ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

June 29, 2023

UNIVERSITY AND FEDERAL ACTIONS TAKEN TO ADDRESS RESEARCH SECURITY ISSUES

Association of American Universities | March 31, 2023

Congress is currently considering several measures related to securing federally funded research data and intellectual property at universities and other research institutions in the United States. As lawmakers consider these measures, it is important to understand the current state of play for research security in the country to avoid new requirements that are duplicative, unnecessary, or counterproductive. This document summarizes actions that have already been taken or are currently being taken by both universities and federal entities regarding research security.

Read the full article here.

DOJ LAUNCHES CYBER UNIT WITH NATIONAL SECURITY FOCUS AS CHINA, RUSSIA THREATS MOUNT

Rohan Goswami | CNBC | June 20, 2023

The U.S. Department of Justice announced Tuesday a new unit within its National Security Division focused on pursuing cyber threats from nation-state and state-backed hackers, formalizing an increasingly significant part of the national security apparatus into the Justice Department's hierarchy. In a statement, Assistant Attorney General Matt Olsen said the new unit would allow the DOJ's national security team "to increase the scale and speed of disruption campaigns and prosecutions of nation-state threat actors, state-sponsored cybercriminals, associated money launderers, and other cyber-enabled threats to national security." The DOJ has aggressively pursued state-backed cyber actors, especially those in China or North Korea. National security officials outside the DOJ have also emphasized China as a top cybersecurity concern, including the U.S.' top cybersecurity official. The announcement made no mention of Chinese cyber efforts, which CISA Director Jen Easterly described last week as an "epoch-defining threat." But in a separate event Tuesday at the Hoover Institution at Stanford University, Olsen emphasized the work that the DOJ has been doing to combat Chinese cyber efforts. "China has compromised telecommunications firms," Olsen said at the event. "It conducts cyber intrusions targeting journalists and dissidents in order to suppress the free flow of information. And the PRC is capable of launching cyberattacks that could disrupt U.S. critical infrastructure."

Read the full article here.

RESTRICTING TIKTOK (PART I): LEGAL HISTORY AND BACKGROUND

Stephen P. Mulligan | Congressional Research Service (CRS) | June 22, 2023

The video-sharing platform TikTok has experienced a dramatic rise in users in the United States in recent years, while at the same time some Members of Congress and Biden Administration officials have described the application (app) as a national security threat. During the Trump Administration, concerns about TikTok's data security and connections to the People's Republic of China (PRC) led to the attempt to restrict the app's U.S. operations. In decisions that inform the current legislative debate, two federal district courts concluded that aspects of the restrictions were unlawful because they exceeded the President's statutory authority. Other elements of the Trump Administration's efforts are ongoing and have been continued by the Biden Administration. This Sidebar discusses these past executive branch-led efforts.

Read the full article here.

CHINA IS READY FOR A WORLD OF DISORDER AMERICA IS NOT

Mark Leonard | Foreign Affairs | June 20, 2023

In March, at the end of Chinese President Xi Jinping's visit to Moscow, Russian President Vladimir Putin stood at the door of the Kremlin to bid his friend farewell. Xi told his Russian counterpart, "Right now, there are changes—the likes of which we haven't seen for 100 years—and we are the ones driving these changes together." Putin, smiling, responded, "I agree." The tone was informal, but this was hardly an impromptu exchange: "Changes unseen in a century" has become one of Xi's favorite slogans since he coined it in December 2017. Although it might seem generic, it neatly encapsulates the contemporary Chinese way of thinking about the emerging global order—or, rather, disorder. As China's power has grown, Western policymakers and analysts have tried to determine what kind of world China wants and what kind of global order Beijing aims to build with its power.

Read the full article here.

