RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE

THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary

April 18, 2024

CHINA'S FLAG IS RED, NOT GREEN

Thomas J. Duesterberg | WSJ Opinion | April 7, 2024

Before environmental protection became a global issue, Chinese leader Deng Xiaoping taught that "only development is a solid truth." Deng saw the degradation of the environment as a "necessary evil" in the drive for Chinese growth. As a result, China now leads the world in carbon-dioxide emissions, land and water pollution, and the depletion of natural resources. China's current leader, Xi Jinping, has pledged to build what he calls an "ecological civilization" in service of a net-zero future. This is a claim ripe for re-evaluation, especially with Treasury Secretary Janet Yellen on a visit to Beijing and Earth Day approaching. The Chinese Communist Party isn't a serious steward of the global commons, and Western leaders must refute this dangerously misleading narrative. China's record of environmental degradation starts with its exploitation of Asia's water resources. Mao Zedong cut down as much as a third of the country's forests to expand agriculture and build modern industry.

Read the full article here.

THE U.S. COUNTERINTELLIGENCE HEAD SAYS THE LIST OF THREATS IS LONG AND GETTING LONGER

Ryan Lucas | NPR WBEZ Chicago | April 12, 2024

As the head of American counterintelligence, Mike Casey sees on a daily basis the scope of foreign spying operations, cyberattacks and economic espionage against the United States. "The scale is impressive and terrifying," said Casey, who stepped into his current job last year after working for more than two decades in Congress. He finished up his time on the Hill as the staff director for the Senate Intelligence Committee, so he already had deep understanding of the array of threats facing the U.S. What's changed now, though, is it's his responsibility to keep those secrets safe. "Fortunately for me, and unfortunately for everybody else, counterintelligence, it turns out, is a growth business," he told NPR in an interview. "More players are getting into it with more tools, going after more targets." The list of concerns is a long one. The usual suspects — China, Russia, Iran and North Korea — lead the way, he says, but there are other actors, including private sector entities and cybercriminals who are also getting involved.

Read the full article here.

ACCESSING AND TRANSFERRING RESEARCH DATA FROM CHINA

Noble Endeavours | Linkedin | April 10, 2024

Institutions rightly expend significant resources ensuring staff understand GDPR and other domestic data protection regulations. However, when collaborating internationally, understanding the regulatory framework of your partner country can be equally important. This is especially true in jurisdictions as large and complex, and that has changed as rapidly, as China. China's emphasis on cyberspace sovereignty as an aspect of national security underlies both its implementation of internet restrictions – often called the 'Great Firewall' – as well as a new suite of data protection legislation that started coming into force from 2017. Data transfer is now subject to a comprehensive set of regulations that significantly clarify what was previously a chaotic morass of rules.

Read the full article here.

WHY WE MUST TAKE SERIOUSLY CHINA'S MASTERY AND MISUSE OF AI ESPIONAGE

Aditya Sinha | First Post | April 9, 2024

In William Gibson's science fiction novel Neuromancer, artificial intelligence is depicted as being used for espionage and to manipulate international relations. The novel revolves around a washed-up computer hacker hired by a mysterious employer to pull off the ultimate hack. In the process, he encounters AIs that manipulate individuals and events to serve their ends, subtly influencing global power structures. While we haven't reached the dystopian future of AI depicted in 'Neuromancer', where artificial intelligence becomes a direct threat to human existence, the world is witnessing the early stages of AI's potential for harm. Countries have begun to harness AI for espionage, sowing discord in foreign nations and inciting political unrest. These actions mark the subtle beginnings of AI's potential to manipulate and destabilise international relations, and China is at the forefront of this.

Read the full article here.

WHAT KEEPS CISOS UP AT NIGHT? MANDIANT LEADERS SHARE TOP CYBER CONCERNS

Billy Mitchell | Cyberscoop | April 12, 2024

An increasing volume of zero days — 97 total in the last year. The evolution of cyber extortion to now include physical threats and advanced coercion. More and more threat actors "living off the land." These are but a few of the top concerns that keep chief information security officers up at night, according to the top leaders of cybersecurity firm Mandiant, now a subsidiary of Google Cloud. Speaking during a press conference at Google Cloud's Next technology conference this week, Mandiant CEO Kevin Mandia convened Sandra Joyce, vice president of Mandiant Intelligence, and Jurgen Kutscher, vice president of Mandiant Consulting, to share their perspectives on the threat landscape and how it's evolving.

