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

Open Source Media Summary

April 4, 2024

A NEW WORLD FOR SCIENCE RESEARCH SECURITY

Alison Snyder | Axios Science | 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.

CHINA'S AMBASSADOR TO THE UK TELLS ITS STUDENTS IN BRITAIN TO SERVE 'THE MOTHERLAND' AND UPHOLD TEACHINGS OF THE CHINESE COMMUNIST PARTY

Kumail Jaffer | Daily Mail | March 29, 2024

China's ambassador to the UK told students at British universities to serve 'the motherland' and uphold the teachings of the Chinese Communist Party, it has emerged. Zheng Zeguang was hosted by the Universities of York, Birmingham and Leeds last summer, and told Chinese students to 'keep in mind' the words of president Xi Jinping. It comes after the ambassador was summoned to the Foreign Office this week when it emerged Beijing had launched a cyber attack on MPs. Former Tory leader Sir Iain Duncan Smith said the events showed universities were 'in hock' to the communist state. He added: 'If the British Government… sent their ambassador around students in a foreign country to tell them that they should behave like British citizens, it would be considered quite peculiar.' The University of York, which has around 3,000 Chinese students, did not publicise Mr. Zheng's visit on its UK social media pages, the i-newspaper reported.

Read the full article here.

THE BIGGEST THREAT FROM CHINA IS RIGHT UNDER OUR NOSES — AND ON OUR SCREENS

Thomas P. Vartanian | The Hill | March 25, 2024

Millions of people anticipated a glimpse of Taylor Swift at this year's Super Bowl. That was likely millions more than noticed the stunning announcement by the government just four days earlier that Volt Typhoon — a conglomerate of cyber actors sponsored by the People's Republic of China — had pre-positioned itself inside American critical infrastructures in preparation for cyberwar. Intellectual theft, weather balloons, TikTok and now cyber war. What's left for China to do before someone in charge takes action? Like Taylor, technology tends to mesmerize and captivate us. Videos of gearheads unpackaging products and peeling plastic off screens in what resemble ritualistic ceremonies litter YouTube. Cryptocurrency computer codes invented by who-knows-who with no underlying value, backing or adult supervision intrigue us as they masquerade as the money of "the people." Tech applications like TikTok have a pollyannish, feel-good, video game aura that lulls us into thinking bad stuff really won't happen.

Read the full article here.

US, UK ACCUSE CHINA OF CYBERESPIONAGE THAT HIT MILLIONS OF PEOPLE

James Pearson, Raphael Satter and Christopher Bing | Reuters | March 25, 2024

U.S. and British officials on Monday filed charges, imposed sanctions, and accused Beijing of a sweeping cyberespionage campaign that allegedly hit millions of people including lawmakers, academics and journalists, and companies including defense contractors. Authorities on both sides of the Atlantic nicknamed the hacking group Advanced Persistent Threat 31 or "APT31", calling it an arm of China's Ministry of State Security. Officials reeled off a laundry list of targets: White House staffers, U.S. senators, British parliamentarians, and government officials across the world who criticized of Beijing. Few other victims were identified by name, but American officials said that the hackers' decade-plus spying spree compromised defense contractors, dissidents and a variety of U.S. companies, including American steel, energy, and apparel firms.

Read the full article here.

RISKS IN INTERNATIONAL RESEARCH RESEARCH COOPERATION

Alexander Plé, Michael Kunkis, and Bert Droste-Franke | Institute for Qualifying Innovation Research and Consulting GmbH German Aerospace Center | March 2024

This document deals with risks in international research cooperation and approaches for a possible risk management system. Chapter 1 deals with the definition of risk in general and of risks in international research cooperation and presents further basic terms and definitions. In order to gain an overview of possible types of risk, Chapter 2 identifies and defines various types of possible risks, provides examples and assigns them to different risk clusters. The resulting overview can help research institutions and public authorities to develop a more systematic understanding of the risks in research collaborations. It is shown how many different types of risks accompany individual collaborative situations and that the occurrence of one risk can often lead to the occurrence of further risks. When considering risks, longer periods of time must be taken into account in order to recognize the occurrence of systemic risks, which can result from the repeated occurrence of other risks.

Read the full article here.

CHINESE SPY OPS ATTACK 7 MSPS, FEDS ALLEGE

D. Howard Kass | MSSP Alert | March 28, 2024

Chinese state-backed operatives attacked and gained access to the networks of seven managed service providers (MSPs) in the U.S. and overseas as part of a 14-year global espionage campaign that included infiltration of the emails of U.S. legislators from more than 10 states. The unnamed MSPs include providers based in California, Colorado, Idaho, New York, Massachusetts and overseas, according to an unsealed indictment in U.S. District Court for the Eastern Division of New York filed in January 2024. Intrusions into the MSPs' networks took place between 2017 and 2019, according to court documents. Each of the seven defendants are charged with conspiracy to commit computer intrusions and wire fraud conspiracy, according to court documents. The federal court's charging affidavit reads, "Customers of managed service providers included corporations, non-government organizations and small and medium-sized businesses. By hacking these networks, the Conspirators gained access to the data belonging to customers of the breached managed service providers."

Read the full article here.

NEW STRATEGY WILL STREAMLINE DOD SUPPORT FOR DEFENSE CONTRACTORS' CYBERSECURITY

Sydney J. Freedberg | Breaking Defense | March 28, 2024

As defense contractors are battling ever more sophisticated cyber threats and baffled by ever-stricter security rules, the Pentagon today wants them to know: We hear you, and help is on the way, real soon now. That was the message around today's rollout of the new Defense Industrial Base (DIB) Cybersecurity Strategy for 2024-2027, [PDF] a three-year plan to strengthen, streamline and centralize Department of Defense support to contractors and small subcontractors. A long list of free, taxpayer-funded services is already available. But they're scattered across a multitude of different agencies, such as the DoD Chief Information Officer, the DoD Cyber Crime Center (aka DC3), the Defense Counterintelligence & Security Agency and even the mighty and mysterious National Security Agency. Those organizations don't always work that well together, let alone with their ostensible customers in the defense industrial base. Congress took notice and, starting in the National Defense Authorization Act for 2020, required the Pentagon to come up with "a consistent, comprehensive framework."

Read the full article here.

SCOOP: CONGRESS BANS STAFF USE OF MICROSOFT'S AI COPILOT

Andrew Solender and Ina Fried | Axios | March 29, 2024

The U.S. House has set a strict ban on congressional staffers' use of Microsoft Copilot, the company's AI-based chatbot, Axios has learned.

Why it matters: It's the latest example of the federal government trying to navigate its internal use of AI while simultaneously attempting to craft regulations for the burgeoning technology.

- The House last June restricted staffers' use of ChatGPT, allowing limited use of the paid subscription version while banning the free version.

Driving the news: The House's Chief Administrative Officer Catherine Szpindor, in guidance to congressional offices obtained by Axios, said Microsoft Copilot is "unauthorized for House use."

- "The Microsoft Copilot application has been deemed by the Office of Cybersecurity to be a risk to users due to the threat of leaking House data to non-House approved cloud services," it said.
-

Read the full article here.

TIKTOK: A THREAT TO US NATIONAL SECURITY

The Jamestown Foundation | March 26, 2024

TikTok is a powerful tool for manipulating mass sentiment in the hands of a company that actively cooperates with and is subject to the coercive power of the Chinese Communist Party (CCP). The CCP has the intent and capability to, as well as a history of, manipulating information on a mass scale. The Party's ability to leverage TikTok directly for its own ends distinguishes the platform from the platform's US-based social media rivals. TikTok and its parent company, ByteDance, have no practical means, legal or otherwise, to resist the CCP's pressure. Only solutions that separate the company from the CCP will protect US national security.

Read the full article here.

THE PENTAGON WANTS TO HELP BOOST CYBERSECURITY FOR SMALL CONTRACTORS

Lauren C. Williams | Defense One | March 28, 2024

The Pentagon is working on a shared virtual cloud-based workspace for contractors as a way to boost their cybersecurity and part of a larger strategic effort to make defense companies more secure. "There are some things that we're working on with the Office of Small Business [Programs] to develop a purpose-built cloud that some of the small businesses can just shoehorn themselves into and work out of there," David McKeown, the Pentagon's deputy CIO for cybersecurity and chief information security officer, told reporters Thursday. The goal is to introduce a pilot version this year with up to 75 small businesses to determine whether data can be adequately secured in a cloud environment. If it's successful, the pilot could be scaled and offered to more companies, McKeown said. "But at some point it may just be a service offering that they'll have to consume themselves. But it sure will beat having to build out all of the cybersecurity inside their own networks and boundaries if they can work out of these environments," he said.

Read the full article here.

THE CFI RELEASES NEW GUIDANCE ON RESEARCH SECURITY

Innovation | March 28, 2024

Today, the Canada Foundation for Innovation (CFI) published its new guidance on research security to support its commitment to providing the Canadian research community with current, relevant information and best practices to mitigate security risks to safeguard research. This new online material provides up-to-date guidance for institutions on the CFI's implementation of research security measures related to the Government of Canada's:

- Policy on Sensitive Technology Research and Affiliations of Concern , and
- National Security Guidelines for Research Partnerships .

Researchers and research administrators can now access the CFI's procedures, resources (including its attestation form) and frequently asked questions about its research security requirements.

The CFI is dedicated to continuing our commitment to open science, international collaboration, and equity, diversity and inclusion while supporting the community to safeguard Canada's research.

Read the full article here.

MIDDLE EAST UNIVERSITIES HEDGE BETS BETWEEN CHINA AND THE US

Yojana Sharma | University World News | March 27, 2024

China's stepping up of research relations with countries in the Middle East – Saudi Arabia and the United Arab Emirates in particular – has caught the eye of the United States which is putting pressure on some countries in the region to scale back research collaboration in potentially sensitive areas such as artificial intelligence (AI). Research collaborations between China and several Middle Eastern countries has risen exponentially, especially in the last few years, with some experts saying research competition between the US and China has migrated to, and intensified within, the MENA (Middle East and North Africa) region, especially the Gulf states. "The exponential increase in collaborations with China-based authors is in line with China's steep rise in its overall scientific publications," said Yusuf Ikbal Oldaç, assistant professor at Lingnan University in Hong Kong, who has researched China's science collaborations with Muslim-majority countries including Saudi Arabia, Egypt, Iran, Pakistan, Turkey and Malaysia.

Read the full article here.

ACADEMICS ADRIFT AFTER HONG KONG PASSES NEW SECURITY LAW

Yojana Sharma | University World News | March 22, 2024

When Aaron Han Joon Magnan-Park secured a tenure track position at the University of Hong Kong (HKU) just over a decade ago, it was the dream job for the American academic specialising in Hong Kong's action cinema. "I felt that I had won the academic lottery," he said. Since then, however, much has changed in a city once admired for its freedoms and openness. The former assistant professor in the department of comparative literature at HKU left Hong Kong last year, pointing to the Beijing-imposed National Security Law (NSL). "Under this new political reality, I could not finish my tenure book the way I wanted to … without somehow finding myself on the wrong side of the new red lines," he told University World News.

Read the full article here.

FY24 BUDGET UPDATE: SECOND PART OF FEDERAL BUDGET PASSED INTO LAW; DEFENSE BASIC RESEARCH HIT WITH SIGNIFICANT CUT

Brian Mosely | Computing Research Policy | March 28, 2024

At the end of last week, Congress passed into law the remaining appropriation bills for the second half of the Fiscal Year 2024 federal budget. As regular readers will recall, earlier this month Congress passed the initial batch of funding legislation, which contained the budgets for the National Science Foundation (NSF), Department of Energy Office of Science, National Institute of Standards and Technology (NIST), and NASA. Those agencies received flat funding or significant cuts to their budgets. And, unfortunately, that trend continues with this second batch of funding legislation. In terms of covered research agencies, this current set of bills includes the budgets for the Department of Defense (DOD) research accounts and the National Institutes of Health (NIH).

Read the full article here.

THE TEXAS A&M
UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute

USEFUL RESOURCES

DEFENSE INDUSTRIAL BASE CYBERSECURITY STRATEGY 2024

Department of Defense | March 21, 2024

The Department of Defense's (DoD) Defense Industrial Base (018) Cybersecurity Strategy is an actionable framework for sustaining a more resilient Joint Force and defense ecosystem-one that prevails within and through one of today's most contested domains: cyberspace. Our nation's defense industrial base is critical to achieving our national security goals and maintaining our technology advantage. It is imperative that we protect it from the threat of malicious cyber activity and attacks. T

View the full resource here.

BUILDING POSITIVE CULTURE

Peter J. Lapp | DITMAC's Behavioral Threat Analysis Center (BTAC) | March 2024

Creating organizational trust and a positive workplace culture is not just about compliance; it's a strategic advantage and a duty to employees that, in turn, boosts organizational morale. By understanding the unique challenges faced by diverse individuals, including social stigmas, discrimination, and barriers to success, organizations can foster a more inclusive and supportive environment that positively affects ALL employees.

View the full resource here.

QUICK REFERENCE TABLE OF CURRENT & UPCOMING FEDERAL RESEARCH SECURITY REQUIREMENTS

Council on Governmental Relations | February 2024

View the full resource here.

DESIGNATION OF CHINESE MILITARY COMPANIES

Office of the Under Secretary of Defense | Federal Register | April 2, 2024

The Secretary of Defense has determined that the entities listed in the **SUPPLEMENTARY INFORMATION** section of this notice qualify as “Chinese military companies” in accordance with the William M. (Mac) Thornberry National Defense Authorization Act (NDAA) for Fiscal Year 2021 (FY21)

View the full resource here.

THE TEXAS A&M
UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute