BIS) published an interim final rule (IFR) today implementing controls on critical and emerging technologies that have reached broad technical agreement among our international partners. This IFR includes controls related to quantum computing, semiconductor manufacturing, and other advanced technologies. Today's action strengthens our international relationships with like-minded countries and ensures that U.S. export controls keep pace with rapidly advancing technologies that pose serious threats to our national security when in the wrong hands. "Today's action ensures our national export controls keep step with rapidly evolving technologies and are more effective when we work in concert with international partners," said Alan Estevez, Under Secretary for the Bureau of Industry and Security. "Aligning our controls on quantum and other advanced technologies makes it significantly more difficult for our adversaries to develop and deploy these technologies in ways that threaten our collective security."

Read the full article here.

CHINA DOMINATES AI AND ADVANCED ANALYTICS RESEARCH

Cliff Saran | ComputerWeekly.com | September 6, 2024

The Australian Strategic Policy Institute's (ASPI) latest technology tracker paints a bleak picture of the artificial intelligence (AI) and advanced analytics strengths of Western countries compared with China. Among the metrics the tracker published is a graph showing research papers published between 2019 and 2023, which it used to rank national research performance in advanced data analytics. When ASPI ranked countries based on their share of highly cited publications, it reported that China was first, with a 33.2% share. According to ASPI's research, China had over twice as many "highly cited publications" compared with the US (14.4%), which was second. The UK came in fourth place, with just 4%, behind India, with 5.4%. Between 2019 and 2023, China published the most research publications (8,672) on advanced analytics, while the number of papers for the US was 3,454, according to ASPI's research. The UK's volume of research publications placed it in seventh, with 719 research papers, behind Italy, with 771.

Read the full article here.

AUSTRALIAN LINKS REVEALED IN GLOBAL DEFENCE COMPANY SCANDAL INVOLVING CHINA, RUSSIA AND IRAN

Andrew Greene | The Australian Broadcasting Corporation (ABC) | September 7, 2024

An American weapons company made illegal technology transfers to Australia at the same time some of its staff members breached strict US regulations by taking their work laptops containing sensitive military secrets into Russia and Iran. Last week, defence giant RTX, formerly known as Raytheon, agreed to pay a $US200 million ($300 million) fine following 750 violations of the Arms Export Control Act and International Traffic in Arms Regulations (ITAR), including exchanging data and products with prohibited countries such as China. US State Department documents reveal several of the voluntarily declared breaches involved exports "without authorisation" of "classified defence articles" to Australia and other nations, related to military programs such as Tomahawk Cruise Missile and the RIM-162 Evolved SeaSparrow Missile. Other violations contained in the State Department's "Proposed Charging Letter" included "Unauthorised Exports Related to Sensitive Military Platforms Resulting from Misclassification" which were sent to Australia between 2017 and 2022.

Read the full article here.

STUDY FINDS HIGH PLAGIARISM LEVELS IN 'HIJACKED JOURNALS'

Wagdy Sawahel | University World News | August 30, 2024

The high percentage of plagiarism in papers submitted to 'hijacked journals', mostly by scholars from developing, emerging market or ex-Soviet countries, poses a threat to scientific integrity, according to recent research. Authored by Anna Abalkina at the Institute for East European Studies, Freie Universität Berlin in Germany, a study, published in Accountability in Research on 17 August, defines hijacked journals as "cloned websites of legitimate journals, imitating them by copying their titles and ISSN, aiming to deceive potential authors into submitting their work and paying publication fees". Abalkina told University World News hijacked journals pose a significant challenge to research integrity. "Unfortunately, it is very difficult to stop the fraudulent activity of hijacked journals, as they are registered anonymously, and anyone can create a website to clone a journal," Abalkina said. Once established, hijacked journals are also difficult to eliminate as they are indexed in Google Scholar and journal content is legitimised if it ends up in international citation databases.

Read the full article here.

CHINA IS BECOMING MUCH HARDER FOR WESTERN SCHOLARS TO STUDY

Chun Han Wong | PressReader | September 9, 2024

While China asserts a more muscular influence on global affairs, Western experts face growing constraints in their efforts to study the emerging superpower. Scholars researching everything from urban development to religious belief in China say they are running into barriers—many erected by Beijing but some arising at home—that increasingly hamper their work. A relentless tightening of political controls by Chinese leader Xi Jinping has curtailed access to even routine information and throttled research into topics that were once open. Interactions between people in China and foreigners are subject to intensifying state surveillance, stymying the flow of ideas. Those obstacles have led some China scholars to change their fields of study, or reprise research techniques developed during the Mao Zedong era, when the country was largely closed off to the rest of the world. A sharp rise in anti-China sentiment in the U.S. and other Western countries is compounding the difficulties, according to many scholars. Some say they fear being denigrated for their association with China.

Read the full article here.

CONGRESS TAKES UP A SERIES OF BILLS TARGETING CHINA, FROM DRONES TO DRUGS

Didi Tang | Yahoo News | September 8, 2024

How to curb and counter China's influence and power — through its biotech companies, drones and electric vehicles — will dominate the U.S. House's first week back from summer break, with lawmakers taking up a series of measures targeting Beijing. Washington views Beijing as its biggest geopolitical rival, and the legislation is touted as ensuring the U.S. prevails in the competition. Many of the bills scheduled for a vote this week appear to have both Republican and Democratic support, reflecting strong consensus that congressional actions are needed to counter China. The legislation "will take meaningful steps to counter the military, economic and ideological threat of the Chinese Communist Party," said Rep. John Moolenaar, chair of the House Select Committee on the Chinese Communist Party and a Michigan Republican. "There's a bipartisan goal to win this competition."