Read the full article here.

PROTECTING QUANTUM SCIENCE AND TECHNOLOGY

Federal Bureau of Investigation | April 12, 2024

World Quantum Day, April 14, was initially conceived to ignite interest and generate enthusiasm for quantum mechanics. It has since morphed into so much more. Quantum information science is an emerging field with the potential to create revolutionary advances in science and engineering and drive innovation across the U.S. economy. When new technologies are the product of American ideas and research, it's the FBI's and our security partner agencies' job to protect them. Today, adversarial nation-states are aggressively attempting to obtain a strategic advantage over the U.S. by stealing U.S. technologies and research know-how to help bolster their respective government's policies that violate international norms—including respect for rule of law, fair trade, and full scientific research collaborative reciprocity—while damaging U.S. economic competitiveness and harming U.S. national and economic security.

Read the full article here.

CHINA'S UNIVERSITIES GRAB 6 OF 10 TOP SPOTS IN WORLDWIDE SCIENCE RANKING

Caroline Wagner | Ohio State News | April 13, 2024

University leaders pay close attention to comparative rankings such as those offered by Times Higher Education, Shanghai Ranking Consultancy and others. Rankings influence student matriculation numbers, attract talented faculty and justify donations from wealthy donors. University leaders rail against them, and some schools "withdraw" from them, but rankings are influential. A radical shift in the data underlying rankings is about to upend the rankings world – largely in favor of China's position. For instance, in early 2024, the Leiden University Center for Science and Technology Studies CWTS group issued new university rankings that add open-data sources to the traditional curated list of elite journals that has Where once the list of universities with the highest scientific impact would have been dominated by U.S. and U.K. schools including Cambridge, Stanford, Harvard and MIT, the new top 10 list of universities with high scientific impact includes six universities from China. been the standard. The results show a world turned upside down for university rankings.

Read the full article here.

NO SUBSTITUTE FOR VICTORY

Matt Pottinger and Mike Gallagher | Foreign Affairs | April 10, 2024

Amid a presidency beset by failures of deterrence—in Afghanistan, Ukraine, and the Middle East—the Biden administration's China policy has stood out as a relative bright spot. The administration has strengthened U.S. alliances in Asia, restricted Chinese access to critical U.S. technologies, and endorsed the bipartisan mood for competition. Yet the administration is squandering these early gains by falling into a familiar trap: prioritizing a short-term thaw with China's leaders at the expense of a long-term victory over their malevolent strategy.

Read the full article here.

RESEARCH FOR SALE: HOW CHINESE MONEY FLOWS TO AMERICAN UNIVERSITIES

James T. Areddy | The Wall Street Journal | April 15, 2024

Chinese companies are feeling a cold shoulder in the U.S.—except at universities, where they are welcomed as customers. American universities sign contracts around the world to sell their research and training expertise, and some of their most lucrative agreements have been with companies based in China. The decadeslong trade thrives despite a deepening U.S.-China rivalry and rising sensitivities about Beijing's influence on American campuses. Nearly 200 U.S. colleges and universities held contracts with Chinese businesses, valued at $2.32 billion, between 2012 and 2024, according to a review by The Wall Street Journal of disclosures made to the Education Department. The Journal tallied roughly 2,900 contracts. The extensive trade in American expertise presents a quandary for universities and policymakers in Washington: Where's the line between fostering academic research and empowering a U.S. rival?

Read the full article here.

