ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

February 2, 2022

FORMER U.S. SECURITY OFFICIALS URGE CONGRESS TO ACT ON CHINA LEGISLATION

Michael Martina | Reuters | February 1, 2022

More than a dozen former senior U.S. national security officials have pressed congressional leaders to quickly pass legislation to boost technology funding, calling it "critical" to compete against China. A letter signed by 16 officials from past Democratic and Republican administrations - including Leon Panetta, who served as defense secretary under President Barack Obama, and President George W. Bush's national security advisor Stephen Hadley - said the legislation would "ensure the U.S. stays on the cutting-edge of microelectronics." The Senate passed the U.S. Innovation and Competition Act last year, including $52 billion for the semiconductor industry and authorizing $190 billion to strengthen U.S. technology and research to compete with China. The House of Representatives began considering its "America Competes" act this week. If it passes, the two chambers will have to resolve differences with the Senate bill. "This is the time to prioritize comprehensive, bipartisan competitiveness legislation, which will ensure that federal investment matches our national security interests and allows the United States to maintain strengths and comparative advantages against rising adversaries," the officials wrote in the letter dated Feb. 1, seen by Reuters.

Read the full article here.

WHITE HOUSE CALLS FOR CONSISTENT RULES FOR DISCLOSING FOREIGN RESEARCH FUNDING

Jeffrey Mervis | Science | January 10, 2022

President Joe Biden's administration last week ordered federal agencies to draft uniform policies describing the outside sources of funding that scientists must disclose when they apply for federal grants, and the penalties for failing to do so. Research groups welcome the directive, but wish it had also specified what kinds of foreign collaborations might get a scientist in trouble. The new directive, issued on 4 January by the White House Office of Science and Technology Policy (OSTP), feeds into a roiling political debate about how to protect federally funded research from attempted theft by some foreign governments. In recent years, the federal government has prosecuted some two dozen academics for failing to disclose financial ties to China, which critics say has criminalized minor violations of often confusing federal rules and chilled research collaborations. The 34-page OSTP memo fleshes out a proposal to improve research security issued 1 year ago, in the final days of then-President Donald Trump's administration, as well as a recent congressional mandate with the same goal.

Read the full article here.

FBI DIRECTOR SAYS THE THREAT FROM CHINA IS 'MORE BRAZEN' THAN EVER BEFORE

Eric Tucker | NPR | January 31, 2022

The threat to the West from the Chinese government is "more brazen" and damaging than ever before, FBI Director Christopher Wray said Monday night in accusing Beijing of stealing American ideas and innovation and launching massive hacking operations. The speech at the Reagan Presidential Library amounted to a stinging rebuke of the Chinese government just days before Beijing is set to occupy the global stage by hosting the Winter Olympics. It made clear that even as American foreign policy remains consumed by Russia-Ukraine tensions, the U.S. continues to regard China as its biggest threat to long-term economic security. "When we tally up what we see in our investigations, over 2,000 of which are focused on the Chinese government trying to steal our information or technology, there's just no country that presents a broader threat to our ideas, innovation, and economic security than China," Wray said, according to a copy of the speech provided by the FBI. The bureau is opening new cases to counter Chinese intelligence operations every 12 hours or so, Wray said, with Chinese government hackers pilfering more personal and corporate data than all other countries combined. "The harm from the Chinese government's economic espionage isn't just that its companies pull ahead based on illegally gotten technology. While they pull ahead, they push our companies and workers behind," Wray said.

Read the full article here.

TACKLING R&I FOREIGN INTERFERENCE

Publications Office of the European Union | January 18, 2022

This publication presents the Staff Working Document on tackling R&I foreign interference. Foreign interference occurs when activities are carried out by, or on behalf of, a foreign state-level actor, which are coercive, covert, deceptive, or corrupting and are contrary to the sovereignty, values, and interests of the European Union (EU). EU Higher Education Institutions (HEIs) and Research Performing Organisations (RPOs) can benefit from a comprehensive strategy for tackling foreign interference that covers key areas of attention grouped into the following four categories: values, governance, partnerships and cybersecurity. The document contains a nonexhaustive list of possible mitigation measures that can help HEIs and RPOs to develop a comprehensive strategy, tailored to their needs.

Read the full article here.

NORTH KOREAN HACKERS USING WINDOWS UPDATE SERVICE TO INFECT PCS WITH MALWARE

Ravie Lakshmanan | The Hacker News | January 28, 2022

The notorious Lazarus Group actor has been observed mounting a new campaign that makes use of the Windows Update service to execute its malicious payload, expanding the arsenal of living-off-the-land (LotL) techniques leveraged by the APT group to further its objectives. The Lazarus Group, also known as APT38, Hidden Cobra, Whois Hacking Team, and Zinc, is the moniker assigned to the North Korea-based nation-state hacking group that's been active since at least 2009. Last year, the threat actor was linked to an elaborate social engineering campaign targeting security researchers. The latest spear-phishing attacks, which Malwarebytes detected on January 18, originate from weaponized documents with job-themed lures impersonating the American global security and aerospace company Lockheed Martin. Opening the decoy Microsoft Word file triggers the execution of a malicious macro embedded within the document that, in turn, executes a Base64-decoded shellcode to inject a number of malware components into the explorer.exe process.

