ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

May 3, 2023

MANAGING UNITED STATES–CHINA UNIVERSITY RELATIONS AND RISKS

Richard Lester, Lily Tsai, Suzanne Berger, Peter Fisher, M. Taylor Fravel, David Goldston, Yasheng Huang, and Daniela Rus | Science | April 20, 2023

The intensifying geopolitical rivalry between the United States and China is clouding the outlook for cross-border academic exchange and collaboration in science and technology. Technological competition is a principal focus of this rivalry, and pressures are building in both countries to erect higher barriers to academic research collaborations and to restrict the flow of students and scholars between the two countries. A major challenge for US universities is how to manage these pressures while preserving open scientific research, open intellectual exchange, and the free flow of ideas and people. New federal regulations designed to strengthen research security on US university campuses are now being introduced. Yet federal policies, no matter how well crafted, cannot be a substitute for actions by universities themselves. We share an approach developed at the Massachusetts Institute of Technology (MIT) to make clear the lines that should not be crossed and the principles that should govern academic relations with China.

Read the full article here.

CHINA HAS WIDENED ITS ALREADY SWEEPING COUNTER-ESPIONAGE LAW. EXPERTS SAY FOREIGN BUSINESSES SHOULD BE WORRIED

Simone McCarthy and Nectar Gan | CNN | April 27, 2023

China has broadened the scope of its already sweeping counter-espionage law in a move that analysts warn could create further legal risks or uncertainty for foreign companies, journalists and academics. The changes expand the definition of espionage from covering state secrets and intelligence to any "documents, data, materials or items related to national security and interests," without specifying specific parameters for how these terms are defined. Cyber attacks targeting China's key information infrastructure in connection with spy agencies are also categorized as espionage under the new version of the law, which goes into effect on July 1. The amendment, approved by China's top legislative body Wednesday, comes amid an increasing emphasis on national security under Chinese leader Xi Jinping, the country's most assertive leader in a generation. Xi has overseen a raft of new measures to crack down on perceived threats within and outside China and sought to control the flow of information outside the country during his 10 years in power.

Read the full article here.

PROSECUTORS TELL JUDGE INFORMATION TEIXEIRA TOOK 'FAR EXCEEDS' WHAT HAS BEEN REPORTED

Hannah Rabinowitz and Evan Perez | CNN | April 27, 2023

Federal prosecutors asked a judge Wednesday to continue the detention of the Air National Guardsman accused of posting a trove of classified documents to social media, saying that he posed a flight risk and that the government was still grappling with the amount of stolen classified information. In a court filing Wednesday evening, prosecutors said that the information Jack Teixeira allegedly took "far exceeds" what has been reported, and that releasing him from jail could pose a grave threat to national security. Teixeira, prosecutors alleged, viewed hundreds of classified documents -- which the government said he may still have access to -- and conducted hundreds more keyword searches "in what appears to be a deliberate effort to disseminate this country's secrets." "The Defendant knows where the information is," prosecutors wrote. "He knows how to access it. And based on his specialized IT skills, he presumably knows how to disseminate that information without being immediately noticed."

Read the full article here.

SAFEGUARDING OUR FUTURE – VIRTUAL TELEWORK PLATFORMS: STRENGTHEN YOUR POSTURE TO GUARD YOUR DATA

The National Counterintelligence and Security Center

Greater workforce use of virtual telework platforms has broadened the virtual threat landscape, giving more opportunities for foreign intelligence entities and other malicious actors to exploit vulnerabilities to access sensitive personal, corporate, and government information. Foreign intelligence entities and other malicious actors could conduct targeted cyber operations to gain and expand access to your networks and data. They could monitor your virtual meetings in real-time, and record and archive them to collect sensitive data in the future. They could access personal and business emails, photos, chats, contacts, and financial data to try to extort you, your colleagues, or the business. They could access data giving them the ability to manipulate your business' operations, intellectual property, and market share. Communicate telework and cybersecurity policies to your workforce Use Virtual Private Networks to guarantee encrypted connections to business networks.

Read the full article here.

TRIAL REVEALS FEDERAL AGENTS FALSELY ACCUSED A UT PROFESSOR BORN IN CHINA OF SPYING

Jamie Satterfield | Knox News | June 13, 2021

Armed with a Chinese press release translated on the fly via Google, federal agents falsely accused an internationally-renown welding technology expert at the University of Tennessee at Knoxville of being a spy and brought him to professional ruin. FBI Agent Kujtim Sadiku admitted last week in an ongoing trial in Knoxville that federal agents:Falsely accused former UTK associate professor Dr. Anming Hu of being a Chinese spy. Falsely implicated him as an operative for the Chinese military in meetings with Hu's bosses. Used false information to put Hu on the federal no-fly list. Spurred U.S. customs agents to seize Hu's computer and phone and spread word throughout the international research community that Hu was poison. Used false information to justify putting a team of agents to spy on Hu and his son, a freshman at UTK, for nearly two years. Used false information to press Hu to become a spy for the U.S. government. Why?"You wanted to find a Chinese spy in Knoxville," defense attorney Phil Lomonaco offered as he cross-examined Sadiku on his tactics to secure a fraud indictment against Hu after the agency's economic espionage probe fell apart.

Read the full article here.

SEVEN CRITICAL TECHNOLOGIES FOR WINNING THE NEXT WAR

Emily Harding and Harshana Ghoorhoo | Center for Strategic and International Studies | April 2023

After an in-depth review of dozens of important emerging technologies, researchers at CSIS identified the seven technologies that are most likely to make a significant difference in the success of the United States and its allies across the spectrum of conflict over the next decade. The U.S. government should "sprint" on three critical technologies where current commercial developments are not fast enough or not tailored enough for U.S. government need: bioengineering technology; secure, redundant communications networks; and quantum technology. This sprint should include robust research in partnership with industry, investment, and innovative approaches to rapid adoption. Further, the U.S. government should "follow" in four areas: space-based sensors; miniaturized, long-lasting batteries; robotics; and artificial intelligence/machine learning. In these sectors, private investment is robust, and encouraging offshoots of commercial technology will create effective dual-use products.

Read the full article here.

EX-HARVARD PROFESSOR CHARLES LIEBER GETS HOUSE ARREST OVER CHINA TIES

Chloe Kim | BBC News | April 26, 2023

Former Harvard professor Charles Lieber was sentenced to six months of house arrest on Wednesday, according to US media. He was found guilty in 2021 of making false statements to authorities, filing false tax returns and failing to report a Chinese bank account. Critics say a US campaign to counter economic espionage from China hurts the academic community. Lieber's lawyers asked he be spared prison time because he has cancer. US District Judge Rya Zobel in Boston also sentenced him two years of supervised release and to one day in prison, which he has already served following his arrest. He must also pay a $50,000 (£40,100) fine, Bloomberg and Semafor reported. His lawyers said he was remorseful and had been punished enough because, they claimed, "his reputation has been ruined". Prosecutors recommended three months in prison, a year of probation and a $150,000 fine along with a $33,600 restitution to the Internal Revenue Service - which Lieber has already paid. Lieber was previously the head of Harvard's department of chemistry and chemical biology.

Read the full article here.

GEOFFREY HINTON TELLS US WHY HE'S NOW SCARED OF THE TECH HE HELPED BUILD

Will Douglas Heaven | MIT Technology Review | May 2, 2023

I met Geoffrey Hinton at his house on a pretty street in north London just four days before the bombshell announcement that he is quitting Google. Hinton is a pioneer of deep learning who helped develop some of the most important techniques at the heart of modern artificial intelligence, but after a decade at Google, he is stepping down to focus on new concerns he now has about AI. Stunned by the capabilities of new large language models like GPT-4, Hinton wants to raise public awareness of the serious risks that he now believes may accompany the technology he ushered in. At the start of our conversation, I took a seat at the kitchen table, and Hinton started pacing. Plagued for years by chronic back pain, Hinton almost never sits down. For the next hour I watched him walk from one end of the room to the other, my head swiveling as he spoke. And he had plenty to say. The 75-year-old computer scientist, who was a joint recipient with Yann LeCun and Yoshua Bengio of the 2018 Turing Award for his work on deep learning, says he is ready to shift gears. "I'm getting too old to do technical work that requires remembering lots of details," he told me. "I'm still okay, but I'm not nearly as good as I was, and that's annoying."

Read the full article here.

COMPLIANCE REQUIREMENTS FOR HANDLING CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Marissa Sims | Winvale | February 22, 2023

As a government contractor, you have to stay vigilant about certain regulations so you are staying within the guidelines of the federal government. However, it's not always an easy guidebook to follow. Some contractors are subject to additional policies if they handle certain types of information. If you are a government contractor within the Defense Industrial Base (DIB), or you handle Controlled Unclassified Information (CUI), there are certain regulations and clauses you have to follow. Here's what you need to know about the security requirements for safeguarding CUI. Controlled Unclassified Information (CUI) is defined as unclassified information that requires safeguarding and distribution controls in accordance with law, regulation, or governmentwide policy. The protection of CUI is extremely important because it directly impacts privacy and security concerns. The Department of Defense (DoD) wanted to standardize the protection of CUI which drove the development of the National Institute of Standards and Technology (NIST) SP 800-171. NIST SP 800-171 was published as a supplement to the DFARS, or the Defense Federal Acquisition Regulation Supplement.

Read the full article here.

UNDERSTANDING OPSEC FROM AN ORGANIZATIONAL PERSPECTIVE

National Counterintelligence and Security Center | The National Operations Security Program (NOP) Office January 2023

National Operations Security (OPSEC) Awareness Month is an opportunity for individuals, government agencies, and private sector entities to reflect on ways to mitigate risks to their organizations. OPSEC is a systematic and proven process for denying adversaries access to information about an organization's capabilities and intentions. An OPSEC program should be codified within an organization and remain ongoing to adequately protect data that can be leveraged by those seeking to harm an organization. The first step in establishing an OPSEC program is acknowledging that adversarial threats to the organization exist. Every organization faces potential adversarial threats, whether they come in the form of crime, foreign espionage, terrorism, or subversion. Ransomware delivered by cybercriminals, sabotage conducted by insiders, theft of intellectual property by agents of a foreign intelligence service, or physical destruction of facilities by foreign or domestic terrorists are all examples of threats that can be mitigated through OPSEC.

Read the full article here.

THE UNTOLD STORY OF THE BOLDEST SUPPLY-CHAIN HACK EVER

Kim Zetter | Wired | May 2, 2023

The attackers were in thousands of corporate and government networks. They might still be there now. Behind the scenes of the SolarWinds investigation. Steven Adair wasn't too rattled at first. It was late 2019, and Adair, the president of the security firm Volexity, was investigating a digital security breach at an American think tank. The intrusion was nothing special. Adair figured he and his team would rout the attackers quickly and be done with the case—until they noticed something strange. A second group of hackers was active in the think tank's network. They were going after email, making copies and sending them to an outside server. These intruders were much more skilled, and they were returning to the network several times a week to siphon correspondence from specific executives, policy wonks, and IT staff. Adair and his colleagues dubbed the second gang of thieves "Dark Halo" and booted them from the network. But soon they were back.

Read the full article here.

CHINA LOCKS INFORMATION ON THE COUNTRY INSIDE A BLACK BOX

Lingling Wei, Yoko Kubota, and Dan Strumpf | The Wall Street Journal | April 30, 2023

China's party-state, long steeped in secrecy, is creating a black box around information on the world's second-largest economy, alarming global businesses and investors. Prodded by President Xi Jinping's emphasis on national security, authorities in recent months have restricted or outright cut off overseas access to various databases involving corporate-registration information, patents, procurement documents, academic journals and official statistical yearbooks. Of extra concern in recent days: Access to one of the most crucial databases on China, Shanghai-based Wind Information Co., whose economic and financial data are widely used by analysts and investors both inside and outside the country, appears to be drying up. Following recent expansion of China's anti-espionage law, aimed at fighting perceived foreign threats, many foreign think tanks, research firms and other nonfinancial entities are finding they can't renew subscriptions to Wind over what Wind described as "compliance" issues, according to interviews with Western researchers and macroeconomic analysts. A Wind service representative said in an email response that customers who want to renew their contracts need to contact their account managers.

Read the full article here.

WHY COUNTRIES ARE TRYING TO BAN TIKTOK

Sapna Maheshwari and Amanda Holpuch | The New York Times | April 26, 2023

In recent months, lawmakers in the United States, Europe and Canada have escalated efforts to restrict access to TikTok, the massively popular short-form video app that is owned by the Chinese company ByteDance, citing security threats. The White House told federal agencies on Feb. 27 that they had 30 days to delete the app from government devices. A growing number of other countries and government bodies — including Britain and its Parliament, Canada, the executive arm of the European Union, France and New Zealand's Parliament — have also recently banned the app from official devices. On April 4, Australia became the latest country to announce that it was prohibiting the TikTok app on government devices on advice from intelligence and security agencies. On March 1, a House committee backed an even more extreme step, voting to advance legislation that would allow President Biden to ban TikTok from all devices nationwide. On March 23, TikTok's chief executive, Shou Chew, was grilled about the app's relationship to its parent company and China's potential influence over the platform in roughly five hours of testimony before the House Energy and Commerce Committee.

Read the full article here.

CONTROLLED UNCLASSIFIED INFORMATION (CUI) TOOLKIT

Center for Development of Security Excellence | Defense Counterintelligence and Security Agency

What is Controlled Unclassified Information? Controlled Unclassified Information (CUI) is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and Government-wide policies but is not classified under Executive Order 13526 "Classified National Security Information" or the Atomic Energy Act, as amended. Components must ensure their personnel receive initial and annual refresher CUI education and training, and maintain documentation of this training for audit purposes. We provide a mandatory training course for all DOD personnel with access to CUI. This course also fulfills CUI training requirements for industry when it is required by Government Contracting Activities for contracts with CUI requirements. Refer to the "Training & Education" section on this page for the link to the "DOD Mandatory Controlled Unclassified Information (CUI) Training" course. Report DoD Component training completion data to the USD(I&S) annually or as directed.

Read the full article here.