THE US GOVERNMENT HAS A MICROSOFT PROBLEM

Eric Geller | WIRED | April 15, 2024

When Mircorsoft revealed in January that foreign government hackers had once again breached it system, the news prompted another round of recriminations about the security posture of the world's largest tech company. When Microsoft revealed in January that foreign government hackers had once again breached its systems, the news prompted another round of recriminations about the security posture of the world's largest tech company. Despite the angst among policymakers, security experts, and competitors, Microsoft faced no consequences for its latest embarrassing failure. The United States government kept buying and using Microsoft products, and senior officials refused to publicly rebuke the tech giant. It was another reminder of how insulated Microsoft has become from virtually any government accountability, even as the Biden administration vows to make powerful tech firms take more responsibility for America's cyberdefense.

Read the full article here.

CONTEXTUALIZING DEEPFAKE THREATS TO ORGANIZATIONS

Cybersecurity Information Sheet | September 12, 2023

Threats from synthetic media, such as deepfakes, present a growing challenge for all users of modern technology and communications, including National Security Systems (NSS), the Department of Defense (DoD), the Defense Industrial Base (DIB), and national critical infrastructure owners and operators. As with many technologies, synthetic media techniques can be used for both positive and malicious purposes. While there are limited indications of significant use of synthetic media techniques by malicious state-sponsored actors, the increasing availability and efficiency of synthetic media techniques available to less capable malicious cyber actors indicate these types of techniques will likely increase in frequency and sophistication.

Read the full article here.

GENERAL COMMENDATIONS AND RECOMMENDATIONS FROM UNIVERSITY VISITS BY THE DIRECTORATE OF DEFENSE TRADE CONTROLS

Office of Defense Trade Controls Compliance (DTCC)

This white paper provides general findings from visiting various universities and research centers that are engaged in activities of the International Traffic in Arms Regulations from 2020 to early 2024. The paper provides "commendations" and "recommendations" that the Office of Defense Trade Controls Compliance (DTCC) provided to the universities following each visit. DTCC highlights "best practices" in complying with the ITAR in the commendations section and offers ways to improve a compliance program in the recommendations section.

Read the full article here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute

SECTION 702 OVERVIEW

Office of the Director of National Intelligence

•Section 702 is a key provision of the FISA Amendments Act of 2008 that permits the government to conduct targeted surveillance of foreign persons located outside the United States, with the compelled assistance of electronic communication service providers, to acquire foreign intelligence information. •The government uses the information collected under Section 702 to protect the United States and its allies from hostile foreign adversaries, including terrorists, proliferators, and spies, and to inform cybersecurity efforts.

View the full resource here.

WHAT IS THE ROLE OF FUTURE INTERNATIONAL COLLABORATION: RISKS AND OPPORTUNITIES

The Hoover Institution | January 22, 2024

The Hoover Institution held a conversation on What is the Role of Future International Collaboration: Risks and Opportunities on January 22, 2024 from 11:00 AM - 12:30 PM PT. Dr. Thomas Mason addressed aspects of research openness and the daily need to protect the information that is critically important to universities, National Labs, the federal government, and the private sector. The conversation was followed by a 30 minute Q&A. As a national security science laboratory Los Alamos National Lab has worked to strike the right balance between openness of research and protection of information for over eighty years. The talk addressed the historic importance of open international collaboration in fostering rapid innovation with economic and national security benefits while still recognizing the need to manage the risks that come with international engagement.

View the full resource here.

ADVANCEMENT OF INSIDER RISK EDUCATION JOURNAL

The National Counterintelligence and Security Center | 2024

Companies and individuals have been selling commercial surveillance tools to governments and other entities that have used them for malicious purposes. Journalists, dissidents, and other persons around the world have been targeted and tracked using these tools, which allow malign actors to infect mobile and internet-connected devices with malware over both WiFi and cellular data connections.

View the full resource here.

CONFERENCE TRACKING TAGS: RISK CONSIDERATIONS

National Counterintelligence And Security Center | April 10, 2024

Attending conventions, trade shows, and symposiums are important elements of any U.S. government (USG) agency's strategy for conducting outreach and staying connected. However, the benefits of such participation also come with Counterintelligence (CI) and Operations Security (OPSEC) risks. The latest concerning trend involves the expanded use of tracking tags by conference organizers which, if not properly mitigated, can place attending USG officers, their home agencies, and sensitive national security information at risk.

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute