ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

July 6, 2023

DEPARTMENT OF DEFENSE STRENGTHENING EFFORTS TO COUNTER UNWANTED FOREIGN INFLUENCE ON DOD-FUNDED RESEARCH AT INSTITUTIONS OF HIGHER EDUCATION

U.S. Department of Defense | June 30, 2023

The Department of Defense today announced the publication of a list of foreign entities that have been confirmed as engaging in problematic activity as described in Section 1286 of the Fiscal Year 2019 National Defense Authorization Act, as amended. These include practices and behaviors that increase the likelihood that DOD-funded research and development efforts will be misappropriated to the detriment of national or economic security or be subject to violations of research integrity or foreign government interference. "Protecting and maintaining the integrity of our research enterprise is integral to national security," said Heidi Shyu, Under Secretary of Defense for Research and Engineering (USD(R&E). "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."

Read the full article here.

NSA AND CISA BEST PRACTICES TO SECURE CLOUD CONTINUOUS INTEGRATION/CONTINUOUS DELIVERY ENVIRONMENTS

National Security Agency/Central Security Service | Press Release | June 28, 2023

Software development and delivery supply chains are attractive targets for malicious cyber actors. They can use these environments to compromise cloud deployments throughout the automated software development and delivery lifecycle. The National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) are publicly releasing a Cybersecurity Information Sheet (CSI) - "Defending Continuous Integration/Continuous Delivery (CI/CD) Environments" to provide recommendations for integrating security best practices into typical software development and operations (DevOps) CI/CD environments. The agencies encourage organizations to use the best practices to harden their CI/CD cloud deployments. "The virtual cloud environment relies on software, making development and delivery a crucial component of providing services in the cloud," said Dr. Ethan Givens, NSA's Technical Director, Critical & Emerging Technologies. "Failure to effectively defend the CI/CD pipeline can provide an attack vector that circumvents security policies and products."

Read the full article here.

THE PERILS OF CHINA'S GREAT INFORMATION WALL

Dewey Murdick and Owen J. Daniels | TIME | June 25, 2023

The Chinese government recently cut off international access to a significant portion of the country's public data—including contracts, patents, scientific conference proceedings, dissertations, and statistical information. Coverage has attributed the disappearance of some of this data to reports by think tanks that leveraged such data to highlight, among other findings, how the People's Liberation Army hoped to access and weaponize American-designed semiconductors. This ongoing situation is unfortunate for numerous reasons, not least because the research we conduct at Georgetown's Center for Security and Emerging Technology (CSET) using Chinese data has consistently been recognized as accurate, balanced, and responsible. More importantly, locking down data and preventing responsible researchers who rely on publicly available materials (often called "open source") from understanding China is a strategic mistake for the People's Republic. Allowing global access only to unsatisfactory data may lead to unsatisfactory outcomes for everyone.

Read the full article here.

CHINA IS GEARING UP TO EVADE CHIP-EXPORT RULES

Matt Brazil and Peter W. Singer | Defense One | June 26, 2023

China has long relied on foreign-made computer chips for bleeding-edge national security efforts, from supercomputers to domestic surveillance to AI. Now, as American policymakers work to stem this flow of advanced technology, China is trying to accelerate its own chipmaking industry—and devising ways to circumvent export restrictions. For over three decades, the business model used by Western companies made it easy for local middlemen to sell and resell pocket-sized supercomputer chips, smoothing their path to sanctioned organizations on the U.S. Entity List. For instance, Intel's multi-core Xeon CPUs were used to build China's Tianhe-2, the world's fastest supercomputer as of 2013, owned by the National University of Defense Technology and used for a wide range of military research. This business model is made up of four parts: company sales and engineering staff and their senior management, who are almost all Chinese citizens; Chinese computer manufacturers such as Lenovo, Haier, and others, that purchase chips in bulk and sometimes resell them on the open market; the huge electronics emporiums throughout China, such as Huaqiang Electronics World in Shenzhen; and the electronics distributors ("distis"), that resell CPUs and GPUs throughout China

Read the full article here.

THE SOUTH KOREAN 'MASTER' OF CHIPS ACCUSED OF SHARING SECRETS WITH CHINA

Christian Davies, Song Jung, and Eleanor Olcott | Financial Times | June 25, 2023

In 2006, a Korean engineer called Choi Jin-seok achieved a feat that earned him the nickname "master of semiconductor yield". Then serving as the chip manufacturing head at semiconductor company Hynix, Choi oversaw the certification of what was then the latest generation of memory chips ahead of Samsung Electronics, its wealthier and more celebrated Korean rival. "He is a genius of process technology and a competent man capable of running a big company," says a person who has worked with Choi.
But his career stalled in 2010, and after a period in the wilderness he embarked on a quixotic mission to re-emerge as a leading light in the Chinese semiconductor industry. Instead, he faces a possible prison term after he was indicted in South Korea earlier this month on charges of stealing Samsung's technology in order to build a copycat memory chip plant in China.

Read the full article here.

THESE ARE THE MOST DANGEROUS SOFTWARE SECURITY FLAWS OF THE YEAR - ARE YOU AT RISK?

Sead Fadilpašić | TechRadar | July 1, 2023

The MITRE Corporation released its annual list of the most dangerous software flaws for 2023, and there's been no change at the top spot. The American not-for-profit organization has been analyzing public vulnerability data found in the National Vulnerability Database (NVD) for root cause mappings to CVE weaknesses for the past two years. During that time, the organization analyzed almost 44,000 CVEs.
As per the analysis, out-of-bounds write flaw is the most dangerous software vulnerability for the year (as was for the year 2022). This is a type of software flaw that sees a program write outside the bounds of an allocated area of memory. As a result, the endpoint might crash, or execute arbitrary code. Threat actors usually abuse this flaw by writing data that's larger in size than the size of the allocated memory area, or by writing the data to an incorrect location within the memory area.

Read the full article here.

NEW CHINESE LAW RAISES RISKS FOR AMERICAN FIRMS IN CHINA, U.S. OFFICIALS SAY

Kate O'Keeffe | The Wall Street Journal | June 30, 2023

U.S. counterintelligence officials are amping up warnings to American executives about fresh dangers to doing business in China under an amended Chinese law to combat espionage. A bulletin issued Friday by the National Counterintelligence and Security Center warns that the revised law is vague about what constitutes espionage and gives the government greater access to and control over companies' data, potentially turning what would be considered normal business activities into criminal acts.
The amended counterespionage law, which takes effect Saturday, has unsettled foreign businesses in China. The publication of those revisions this spring came amid a wave of raids, inspections, and other acts by Chinese authorities against foreign, chiefly American businesses, as tense U.S.-China relations deteriorated further.

Read the full article here.

CHINA APPROVES WIDE-RANGING EXPANSION OF COUNTER-ESPIONAGE LAW

Laurie Chen | Reuters | April 26, 2023

Chinese lawmakers passed a wide-ranging update to Beijing's anti-espionage legislation on Wednesday, banning the transfer of any information related to national security and broadening the definition of spying. China's top legislative body passed the revised Counter-Espionage Law - its first update since 2014 - following three days of deliberations, and it will take effect from July 1, state media reported. President Xi Jinping has made national security a key focus of his administration since taking office in 2012 and analysts say these revisions are evidence of that stricter regime as suspicion of the United States and its allies grows. All "documents, data, materials, and items related to national security and interests" are under the same protection as state secrets following the revisions, according to the full text of the revised law published by Xinhua late Wednesday. The law does not define what falls under China's national security or interests.

Read the full article here.

CHINA'S UPDATED COUNTERESPIONAGE LAW IS 'DIRECT ATTACK' ON US CITIZENS, BUSINESSES: SEN MARKWAYNE MULLIN

Madeline Coggins | Fox News | July 1, 2023

U.S. intelligence officials have issued a warning to American businesses and company employees in China as sweeping updates to the country's counterespionage legislation go into effect on Saturday. One lawmaker, however, warns the revision is a "direct attack" on American citizens and businesses. "This is a direct attack on United States citizens and businesses," Sen. Markwayne Mullin, R-Okla., said on "Fox & Friends Weekend" Saturday. "When they talk about the word espionage ... and national security with no definition, that holds every American citizen that goes to China to do business or on vacation liable for just about anything the Communist Party of China wants to interpret and could arrest you and hold you in contempt."

Read the full article here.

CHINESE INVESTMENT IN U.S. STARTUPS UNDER SCRUTINY FOR ESPIONAGE

Sabri Ben-Achour | MARKETPLACE | June 21, 2023

When he was an undergrad at UC Santa Barbara, Alon Raphael cofounded a startup called Femtometrix. It sells technology to computer chip makers that detects mind bogglingly tiny defects buried within chips. "It's the bleeding edge of the most advanced chips that are coming out that we are applicable to," he said. Raphael eventually hired engineers, including three who were Chinese nationals whose work visas he sponsored. Two came on board in 2018, the third in 2020. Over time they grew close, he said. After a little while, one of them said he wanted to invest in the company. "One of the requests for the investment was to know the details of the patent portfolio," Raphael explained. When investors and startups connect, investors can get significant access to a company's information. Startups set up what are called "data rooms," where prospective investors can view proprietary data and plans. Once they consummate their investment, they can obtain more information.

Read the full article here.

KILTS AND QIPAOS IN BRITAIN: NEARLY 400 CHINA 'UNITED FRONT' GROUPS THRIVE

Didi Kirsten Tatlow | Newsweek | June 29, 2023

An investigation by Newsweek identifies hundreds of groups in Britain tied to the Chinese Communist Party. Many work to deepen Beijing's influence worldwide. The goal of the Chinese Qipao Association in Scotland is to celebrate the slim-fitting dress that is the quintessence of Chinese elegance. At least on the surface. The association is one of nearly 400 groups identified by a Newsweek investigation that are embedded in British society but are also part of Communist Party of China networks that aim to spread influence around the world and help China achieve global pre-eminence by 2049. That has put China at the top of the list of global security threats for U.S. political and intelligence leaders—even ahead of Russia. The extent of the organizations that are linked—directly or indirectly—to the party's United Front system in America's closest intelligence ally is revealed for the first time just as Washington is pressing its friends to do more to counter growing CCP influence and what is known as transnational repression of Chinese abroad. The United States has made multiple arrests recently.

Read the full article here.

CHINA OWNS 380,000 ACRES OF LAND IN THE U.S. HERE'S WHERE

Ximena Bustillo and Connie Hanzhang Jin | National Public Radio (NPR) | June 26, 2023

In 2021, a Chinese company bought land near an Air Force base in Grand Forks, N.D., sending lawmakers into a frenzy. Lawmakers feared that China, which many policymakers view as a strategic adversary even though it's the country's top trading partner outside North America, could gain control over the U.S. food and energy supply, as well as a hold on markets and critical infrastructure. Although Chinese-owned land is a tiny fraction of all foreign-owned land in the U.S., its purchases have raised fears that the Chinese government could have control, through the Chinese corporations, over U.S. assets or gain access to U.S.-based information.

Read the full article here.

NSF ANNOUNCES GUIDELINES FOR AGENCY RESEARCH SECURITY ANALYTICS PRACTICE

National Science Foundation | June 20, 2023

The U.S. National Science Foundation recently released guidelines for research security analytics on the agency's research security website. Research security, defined as safeguarding of the U.S. enterprise against the misappropriation of research and development, has received increased attention due to emerging competition and conflicting practices by competing economies. NSF is a leading advocate for an open, inclusive research enterprise that welcomes the contributions of international scientists to further U.S. science. The guidelines are one of several NSF activities demonstrating that the principles of open science can align with research security standards and reflect a fruitful dialogue between the federal government and the research community on appropriate mechanisms for ensuring transparent reporting of research commitments.

Read the full article here.

THE 'COLDEST WAR' IS AN INVISIBLE ONE FOR THE ARCTIC

Lilian Alessa | The Messenger Opinion | June 24, 2023

Climate change in the Arctic complicates implementation of the Department of Defense's Joint Mission, bringing both challenges and opportunities. Russia and China will use this Arctic transformation to benefit their national interests and try to limit the United States' ability to adapt to, and counter, such efforts. Highly aggressive, but conducted in a "gray zone" between war and peace, Russia and China are waging campaigns of influence, money, disinformation, and incremental change to subvert cooperative frameworks and gain power projection throughout the Arctic. Of concern to the United States and its allies and partners is the extension of Chinese and Russian malign influence campaigns to the previously inviolable forums of Arctic dialogues where data, information and sentiment can be collected and synthesized to gain insights about U.S. Arctic knowledge, capabilities, and posture.

Read the full article 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