INSIDE CHINA'S SPY WAR ON AMERICAN CORPORATIONS

Eamon Javers | CNBC | June 21, 2023

Top intelligence and law enforcement officials in Washington are issuing a stark warning to American companies: The Chinese government wants to replace you. That message comes in a new CNBC documentary, "China's Corporate Spy War," which details the increasing sophistication of Beijing's efforts to steal sensitive U.S. technology and corporate information. For years, corporate America largely saw theft by the Chinese government and state-run companies as an attempt to catch up with advanced U.S. technology. But officials now say the effort is more nefarious than generally understood, viewing — in many cases — an adversary that wants to eliminate the American companies they are targeting, not just narrow the gap between Chinese firms and their U.S. competition. Asked whether the Chinese government wants to compete with or eliminate American companies, FBI Director Christopher Wray told CNBC: "Well, their definition of competing, I think, involves embracing the idea of eliminating."

Read the full article here.

US URGES GLOBAL COALITION AGAINST CHINA'S TECH CYBERTHEFT "PLAYBOOK"

Rob Thubron | TechSpot | June 23, 2023

China's IP theft is helping it race ahead in AI and cloud technologies
What just happened? Not for the first time, a US official has accused China of stealing intellectual property to gain an advantage in key technologies such as artificial intelligence and cloud computing. Nathaniel Fick, ambassador at large for Cyberspace and Digital Policy, said the US and other countries should form a coalition to stop China's cybertheft. Fick said that China executed a deliberate strategy of IP theft and government subsidies decades ago after noticing the global advantage in telecoms that big companies gave democratic nations. China, of course, denies any wrongdoing. "I don't think we appreciated or acted on the reality that these technologies were going to be central to our geopolitical standing," Fick said during an event hosted by think tank Hudson Institute (via The Reg). Fick added that stealing core intellectual property allowed China to start building the next generation wireless networks and subsidize Huawei and ZTE around the world to do deals at less competitive terms. He called China's actions a "playbook."

Read the full article here.

STEALTHY USB: NEW VERSIONS OF CHINESE ESPIONAGE MALWARE PROPAGATING THROUGH USB DEVICES FOUND BY CHECK POINT RESEARCH

Check Point Team | Check Point Blog | June 22, 2023

Executive Summary
In a recent incident at a healthcare institution in Europe, the Check Point Incident Response Team (CPIRT) uncovered a disturbing malware attack. This incident shed light on the activities of Camaro Dragon, a Chinese-based espionage threat actor also known as Mustang Panda and LuminousMoth. While their primary focus has traditionally been Southeast Asian countries, this latest discovery reveals their global reach and highlights the alarming role USB drives play in spreading malware. The Uninvited Guest: Malware Sneaks in Through USB Drives: The healthcare institution fell victim to malware that infiltrated their systems through an infected USB drive.

Read the full article here.

THE CHINESE (AND RUSSIAN, AND NORTH KOREAN) SPIES AMONG US

Michele McPhee | Los Angeles Magazine | June 21, 2023

How California became a hub of espionage
Five years ago, back when Dianne Feinstein was still a relatively vigorous political figure, she gave a little speech at a Judiciary Committee hearing on Chinese spying in the United States. "Today's hearing will examine other more nontraditional forms of espionage," the veteran senator from California began her remarks, listing some of the numerous ways the People's Republic had been snooping on the American continent, including planting its own scientists at top U.S. universities and luring U.S. companies into revealing their source codes and other confidential information by promising lucrative openings to Chinese markets. "The Chinese government has deliberately and pur-posefully created a system of maximum information extraction at nearly every level in every sector of the United States economy," she warned. "Many of these efforts occur in plain sight."

Read the full article here.

WHEN CHINESE AND US SCIENTISTS COLLABORATE, GREAT THINGS HAPPEN

Enda Curran | Bloomberg | June 21, 2023

Too bad government relations make it tricky. Plus: A new way to unlock history's secrets.
When searching for a word to describe the relationship between the US and China, "cooperative" doesn't really come to mind. According to a new paper, that's a mistake. In their analysis of thousands of science reports, co-authors Qingnan Xie of Harvard University and Richard Freeman, also of Harvard and the National Bureau of Economic Research, found that when researchers from the two countries worked together, great things happened. They focused on China-born researchers who work in the US (known as diaspora) and those who returned to China (returnee).

Read the full article here.

SAFEGUARDING RESEARCH IN CANADA: A GUIDE FOR UNIVERSITY POLICIES AND PRACTICES

U15 Group of Canadian Research Universities | June 22, 2023

A defining characteristic of Canada's university system is its openness to the world. Global engagement is indispensable to the success of our top research-intensive universities, their competitiveness on the world stage, and their ability to enhance the quality of life of Canadians through learning, discovery, and community service. As stated by the Chief Science Advisor of Canada in describing open science, the practice of sharing data, information tools, and research results while also eliminating barriers to collaboration, accelerates discovery and encourages transparency, scientific integrity and professional accountability. A second defining characteristic of Canada's leading universities is their commitment to ensuring the responsible conduct of research and research integrity. Over many years, Canadian universities have developed robust policies and practices that guide how research should be conducted throughout the life cycle of each project in keeping with the highest standards of honesty, fairness, trust, accountability, and openness.

Read the full article here.

ENUMERATING, TARGETING AND COLLAPSING THE CHINESE COMMUNIST PARTY'S NEUROSTRIKE PROGRAM

Ryan Clarke, Xiaoxu Sean Lin, LJ Eads | The CCP BioThreats Initiative

Aggregating Intelligence Fragments and The Power of Network Graphs
Unknown to many, the Chinese Communist Party (CCP) and its People's Liberation Army (PLA) have established themselves as world leaders in the development of NeuroStrike weapons. These platforms directly attack, or even control, mammalian brains (including humans) with microwave/directed energy weapons via standalone platforms (i.e., handheld gun) or the broader electromagnetic spectrum.
1 NeuroStrike, as defined by McCreight, refers to the engineered targeting of warfighter and civilian brains using distinct non-kinetic technology to impair cognition, reduce situational awareness, inflict long term neurological degradation and fog normal cognitive functions.
2 The CCP views NeuroStrike and psychological warfare as a core component of its asymmetric warfare strategy against the United States and its Allies in the Indo-Pacific.

Read the full article here.

TRAVELING OVERSEAS WITH MOBILE PHONES, LAPTOPS, PDAS, AND OTHER ELECTRONIC DEVICES

Office of the Director of National Intelligence

YOU SHOULD KNOW

For general travel alerts and information, see the Department of State Site. http://travel.state.gov/content/passports/en/alertswarnings.html.

- In most countries you have no expectation of privacy in Internet cafes, hotels, offices, or public places. Hotel business centers and phone networks are regularly monitored in many countries. In some countries, hotel rooms are often searched.
- All information you send electronically – by fax machine, personal digital assistant (PDA), computer, or telephone – can be intercepted. Wireless devices are especially vulnerable.
- Security services and criminals can track your movements using your mobile phone or PDA and can turn on the microphone in your device even when you think it's off. To prevent this, remove the battery.
- Security services and criminals can also insert malicious software into your device through any connection they control. They can also do it wirelessly if your device is enabled for wireless. When you connect to your home server, the "malware" can migrate to your business, agency, or home system, can inventory your system, and can send information back to the security service or potential malicious actor.
- Malware can also be transferred to your device through thumb drives (USB sticks), computer disks, and other "gifts."
- Transmitting sensitive government, personal, or proprietary information from abroad is therefore risky.
- Corporate and government officials are most at risk, but don't assume you're too insignificant to be targeted.
- Foreign security services and criminals are adept at "phishing" – that is, pretending to be someone you trust in order to obtain personal or sensitive information.
- If a customs official demands to examine your device, or if your hotel room is searched while the device is in the room and you're not, you should assume the device's hard drive has been copied.

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