Read the full article here.

POSITION PAPER OF THE GERMAN FEDERAL MINISTRY OF EDUCATION AND RESEARCH ON RESEARCH SECURITY IN LIGHT OF THE ZEITENWENDE

The Federal Ministry of Education and Research (BMBF) | March 2024

We are experiencing a Zeitenwende (turning point in history) which is having a wide-ranging impact on our lives. The Russian war of aggression against Ukraine and its serious consequences play a substantial role in this. But our world was already undergoing radical change, with multipolarity, cyber threats and systemic rivalry, particularly with China, all on the rise. All this has significant consequences for science and research. The Federal Ministry of Education and Research (BMBF) responded to Russia's attack on Ukraine by suspending all ongoing and planned measures with Russia. At the same time, the BMBF is taking a more critical view of countries like China and Iran. The Zeitenwende requires a more strategic approach that dovetails the freedom of science that we cherish with our security policy interests.

Read the full article here.

THE HANDLING OF SECURITY-RELEVANT RESEARCH IN GERMANY — AN OVERVIEW

Leopoldina | September 8, 2024

What is security-relevant research?
Research freedom as protected by the German constitution gives researchers the right to address scientific questions independently and to discuss their work freely among themselves. Research freedom is fundamental to expanding human knowledge and ensuring social progress and prosperity. However, useful research findings and research methods can also be misused, for example for harmful military, political or criminal purposes. One example that illustrates this "dual-use dilemma" in research is the discovery of nuclear fission, which ultimately led to the development and use of nuclear weapons.

Read the full article here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute

USEFUL RESOURCES

RUSSIAN MILITARY CYBER ACTORS TARGET U.S. AND GLOBAL CRITICAL INFRASTRUCTURE

Joint Cybersecurity Advisory | September 5, 2024

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and National Security Agency (NSA) assess that cyber actors affiliated with the Russian General Staff Main Intelligence Directorate (GRU) 161st Specialist Training Center (Unit 29155) are responsible for computer network operations against global targets for the purposes of espionage, sabotage, and reputational harm since at least 2020. GRU Unit 29155 cyber actors began deploying the destructive WhisperGate malware against multiple Ukrainian victim organizations as early as January 13, 2022. These cyber actors are separate from other known and more established GRU-affiliated cyber groups, such as Unit 26165 and Unit 74455. To mitigate this malicious cyber activity, organizations should take the following actions today:

- Prioritize routine system updates and remediate known exploited vulnerabilities.
- Segment networks to prevent the spread of malicious activity.

View the full resource here.

AMENDMENT TO THE JULY 2021 BUSINESS ADVISORY ON RISKS AND CONSIDERATIONS FOR BUSINESSES OPERATING IN HONG KONG

The U.S. Department of State, the U.S. Department of the Treasury, the U.S. Department of Commerce, the U.S. Department of Agriculture, and the U.S. Department of Homeland Security | September 6, 2024

The U.S. Department of State, the U.S. Department of the Treasury, the U.S. Department of Commerce, the U.S. Department of Agriculture, and the U.S. Department of Homeland Security are issuing this amendment to the July 2021 Hong Kong Business Advisory to highlight new and heightened risks associated with actions undertaken by People's Republic of China (PRC) and Hong Kong Special Administrative Region (SAR) authorities. These risks could adversely affect U.S. companies that operate in the Hong Kong SAR of the PRC (Hong Kong). This amended advisory highlights the potential reputational, regulatory, financial, and, in certain instances, legal risks to U.S. companies operating in Hong Kong.

View the full resource here.

TRUSTED RESEARCH

National Protective Security Authority (NPSA)

The UK has a thriving research and innovation sector that attracts investment from across the world. Trusted Research is advice and guidance published jointly by NPSA and the NCSC which supports the integrity of the system of international research collaboration. Designed in partnership with the sector, it provides guidance to researchers, university staff and funding organisations to help keep sensitive research and intellectual property secure from theft, misuse or exploitation.

View the full resource here.

FURTHERING AMERICA'S RESEARCH ENTERPRISE

Committee on Assessing the Value of Research in Advancing National Goals; Division of Behavioral and Social Sciences and Education; and National Research Council | National Library of Medicine
October 28, 2014

Scientific research has enabled America to remain at the forefront of global competition for commercially viable technologies and other innovations. For more than 65 years, the United States has led the world in science and technology. Discoveries from scientific research have extended our understanding of the physical and natural world, the cosmos, society, and of humans—their minds, bodies, and economic and other social interactions. Through these discoveries, science has enabled longer and healthier lives, provided for a better-educated citizenry, enhanced the national economy, and strengthened America's position in the global economy. At a time of budget stringency, how can we foster scientific innovation to ensure America's unprecedented prosperity, security, and quality of life?

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute

UPCOMING RESEARCH SECURITY EVENTS

TECHNOLOGICAL COMPETITION BETWEEN CHINA AND THE U.S.: WASHINGTON SEMINAR SERIES 2024-2025

Join the MIT Club of Washington's 42nd annual Seminar Series on an important national topic related to science, technology, and public policy. Each year, the series offers engineers, scientists, industry leaders, policy makers and educators an opportunity to explore a specific topic in depth. Both those within and outside the Washington area MIT community gain the opportunity to develop a better understanding of recent developments and key issues.

View event details here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute