ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

August 31, 2022

THE MOTHER OF ALL 'ZERO-DAYS' — IMMORTAL FLAWS IN SEMICONDUCTOR CHIPS

Michael D. Lumpkin and Peter L. Levin | The Hill | August 27, 2022

The CHIPS Act of 2022 was signed into law on Aug. 9. It provides tens of billions of dollars in public support for revitalization of domestic semiconductor manufacturing, workforce training, and "leap ahead" wireless technology. Because we outsource most of our device fabrication — including the chips that go into the Navy's submarines and ships, the Army's jeeps and tanks, military drones and satellites — our industrial base has become weak and shallow. The first order of business for the CHIPS Act is to address a serious deficit in our domestic production capacity. Notoriously absent from the language of the bill is any mention of chip security. Consequently, the U.S. is about to make the same mistake with microelectronics that we made with digital networks and software applications: Unless and until the government demands in-device security, our competitors will have an easy time of manipulating how chips function and behave. Nowhere is this more dangerous than our national security infrastructure. For the first quarter-century of ubiquitous internet access, policy makers and industry leaders did not imagine — literally could not conceive — a deliberate electronic intrusion from an ideological adversary.

Read the full article here.

FEDERALLY FUNDED RESEARCH TO BE FREE AND PUBLICLY ACCESSIBLE UNDER NEW WHITE HOUSE GUIDANCE

Edward Graham | Nextgov | August 26, 2022

The White House Office of Science and Technology Policy directed federal agencies on Thursday to begin adopting policies that would make taxpayer-funded research free and accessible to the general public. In a memo to the heads of executive departments and agencies, Dr. Alondra Nelson, deputy assistant to the president and deputy director for science and society performing the duties of director at OSTP, instructed officials to implement their public access policies by December 31, 2025, "in order to make publications and their supporting data resulting from federally funded research publicly accessible without an embargo on their free and public release." OSTP will also work with federal agencies to update their public access policies and data sharing plans by mid-2023. "When research is widely available to other researchers and the public, it can save lives, provide policymakers with the tools to make critical decisions and drive more equitable outcomes across every sector of society," Nelson said in a statement. "The American people fund tens of billions of dollars of cutting-edge research annually.

Read the full article here.

CHINA'S RESEARCHER RANKS CONTINUE TO GROW: REPORT

Sixth Tone | August 28, 2022

Tens of thousands of "high-level" scientists settled in China's largest cities over the past decade, helping reverse years of brain drain and turning their new homes into some of the largest research centers in the world, according to a report published Saturday at the annual Pujiang Innovation Forum in Shanghai. Compiled by German-British academic publishing company Springer Nature for a Chinese research institute, the report found the number of "high-level" scientists living and working in China surged 350% between 2012 to 2021. Cities in North America, Europe, and the rest of the Asia-Pacific region roughly doubled their scientist headcounts over the same period. High-level scientists were identified and located by tracking author address information for papers published in journals listed on the prestigious Nature Index. Beijing and Shanghai topped the scientist growth list, followed by London, New York, and Shenzhen.

Read the full article here.

MICROSOFT WARNS ABOUT PHISHING ATTACKS BY RUSSIA-LINKED HACKERS

Ravie Lakshmanan | The Hacker News | August 16, 2022

Microsoft on Monday revealed it took steps to disrupt phishing operations undertaken by a "highly persistent threat actor" whose objectives align closely with Russian state interests. The company is tracking the espionage-oriented activity cluster under its chemical element-themed moniker SEABORGIUM, which it said overlaps with a hacking group also known as Callisto, COLDRIVER, and TA446. "SEABORGIUM intrusions have also been linked to hack-and-leak campaigns, where stolen and leaked data is used to shape narratives in targeted countries," Microsoft's threat hunting teams said. "Its campaigns involve persistent phishing and credential theft campaigns leading to intrusions and data theft." Attacks launched by the adversarial collective are known to target the same organizations using consistent methodologies applied over long periods of time, enabling it to infiltrate the victims' social networks through a combination of impersonation, rapport building, and phishing. Microsoft said it observed "only slight deviations in their social engineering approaches and in how they deliver the initial malicious URL to their targets."

Read the full article here.

SUPPLY CHAIN RISK MANAGEMENT

Office of the Director of National Intelligence | The National Counterintelligence and Security Center | 2022

The mission of NCSC's Supply Chain and Cyber Directorate (SCD) is to enhance the nation's supply chain and cyber security, leveraging multidisciplinary counterintelligence and security expertise to inform, guide, and coordinate integrated risk decisions and responses with strategic partners. In October 2021, the National Counterintelligence and Security Center (NCSC) prioritized outreach efforts in five critical technology sector areas: Artificial Intelligence (AI), Bioeconomy, Autonomous Systems, Quantum, and Semiconductors. These technologies present unique opportunities and challenges where the stakes are potentially greatest for U.S. economic and national security. One of the unique challenges is managing the threats and risks to the very complex supply chains that support each one of these critical and emerging technologies. During April Supply Chain Integrity Month, NCSC focused on supply chain security issues unique to AI, specifically machine learning (ML) an AI subset; autonomous systems, specifically autonomous vehicles; and semiconductors.

Read the full article here.

U.S. ADDS SEVEN CHINA-RELATED ENTITIES TO EXPORT CONTROL LIST

Reuters | August 23, 2022

The United States has added seven China-related entities, mostly related to aerospace, to its export control list, citing national security and foreign policy concerns, according to a U.S. Commerce Department notice published online on Tuesday. According to a notification posted to the Federal Register, China Aerospace Science and Technology Corporation 9th Academy 771 Research Institute, China Aerospace Science and Technology Corporation 9th Academy 772 Research Institute, China Academy of Space Technology 502 Research Institute, China Academy of Space Technology 513 Research Institute, China Electronics Technology Group Corporation 43 Research Institute, China Electronics Technology Group Corporation 58 Research Institute, and Zhuhai Orbita Control Systems were added to the list, indicating suppliers of U.S. materials or services to these entities will need a license before shipping any goods. Commerce said the entities were added for "acquiring and attempting to acquire U.S.-origin items in support of China's military modernization efforts."

Read the full article here.

VYING FOR TALENT

The Brookings Institution and the Center for Strategic and International Studies (CSIS) | 2022

Vying for Talent is a joint Brookings-CSIS project that examines the role human talent plays in the sprawling competition between China and the United States. Through podcast interviews, reports, and public discussions with experts, this project aims to evaluate the current state of US-China competition in human capital across all its strategically relevant domains, elevate awareness in the U.S. foreign policy communities of the strategic importance of attracting and developing top global talent, and generate recommendations for strengthening the United States relative position in this core feature of future competition. The project has produced a keystone report evaluating China's human capital competitiveness, launched the Vying for Talent podcast miniseries, and convened an ongoing series of public events examining critical elements of US-China human capital competition.

Read the full article here.

DO MORE TO PREVENT CHINESE ESPIONAGE

Dustin Carmack | The Dallas Morning News | August 26, 2022

China is not a friendly competitor. It is very much a strategic threat, one that is actively working to undermine the United States and Western values of freedom and liberty. Yet too many universities and policymakers fail to recognize the danger. Many universities have been blinded by dollar signs. They pay agents to recruit international students, primarily because they will pay full tuition. China is more than happy to pay the price. Prior to the pandemic, 35% of all foreign students in the U.S. were Chinese nationals. That number has since dropped by more than half, but Chinese students still fill a disproportionately large share of seats, especially in post-graduate STEM classrooms. Innovations and technical advances generated by university-based research (along with private-sector research and development) have been a boon to U.S. security as well as our economy. But in its quest to become a global power, Beijing uses a variety of tactics — illegal as well as legal — to glean cutting-edge technology and intellectual property from university research systems, international laboratories and corporate research and development facilities. As a result, China is catching up fast. Last fall, officials at the National Counterintelligence and Security Center warned that universities, business executives and state and local officials need to do a better job of protecting their intellectual property.

Read the full article here.

SAFEGUARDING OUR FUTURE: PROTECTING GOVERNMENT AND BUSINESS LEADERS AT THE U.S. STATE AND LOCAL LEVEL FROM PEOPLE'S REPUBLIC OF CHINA (PRC) INFLUENCE OPERATIONS

The National Counterintelligence and Security Center | July 2022

For decades, a broad range of entities in China have forged ties with government and business leaders at the state and local levels of the United States, often yielding benefits for both sides. However, as tensions between Beijing and Washington have grown, the government of the People's Republic of China (PRC) under President Xi Jinping has increasingly sought to exploit these China-U.S. subnational relationships to influence U.S. policies and advance PRC geopolitical interests.[1] [2] In confronting this challenge, it is important that U.S. state and local leaders not cast blanket suspicion on all outreach from China, given that the threat of exploitation emanates from the PRC government and the Chinese Communist Party (CCP), not the people of China generally and not Chinese Americans, who themselves are often victimized by PRC aggression.[3] In partnering with any foreign entity, U.S. state and local leaders should exercise vigilance, conduct due diligence, and ensure transparency, integrity, and accountability are built into the partnership to guard against potential foreign government exploitation.

Read the full article here.

CISA: PREPARE NOW FOR QUANTUM COMPUTERS, NOT WHEN HACKERS USE THEM

Bill Toulas | Bleeping Computer | August 27, 2022

Although quantum computing is not commercially available, CISA (Cybersecurity and Infrastructure Security Agency) urges organizations to prepare for the dawn of this new age, which is expected to bring groundbreaking changes in cryptography, and how we protect our secrets. The agency published a paper earlier in the week, calling for leaders to start preparing for the migration to stronger secret guarding systems, exploring risk mitigation methods, and participating in developing new standards. Quantum computers are systems that harness quantum mechanics to perform much more powerful computations than are available today on systems that rely on binary (0, 1) computations. Experts in the field widely accept that the currently experimental quantum computers will achieve superiority over conventional systems by the end of the decade and will quickly render them obsolete with subsequent capability leaps. This is expected to revolutionize research, solve long-standing mathematical problems, perform higher-level physics simulations, and accelerate the development of artificial intelligence models.

Read the full article here.

IF COMMERCE ISN'T ADEQUATELY CONTROLLING TECH TRANSFER TO CHINA, WILL CFIUS STEP IN?

Jonathan Gafni | Linklaters | August 17, 2022

On August 16, The Wall Street Journal published an article saying the U.S. Department of Commerce in 2020 cleared 94% of export license requests for technology exports to China, with a clearance rate of 88% in 2021 (though the statistics are not directly comparable because of a change in data reporting). Explanations for the high clearance rates include: the competing internal mandates of Commerce to support U.S. exports while also implementing the U.S. government's dual-use (military/civilian) export control regime; and the risk that if U.S. businesses do not transfer the technology to China, some other country will in the absence of harmonized multilateral export controls. Commerce has slowly implemented the Export Control Reform Act of 2018 and expanded export controls referred to in the act as "emerging and foundational technologies" (now called "Section 1758 technologies" by Commerce).

Read the full article here.

IS THIS BRITISH COMPANY ARMING CHINA?

David Rose | UnHerd | August 26, 2022

By all accounts, the visit by the delegation of leading Chinese businessmen was a resounding success. Hidden away in sleepy Shropshire, Grainger and Worrall is a world-leader in the precision casting business. It prides itself on turning molten metal into complex components used in wind turbines, racing car engines, and speedboats. But not all its products are so benign. The firm also makes key parts for military drones, vehicles, and artillery; its website is illustrated with photos of RAF helicopters, Royal Navy destroyers and Army tanks. And it's with these products in mind that the team from the China North Industries Corporation, a Chinese manufacturing giant usually known as Norinco, paid a visit in 2015. The Norinco team, led by Wang Yulin, president of its Development Academy of Machinery and Equipment, and Xiaoqing Cheng, the general legal adviser to its Vehicle Research Unit, were evidently impressed. "They are a large industrial company with 300,000 employees that covers planes, trains and automobiles," Charlie Bamber, G&W's business development manager for Asia, later told the Shropshire Star.

Read the full article here.

PROTECTING YOUR ORGANIZATION'S SECRETS: SAFEGUARDING SENSITIVE AND PROPRIETARY INFORMATION FROM FOREIGN ADVERSARIES AND COMPETITORS

Office of the Director of National Intelligence | The National Counterintelligence and Security Center | January 3, 2019

You have access to facilities and computer networks, as well as sensitive information, resources, technologies, research and other data that our foreign adversaries and competitors desperately want. Our adversaries and competitors are interested in you because you have connections and access. You also have social media accounts. A work and/or personal smartphone. Social and professional networks include others in sensitive positions. You may travel, both domestically and abroad. These are all potential vulnerabilities. You may be a target. And in this fight, you matter. Phishing is a common method used to compromise computer networks and gain access to valuable information they contain. You may receive a seemingly real and plausible or official-looking email, text message, or pop-up window to lure you into clicking on a link or attachment. That action allows the attacker to bypass your network's technical defense, upload malware, or otherwise infiltrate your network and steal information. Social media provides adversaries and competitors with a platform to gain your trust.

Read the full article here.

MITRE ATT&CK®

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

View the full resource 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