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

Open Source Media Summary
July 18, 2024

WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY RELEASES GUIDELINES FOR RESEARCH SECURITY PROGRAMS AT COVERED INSTITUTIONS

The White House | Office of Science and Technology Policy | July 9, 2024

Today, the White House Office of Science and Technology Policy issued guidelines to federal research agencies on research security programs at certain universities and federally-funded research institutions. To address risks posed by strategic competitors to the U.S. research and development (R&D) enterprise, the Biden-Harris Administration is implementing several measures to improve research security while preserving the openness that has long enabled U.S. R&D leadership and without exacerbating xenophobia, prejudice, or discrimination. This memorandum provides federal research agencies with guidelines for implementing a certification requirement imposed by National Security Presidential Memorandum-33 (NSPM-33) and certain provisions of the CHIPS and Science Act. Specifically, federal research agencies must require certain research institutions to certify to a federal funding agency that the institution has established and operates a research security program. This memorandum describes and sets forth a standardized requirement for fulfilling these obligations.

Read the full article here.

WHITE HOUSE REVAMPS GUIDELINES FOR RESEARCH SECURITY AT TOP UNIVERSITIES

Richard L. Hudson | Science/Business | July 11, 2024

In a push to tighten research security, the White House issued broad new guidelines for big American universities to track foreign travel by their researchers, provide regular security training, and toughen cybersecurity. The new policy will affect about 150 of the largest US universities, an official of the White House Office of Science and Technology Policy told *Science|Business*. The aim is to toughen safeguards against sensitive US research leaking to China, Russia or others. "This stems from a need to bolster our national security," the official said. The policy memo, by OSTP director Arati Prabhakar and addressed to US funding agencies, could be sweeping in its impact on big American research universities. But, say university officials who have been following it in the drafting phase over the past few years, the practical impact is hard to gauge. That's because it gives federal funding agencies and the universities wide latitude in exactly how they implement the policy, and it allows the universities to modify or expand their existing security measures rather than entirely reinvent them. "All of our members are affected," said Tobin Smith, senior vice president for government relations and public policy at the Association of American Universities, representing 69 of the leading US research universities.

Read the full article here.

WHITE HOUSE TO REQUIRE INCREASED CYBERSECURITY PROTOCOLS FOR R&D INSTITUTIONS

Caroline Nihill | FedScoop | July 11, 2024

Federal research agencies will now require certain covered institutions to implement cybersecurity programs for research and development security, a move the White House attributes to growing threats posed by the People's Republic of China. Office of Science and Technology Policy Director Arati Prabhakar made her case in the memorandum for increased awareness of security threats from adversaries. The guidance aims to enable national R&D enterprise research agencies and participants to "respond appropriately" through certifying that institutions' research security programs — and cybersecurity protocols — include foreign travel security, research security training and export control training. "Technology and R&D are central to this strategic competition, and the PRC has exploited international research collaboration by undermining values — such as transparency, accountability and reciprocity — in order to advance its strategic objectives and military modernization," the memo states.

Read the full article here.

MANAGEMENT ADVISORY: REVIEW OF DOD FUNDS PROVIDED TO THE PEOPLE'S REPUBLIC OF CHINA AND ASSOCIATED AFFILIATES FOR RESEARCH ACTIVITIES OR ANY FOREIGN COUNTRIES FOR THE ENHANCEMENT OF PATHOGENS OF PANDEMIC POTENTIAL (REPORT NO. DODIG-2024-099)

Department of Defense | Office of Inspector General | June 18, 2024

The purpose of this management advisory is to inform Congress and DoD leadership of the results of our review required in response to Public Law 118-31, "National Defense Authorization Act for Fiscal Year 2024," section 252, "Audit to Identify Diversion of Department of Defense Funding to China's Research Labs. Section 252 of the FY 2024 NDAA requires that the DoD Inspector General submit a report to the congressional defense committees within 180 days of December 22, 2023. The legislation requires a report on the amount of Federal funds awarded by the DoD, directly or indirectly, through grants, contracts, subgrants, subcontracts, or any other type of agreement or collaboration, to Chinese research labs or to fund research or experiments in China or other foreign countries that could have reasonably resulted in the enhancement of pathogens of pandemic potential, from 2014 through 2023.

Read the full article here.

PROTECTING CRITICAL SUPPLY CHAINS

Office of the Director of National Security and National Counterintelligence and Security Center

Public and private organizations must defend themselves from evolving—and increasingly sophisticated—cyber supply chains attacks. Foreign adversaries and non-state actors conduct campaigns that target supply chains—either directly or through proxy groups—to advance their global ambitions. These threat actors position themselves throughout the supply chain, fully aware that organizations trust and depend on this critical, complex, diverse, and distributed ecosystem. While the global supply chain saves money and accelerates innovation, it also exposes a multitude of vulnerabilities.

Read the full article here.

BLACKLISTED CHINESE COMPANIES REBRAND AS AMERICAN TO DODGE CRACKDOWN

Heather Somerville | The Wall Street Journal | May 28, 2024

In December, a new company registered in Michigan: American Lidar. Its planned home would be an easy drive from the big three U.S. automakers. The company behind American Lidar, and not mentioned in its registration, is China-based lidar maker Hesai Group, which the U.S. has labeled a security concern. It is a familiar playbook: a company facing regulatory or reputational problems sets up a subsidiary or affiliate with a different name. Chinese firms trying to buffer themselves from Washington's anti-China policies are rebranding and creating U.S.-domiciled businesses to sell their wares as the Biden administration expands the government entity lists that restrict Chinese companies' business dealings in the U.S., say policymakers and national-security experts. The blacklisting has also created opportunities for American entrepreneurs who want to work with Chinese companies that are popular with U.S. consumers. "Chinese firms take a blow but then adjust business strategy and are able to move in another direction," said Derek Scissors, a former commissioner on the U.S.-China Economic and Security Review Commission.

Read the full article here.

PEOPLE'S REPUBLIC OF CHINA (PRC) MINISTRY OF STATE SECURITY APT40 TRADECRAFT IN ACTION

America's Cyber Defense Agency | July 8, 2024

This advisory, authored by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), the United States Cybersecurity and Infrastructure Security Agency (CISA), the United States National Security Agency (NSA), the United States Federal Bureau of Investigation (FBI), the United Kingdom National Cyber Security Centre (NCSC-UK), the Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), the German Federal Intelligence Service (BND) and Federal Office for the Protection of the Constitution (BfV), the Republic of Korea's National Intelligence Service (NIS) and NIS' National Cyber Security Center, and Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and National Police Agency (NPA)—hereafter referred to as the "authoring agencies"—outlines a People's Republic of China (PRC) state-sponsored cyber group and their current threat to Australian networks. The advisory draws on the authoring agencies' shared understanding of the threat as well as ASD's ACSC incident response investigations.

Read the full article here.

TIKTOK OPERATIONS IN THE UNITED STATES UNVEILING STRATEGIC MOVES, SCIENTIFIC INSIGHTS AND WHAT LIES AHEAD

Ryan Clarke and LJ Eads | The CCP BioThreats Initiative (CCP BTI) | July 2024

On 24 April 2024 President Biden signed a Bill to force the divestment of ByteDance in TikTok's American legal entity. Biden and the Bill's many supporters cited national security concerns and accusations that TikTok is effectively an influence operations capability of the Chinese government. Current analysis on the nature of TikTok operations in the United States (and elsewhere) has focused heavily on comparative content analysis where content that is pushed to American users is compared to what content is pushed to Chinese users on domestic platforms such as Douyan (抖音). While comparative content analysis methods do have merit, there remains a substantial degree of subjectivity and a lack of consistent analytical techniques.

Read the full article here.

PEER REVIEW IS ESSENTIAL FOR SCIENCE. UNFORTUNATELY, IT'S BROKEN.

Paul Sutter | ARS Technica | July 12, 2024

Rescuing Science: Restoring Trust in an Age of Doubt was the most difficult book I've ever written. I'm a cosmologist—I study the origins, structure, and evolution of the Universe. I love science. I live and breathe science. If science were a breakfast cereal, I'd eat it every morning. And at the height of the COVID-19 pandemic, I watched in alarm as public trust in science disintegrated. But I don't know how to change people's minds. I don't know how to convince someone to trust science again. So as I started writing my book, I flipped the question around: is there anything we can do to make the institution of science more worthy of trust? The short answer is yes. The long answer takes an entire book. In the book, I explore several different sources of mistrust—the disincentives scientists face when they try to communicate with the public, the lack of long-term careers, the complicitness of scientists when their work is politicized, and much more—and offer proactive steps we can take to address these issues to rebuild trust.

Read the full article here.

STOP FEDERAL GRANTS FROM STRENGTHENING CHINA'S MILITARY

Marco Rubio | The National Interest | July 7, 2024

Last November, investigative reporters uncovered that the U.S. Department of Defense (DoD) had provided $30 million in artificial intelligence research grants to a Chinese scientist at the Beijing Institute of Technology, a university tasked with developing next-generation weapons for the People's Liberation Army. The news came as a shock to American policymakers and ordinary citizens alike. It was unthinkable that the U.S. government would fund our chief adversary's defense industrial base. I would like to say the story ends there. The reality, however, is that this scandal is just the tip of the iceberg. A new unclassified analysis provided to my office by the Naval Criminal Investigative Service (NCIS) reveals that U.S. taxpayers have been unwittingly funding thousands of Chinese experiments with direct applications to the Chinese military. Their findings note more than 5,000 instances of research collaboration between the DoD's funding agencies and Chinese entities between 2019 and 2024. These are not just any entities but groups closely linked to Beijing's ambitions to steal American technology and defeat the U.S. military in a potential conflict

Read the full article here.

WATCH OUT EUROPE: CHINA IS STEALING YOUR CHIP SECRETS

Ian O'Connor | The Center for European Policy Analysis (CEPA) | July 9, 2024

When Chinese state-affiliated hackers infiltrated Dutch semiconductor manufacturer NXP, they remained within NXP networks for more than two-and-a-half years, obtaining access to a large quantity of sensitive chip design data and research. It's far from an isolated incident. Ever since the semiconductor industry emerged in the 1950s, spies have attempted to steal trade secrets. The problem recently became acute, and China is the biggest culprit. Sanctioned by the West and eager to develop its own chip industry, Beijing has intensified its industrial espionage. ASML, the well-known Dutch semiconductor lithography firm, now faces "thousands of security incidents each year" with several successful Chinese infiltration attempts in the public record. Research champions such as Belgium-based imec are other prime Chinese targets. In recent years, Belgian authorities deported Chinese researchers at the institution suspected of spying. In response, the European Union is upping security.

Read the full article here.

CHINA'S GRAND STRATEGY FOR GLOBAL DATA DOMINANCE

Matthew Johnson | Hoover Institution | April 18, 2023

The United States and China are engaged in a global contest to shape how digitized information—data—will be distributed and controlled for the foreseeable future. For the Biden administration, the contours of this contest are only just becoming visible. While officials have addressed the importance of data in US-China competition, there is not yet a clear set of laws and policies that would support a strategy of protecting Americans' data from our biggest global rival. The opposite is true in Beijing, where Xi Jinping's Party-state is building a massive institutional architecture to draw more and more of the world's data resources toward China. This report, based on the Chinese Communist Party's own documents, dissects how the CCP has created a policy and regulatory architecture to maximally exploit data as the fundamental resource of the future global economy and governance system. It illustrates how People's Republic of China (PRC) technology companies that are now omnipresent in foreign markets are increasingly integrated with the Party's data storage and processing—and control and security—systems.

Read the full article here.

EUROPEAN RESEARCH COUNCIL HEAD PLEADS FOR OPENNESS AT G7 SCIENCE SUMMIT

David Matthews | Science/Business | July 11, 2024

The president of the European Research Council has pleaded with G7 science ministers not to strangle global cooperation by further tightening research security measures, as Western countries worry about leaking valuable knowledge to China and Russia. During a gathering in Italy this week, Maria Leptin told ministers that there would be "costs to applying restrictions" during a special closed-door discussion on research security and integrity. This year, Italy is hosting the G7's annual get-together. Science ministers and their equivalents from France, Italy, the UK, US, Germany, Japan and Canada – plus EU research commissioner Iliana Ivanova - met this week in Bologna to hash out a communique on future collaboration. The language is unsurprisingly diplomatic, and there are few concrete measures, but the communique gives some sense of the G7's top-level priorities over the next year.

Read the full article here.

SCIENCE AND SECURITY: SETTING THE DIRECTION FOR THE UK'S RESEARCH RELATIONSHIP WITH CHINA

Peter Carlyon | The Higher Education Policy Institute | June 27, 2022

Policy discussions of the UK's research relationship with China are dominated by security concerns. While the idea of decoupling from China appears to be gaining increasing traction, recent research by RAND Europe has highlighted that these partnerships contribute notably to the UK's academic excellence. UK-China collaboration can be mutually beneficial and crucial to tackling shared challenges. Rather than severing ties, many UK academics want to engage. For them to safely do so it is important that the UK provides clear guidance and develops a coherent overall China strategy. As both RAND Europe and HEPI have concluded, that will require substantially improving the level of China knowledge in the UK. Top of the list is research security – making sure rivals do not get their hands on the G7's most advanced knowhow. China is not named, but it is the G7's top scientific competitor and the chief target of new security measures.

Read the full article here.

A NEW WORLD FOR SCIENCE RESEARCH SECURITY

Alison Snyder | AXIOS | March 31, 2024

Countries around the world are debating and deploying new rules and tools to try to minimize the risks and maximize the benefits of increasingly global scientific research.
Why it matters: These policies will shape the course of science and the technologies it powers — as well as govern who collaborates with whom.
Driving the news: A new report commissioned by the National Science Foundation (NSF) urged the agency to "proceed with caution" before adding controls over fundamental science research.
Friction points: Many scientists argue an open research environment where results and hypotheses can be tested and exchanged is vital for science.

- Some security experts concerned about IP theft and foreign interference in research are calling for controls on access to scientific information or restricting collaborations in AI, aerospace, advanced materials and other fields.

Read the full article here.

REVERSE BRAIN DRAIN? EXPLORING TRENDS AMONG CHINESE SCIENTISTS IN THE U.S.

Stanford Center on China's Economy and Institutions | July 15, 2024

Along with native-born Chinese Americans, Chinese immigrants have become a large and visible demographic group in American science, technology, and engineering. However, the pressure of potential federal investigations since the 2018 launch of the "China Initiative" by the U.S. Department of Justice has provided scientists of Chinese descent in the U.S. with higher incentives to leave and lower incentives to apply for federal grants. What are the long-term consequences of the China Initiative on scientists of Chinese descent in the U.S. and the global leadership of the U.S. in science and technology? The data. Researchers utilized Microsoft Academic Graph to analyze trends in the migration of U.S.-based Chinese scientists. Microsoft Academic Graph is a comprehensive database that tracks over 200 million scientists from over 25,000 institutions authoring over 200 million scientific publications through 2021.

Read the full article here.

USEFUL RESOURCES

GUIDELINES FOR RESEARCH SECURITY PROGRAMS AT COVERED INSTITUTIONST

The White House | Office of Science and Technology Policy | July 9, 2024

To address risks posed by strategic competitors to the U.S. research and development (R&D) enterprise, the Biden-Harris Administration is implementing several measures to improve research security while preserving the openness that has long enabled U.S. R&D leadership throughout the world and without exacerbating xenophobia, prejudice, or discrimination. This memorandum provides federal research agencies with guidelines for implementing a certification requirement imposed by National Security Presidential Memorandum-33 (NSPM-33).

View the full resource here.

LIMIT YOUR DIGITAL FOOTPRINT

America's Cyber Defense Agency | July 1, 2024

Your activity on your device and applications (apps) generates data that tells a lot about your interests, associations, and pattern of life. Data brokers compile this data into user profiles that can be bought and sold by virtually anyone, meaning threat actors can use this information to develop a targeted cyber campaign. Disabling your advertising identifier (Ad ID) is one step that will help to minimize your digital footprint.

View the full resource here.

NSA JOINS IN RELEASING CASE STUDIES SHOWING PRC TRADECRAFT IN ACTION

National Security Agency/Central Security Service | Press Release | July 8, 2024

The National Security Agency (NSA) is joining the Australian Signals Directorate (ASD) and other agencies to publish a Cybersecurity Advisory (CSA) detailing the tradecraft used by a cyber actor group associated with the People's Republic of China (PRC) Ministry of State Security (MSS). "PRC MSS Tradecraft in Action" helps cybersecurity practitioners prevent, identify, and remediate intrusions against their own networks by sharing significant case studies of the adversary's tactics and techniques. The cyber actor group has targeted organizations in various countries, including the United States and Australia.

View the full resource here.