ASCE
ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM
https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

August 10, 2023

DOD LOOKS TO BLOCK CHINESE AND RUSSIAN INFLUENCE ON US ACADEMIA

Jonathan Lehrfeld | Defense News | July 5, 2023

The Pentagon just released a black list of mostly Chinese and Russian research institutes that it says have engaged in “problematic activity,” including trying to infiltrate sensitive Defense Department research at U.S. colleges and universities. The Pentagon partners with hundreds of U.S. universities and research institutions, a relationship malign actors have been able to reportedly hijack to steal U.S. defense technology. When those U.S. institutions also get funding from the black-listed entities, the foreign partners have in the past used the research relationship to try to access and even steal sensitive defense research. “The publication of these foreign entities underscores our commitment to ensuring the responsible use of federal research funding and safeguarding our critical technologies from exploitation or compromise,” Heidi Shyu, the undersecretary of defense for research and engineering, said in a June 30 release. The statement went on to encourage U.S. universities and industry to “review the list and exercise caution when engaging with entities listed.”

Read the full article here.

CISA: MOST CYBERATTACKS ON GOV’TS, CRITICAL INFRASTRUCTURE INVOLVE VALID CREDENTIALS

Jonathan Greig | The Record | July 26, 2023

More than half of all cyberattacks on government agencies, critical infrastructure organizations and state-level government bodies involved the use of valid accounts, according to a new report from the Cybersecurity and Infrastructure Security Agency (CISA). In 2022, CISA worked with the United States Coast Guard (USCG) to conduct 121 Risk and Vulnerability Assessments (RVAs) on federal civilian agencies, high priority private and public sector critical infrastructure operators; and select state, local, tribal, and territorial stakeholders. Gabriel Davis, a risk operations federal lead at CISA, told Recorded Future News that these assessments are designed to test an organization's defenses and give the government a chance to see how they would respond to a sophisticated attack. They also give CISA insights into how hackers operate. The report of the agency's findings, published on Wednesday, noted that threat actors “completed their most successful attacks via common methods, such as phishing and using default credentials.”

Read the full article here.

SCIENTISTS OF CHINESE DESCENT LEAVING THE US AT AN ACCELERATING PACE

Rebecca Trager | Chemistry World | August 2, 2023

Even before the US government announced plans to crack down on perceived espionage by China in 2018, scientists of Chinese descent were leaving the US. Since then the numbers leaving have only accelerated as both junior and experienced faculty depart, according to a new analysis. The work reveals that nearly 20,000 scientists of Chinese descent who began their careers in the US have left for other countries, including China, between 2010 and 2021, a team at Princeton, Harvard and the Massachusetts Institute of Technology has found. 'The migration has increased during those 12 years, from 900 scientists in 2010 to 2621 in 2021, with an accelerated departure rate (75% higher) in the last three years … coinciding with the launch of the China Initiative in 2018,' the authors wrote in the supplementary material. Launched during the Trump administration to curb Chinese state-backed espionage and efforts aimed at stealing US intellectual property, the China Initiative was terminated in February of last year following criticism that it was tantamount to racial profiling and damaging to the US's scientific enterprise.

Read the full article here.

TIKTOK HAS PUSHED CHINESE PROPAGANDA ADS TO MILLIONS ACROSS EUROPE

Iain Martin and Emily Baker-White | Forbes | July 27, 2023

TikTok has served up a flood of ads from Chinese state propaganda outlets to millions of Europeans in recent months, according to a new ad library published by the company on July 20. The promotions range in topic from defenses of Chinese Covid-19 lockdowns to adorable cats playing on the Great Wall of China to efforts to recast the country's Xinjiang region — where it has persecuted and detained more than one million mostly Muslim Uyghurs — as a spectacular tourist destination. An analysis of the ad library conducted by Forbes showed that as of Wednesday, July 26, more than 1,000 ads from Chinese state media outlets like People's Daily and CGTN have run on the platform since October 2022. They have been served to millions of users across Austria, Belgium, the Czech Republic, Germany, Greece, Hungary, Italy, Ireland, the Netherlands, Poland, and the United Kingdom.

Read the full article here.

NEW ACOUSTIC ATTACK STEALS DATA FROM KEYSTROKES WITH 95% ACCURACY

Bill Toulas | BleepingComputer | August 5, 2023

A team of researchers from British universities has trained a deep learning model that can steal data from keyboard keystrokes recorded using a microphone with an accuracy of 95%.When Zoom was used for training the sound classification algorithm, the prediction accuracy dropped to 93%, which is still dangerously high, and a record for that medium. Such an attack severely affects the target's data security, as it could leak people's passwords, discussions, messages, or other sensitive information to malicious third parties. Moreover, contrary to other side-channel attacks that require special conditions and are subject to data rate and distance limitations, acoustic attacks have become much simpler due to the abundance of microphone-bearing devices that can achieve high-quality audio captures. This, combined with the rapid advancements in machine learning, makes sound-based side-channel attacks feasible and a lot more dangerous than previously anticipated.

Read the full article here.

CHINA CURBS DRONE EXPORTS OVER 'NATIONAL SECURITY CONCERNS'

Simone McCarthy | CNN | August 1, 2023

China will place export controls on drone and drone equipment in order to "safeguard national security and interests," its commerce ministry announced Monday, in a move that could impact the war in Ukraine. The restrictions on equipment will require vendors to seek permission to export certain drone engines, lasers, imaging, communications and radar gear, and anti-drone systems. Consumer-grade drones with certain specifications are also subject to the controls, which come into effect September 1. All civilian drones not included in the controls are prohibited from being exported for military purposes, an unidentified ministry spokesperson said in an online statement. "China's modest expansion of the scope of drone control this time is an important measure to demonstrate its commitment as a responsible major country to implement global security initiatives and maintain world peace," the statement said, adding that China has "consistently opposed the use of civilian drones for military purposes."

Read the full article here.

AI IN RESEARCH

UK Research Integrity Office | July 25, 2023

The explosion of interest in chatbots is unsurprising given that the content they generate is impressive, especially compared to earlier clunky efforts in automated language production. They have passed the Turing Test in a way that ELIZA never could. Although neural networks date back decades, the underlying 'transformer' technology that has enabled the new chatbots is only six years old. This is genuinely new ground. However, these new chatbots are not truly Artificial Intelligence (AI) because they are not intelligent. The language-language models (LLMs) they are based on work by creating a network of billions of connections between words or stems of words – known as 'tokens' – and weighting those links based on training material, often taken from the web, to suggest the next appropriate token based on a prompt. Human moderators usually rate outputs on how coherent, convincing, or human-like they sound as a second layer of training, known as Reinforcement Learning from Human Feedback or RHLF.

Read the full article here.

THE RACE FOR U.S. TECHNICAL TALENT

Diana Gelhaus, James Ryseff, and Jack Corrigan | Center for Security and Emerging Technology | August 2023

Technical talent—individuals in computer and mathematical occupations who make up a large share of the AI workforce—is essential to U.S. innovation and growth. The mobility of this talent is also essential, as the movement of technical talent promotes the diffusion of ideas, expands professional networks, and spurs the development of innovative products. Attracting these highly mobile tech workers is therefore critical to staying on the cutting edge of the technological frontier. This is especially true for the defense community, which needs ready access to cutting-edge technologies and the workers who can design, develop, and deploy them. In the years ahead, understanding how this human capital flows within and between industry sectors is critical for maintaining U.S. technological leadership. Conventional wisdom holds that the Department of Defense (DOD) and the defense industrial base (DIB)—collectively referred to as the defense community—generally struggle to access the technical talent they need.

Read the full article here.

THE WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY: ISSUES AND OPTIONS FOR THE 118TH CONGRESS

Emily G. Blevins and Rachael D. Roan | Congressional Research Service | July 26, 2023

Congress has a long-standing interest in the development and implementation of science and technology (S&T) policies across the federal government as well as the effective coordination of multi-agency research and development (R&D) initiatives. To ensure a permanent source of S&T-related advice and policy coordination within the White House, Congress established the Office of Science and Technology Policy (OSTP) within the Executive Office of the President (EOP) through the National Science and Technology Policy, Organization, and Priorities Act of 1976 (P.L. 94-282). The act charged it with serving as "a source of scientific and technological analysis and judgment for the President with respect to major policies, plans, and programs of the Federal Government." OSTP develops and coordinates the implementation of federal S&T policies and R&D initiatives through the work of the National Science and Technology Council (NSTC). Established in 1993 by Executive Order 12881, the NSTC is composed of representatives from federal departments and agencies with significant S&T responsibilities and is charged with coordinating S&T policy across the federal government.

Read the full article here.

MAPPING EMERGING TECHNOLOGIES AND THEIR SUPPLY CHAINS

John VerWey, Jennifer Melot, Ilya Rahkovsky Zachary Arnold, and Neha Singh | The Center for Security and Emerging Technology | August 2, 2023

Emerging technologies are of keen interest to policymakers, private firms, and researchers due to their perceived economic and national security promise. While interest in emerging technologies has spiked, ongoing supply chain interruptions have exposed the worldwide reliance and fragility of some technologies' global value chains. This policy brief argues that policymakers' efforts to increase competitiveness in emerging technologies and resilience in supply chains should be closely coordinated and aligned. It assesses the challenges of promoting emerging technologies and the tools that may assist in this, and turns to supply chain security management to show how using similar sources of information and analytical methods could increase resilience. The brief concludes by providing policymakers with a template to map emerging technology supply chains based upon two tools developed by CSET's Emerging Technology Observatory: the Map of Science and the Supply Chain Explorer.

Read the full article here.

THE PRC INVESTS IN QUANTUM TECHNOLOGY

Strider Insights | August 7, 2023

Massive PRC government investments in quantum technology, targeted exploitation of foreign research institutions, and burgeoning efforts to shape international quantum standards pose a growing threat to non-PRC companies' future market share. In 2015, the Chinese Communist Party (CCP) published "Made in China 2025," a strategic plan and industrial policy strategy that, among other goals, called for the PRC to capture global market share through technology transfer and industrial subsidies. The drive from the PRC to dominate the future of quantum is being fueled by government subsidies that dwarf the investments seen in other countries. By 2021, for example, the PRC had spent more than EU $10 billion, roughly half the world's total, while the UNSN invested $4.5 billion and the EU $1.4 billion. The disparity in funding has resulted in a comparable innovation imbalance, with the PRC patenting more than 600 quantum technologies between 2012 and 2019 and the UNSN patenting around 400.

Read the full article here.

EVENT: (REGISTRATION REQUIRED)
WHAT HAPPENS TO GLOBAL SCIENCE IF THE UNITED STATES AND CHINA QUIT COLLABORATING?

Issues in Science and Technology

Over the last 40 years, international scientific collaboration between the United States and China in particular has increased global research productivity. But more recently, as the US policy community has become focused on competitiveness and security, these collaborations have begun to decrease, and many Chinese scientists and students are now leaving the country. E. William Colglazier argues in Issues in Science and Technology that it is in the national interest for US scientists to collaborate with the best scientists in the world, regardless of where they reside—however, “politics remains a more powerful force than science.” How is the science community experiencing and responding to these changes? In the long term, how will this period of US-China disentanglement reshape international scientific partnerships and collaboration? And what will this realignment mean for the promise of the global scientific enterprise itself?

On August 17 at 2:00 p.m. ET, join us to talk about how US-China competition is changing the trajectory of global scientific collaboration and engagement.

Register here.

THE TEXAS A&M
UNIVERSITY SYSTEM

The Academic Security and Counter Exploitation Program is coordinated by The Texas A&M University System Research Security Office as a service to the academic community.
https://rso.tamus.edu