Read the full article here.

WHY A HIGH-PROFILE CHINA INITIATIVE CASE COLLAPSED

Jeffrey Mervis | Science | January 25, 2022

For the past year, the U.S. government had argued that Massachusetts Institute of Technology (MIT) engineering professor Gang Chen broke the law by failing to disclose his ties to China when applying for a grant from the Department of Energy (DOE). But last week, prosecutors abruptly reversed course and dropped all charges against him, telling a federal court on 20 January that the government "can no longer meet its burden of proof at trial." How did prosecutors get it so wrong? Chen's case was one of the highest profile prosecutions of an academic scientist brought under the China Initiative, a controversial government effort to prevent China from stealing federally funded research that has ensnared some two dozen university researchers. Last month, in another prominent case, a jury convicted Harvard University chemist Charles Lieber of failing to disclose his financial ties to China to federal agencies. But Chen's case never made it to a jury.

Read the full article here.

IRANIAN HACKERS USING NEW POWERSHELL BACKDOOR IN CYBER ESPIONAGE ATTACKS

Ravie Lakshmanan | The Hacker News | February 1, 2022

An advanced persistent threat group with links to Iran has updated its malware toolset to include a novel PowerShell-based implant called PowerLess Backdoor, according to new research published by Cybereason. The Boston-headquartered cybersecurity company attributed the malware to a hacking group known as Charming Kitten (aka Phosphorous, APT35, or TA453), while also calling out the backdoor's evasive PowerShell execution. "The PowerShell code runs in the context of a .NET application, thus not launching 'powershell.exe' which enables it to evade security products," Daniel Frank, senior malware researcher at Cybereason, said. "The toolset analyzed includes extremely modular, multi-staged malware that decrypts and deploys additional payloads in several stages for the sake of both stealth and efficacy." The threat actor, which is active since at least 2017, has been behind a series of campaigns in recent years, including those wherein the adversary posed as journalists and scholars to deceive targets into installing malware and stealing classified information.

Read the full article here.

JUDGE LIMITS TESTIMONY AT TRIAL OF PROFESSOR ACCUSED OF HIDING CHINESE TIES

Josh Gerstein | Politico | January 27, 2022

A judge handling a criminal case against a University of Kansas professor born in China faulted federal prosecutors' plans for the looming trial, saying their intended approach could fan anti-Chinese sentiment and prejudice the defendant's right to a fair trial. U.S. District Court Judge Julie Robinson made the provocative comments in an order Thursday denying the prosecution's request to have an expert witness at the trial of Feng Tao, a chemistry professor, testify about China's efforts to gather U.S. technology secrets. Tao, who has pleaded not guilty, is accused of failing to disclose his ties to a Chinese government talent recruitment program. "This testimony … poses a significant risk of stoking Sinophobia — especially given that [the] Defendant, who is Chinese, faces trial amid increasing reports of anti-Asian discrimination and violence since the outbreak of the COVID-19 pandemic — and evoking exactly the kind of negative emotional response that might 'lure the [jury] into declaring guilt on a ground different from proof specific to the offense charged,'" Robinson wrote. "Whether a purpose of his scheme was to benefit the [People's Republic of China] is irrelevant."

Read the full article here.

BIDEN'S CHINA POLICY NEEDS TO BE MORE THAN JUST TRUMP LITE

Jeffrey A. Bader | Brookings | January 25, 2022

The Biden administration has prided itself on breaking with the policies and practices of its predecessor, which did untold damage to U.S. foreign policy and domestic tranquility. But curiously, when it comes to the greatest foreign policy challenge facing the United States — how to deal with the rise of China — Biden's team have continued and mimicked Trump's destructive approach. This has prompted glee among departed Trump officials, who proudly declare themselves innovators and the Biden administration unimaginative and dutiful implementers. Biden officials begin their defense of their China policy by citing supposed strong bipartisan support for their tough line. When asked to distinguish their China strategy from their predecessor's, they say little more than that they favor a multilateral approach of rallying allies, in contrast to the unilateralism of the "America First" practitioners. Yet, it is intellectual laziness to justify policy on the basis of bipartisanship rather than formulate one based on national interests. In no other instance, e.g. policy toward Iran, Ukraine and Russia, NATO and the EU, has the administration sought to duplicate Trump policy.

Read the full article here.

COUNTERING THREATS POSED BY THE CHINESE GOVERNMENT INSIDE THE U.S. – REMARKS AS DELIVERED

Christopher Wray | U.S. Department of Justice Federal Bureau of Investigation | January 31, 2022

Well, thank you, John. And I have to say, I'm honored to be here with you at the Ronald Reagan Presidential Library. The years of President Reagan's administration were momentous ones, defined, in large part, by our struggle against the Soviet Union, whose empire, where freedoms we hold dear were snuffed out. I'm sure everyone here is familiar with President Reagan's speech at the Brandenburg Gate in June 1987, when he called out Mr. Gorbachev by name and challenged him to "tear down this wall" between free West Berlin and imprisoned East Germany—a nightmare surveillance state, where no personal information was off limits to the government. The FBI was deeply engaged in that struggle, tracking Soviet agents operating here in the United States and protecting our freedoms from a dangerous enemy. That era and that work are a huge part of the FBI's legacy and history—a history that the library has captured so well in this exhibit.

Read the full article here.

PHYSICISTS DISCOVER 'SECRET SAUCE' BEHIND EXOTIC PROPERTIES OF NEW QUANTUM MATERIAL

Elizabeth A. Thomson | MIT Physics | January 13, 2022

MIT physicists and colleagues have discovered the "secret sauce" behind some of the exotic properties of a new quantum material that has transfixed physicists due to those properties, which include superconductivity. Although theorists had predicted the reason for the unusual properties of the material, known as a kagome metal, this is the first time that the phenomenon behind those properties has been observed in the laboratory. "The hope is that our new understanding of the electronic structure of a kagome metal will help us build a rich platform for discovering other quantum materials," says Riccardo Comin, the Class of 1947 Career Development Assistant Professor of Physics at MIT, whose group led the study. That, in turn, could lead to a new class of superconductors, new approaches to quantum computing, and other quantum technologies. The work is reported in the January 13, 2022 online issue of the journal Nature Physics. Classical physics can be used to explain any number of phenomena that underlie our world—until things get exquisitely small.

Read the full article here.

PROTECTING PERSONAL HEALTH DATA FROM FOREIGN EXPLOITATION

The National Counterintelligence and Security Center | January 31, 2022

Foreign companies and some U.S. businesses with facilities abroad have been partnering or contracting with U.S. organizations to provide diagnostic tests and services that in some cases collect specimens, DNA, fitness / lifestyle information, or other personal health data from patients or consumers in the United States. Some of these companies may be subject to foreign laws that can compel them to share such data with foreign governments, including governments that exploit personal health data for their own ends and without regard to individual privacy. For example, several Chinese companies have partnered or contracted with U.S. organizations and are accredited, certified, or licensed to perform genetic testing or whole-genome sequencing on patients in the U.S. healthcare system, potentially giving them direct access to the genetic data of patients in the United States. Chinese companies are compelled to share data with the government of the People's Republic of China, which has used genetic data for state surveillance and repression of its ethnic and religious minorities, as well as for military research and applications.

Read the full article here.

EU ISSUES GUIDELINES ON FOREIGN INTERFERENCE IN RESEARCH

Florin Zubașcu | Science|Business | January 18, 2022

The European Commission has published today a guidebook advising national research organisations and universities on how to deal with foreign interference, as fears over technology espionage from China are heightened and the western world collectively takes a more cautious approach to science cooperation. The guidelines will help the EU protect its "fundamental values, key research findings and intellectual assets," EU research commissioner Maryia Gabriel said. A senior Commission official put it more bluntly in a briefing on the guidelines, saying they will help research institutions to block "actions that could put in danger the technological leadership and sovereignty of Europe." The Commission recently morphed its motto for international research cooperation from "Open to the world" to "Open strategic autonomy", as part of a reset that has seen it limit access to EU funding for scientists in countries that flout academic freedom and intellectual property rights.

Read the full article here.

CCP'S USE OF OVERSEAS CHINESE TO INFLUENCE WESTERN DEMOCRACIES

Kalpit A Mankikar | Observer Research Foundation | January 29, 2022

Overseas Chinese have always had a unique relationship with China's rulers since its imperial past. Since the Communist takeover in 1949, the party-state has sought to co-opt ethnic Chinese settled abroad through the United Front Work Department (UFWD). Now, Xi Jinping is weaponising overseas Chinese on an industrial scale, and its reverberations are being felt in western democracies. A senior British politician has been accused of accepting funds from an individual with links to the Chinese Communist Party (CCP). Christine Ching Kui Lee's law firm, Christine Lee & Co, was said to be channeling money to the office of Labour MP Barry Gardiner—who had been bestowed with the Padma Shri award by the Indian government in 2020—and her son was hired in the parliamentarian's office in Westminster—the heart of the British government—to manage the politician's appointments. Lee's firm was the chief legal adviser to the Chinese embassy in London; and at the same time the British government's Department of International Trade directed foreign businesspeople keen to invest in UK to seek Lee's legal-advisory services. Lee has been active in UK's public life for some time, cultivating the Westminster elite.

Read the full article here.

HIGHER EDUCATION R&D INCREASE OF 3.3% IN FY 2020 IS THE LOWEST SINCE FY 2015

Michael T. Gibbons | National Center for Science and Engineering Statistics | December 27, 2021

Research and development spending by academic institutions totaled $86.4 billion in FY 2020, an increase of $2.7 billion (3.3%) from FY 2019. This was the slowest growth since the 4 years of decreasing federal funding from FY 2012 to FY 2015. Despite the recent year's slower growth, due in part to the COVID-19 pandemic (see "R&D Disruptions Due to the Pandemic"), R&D expenditures funded from federal sources and institutions' own funds rose annually in both current and constant dollars from FY 2016 to FY 2020 (figure 1 and table 1). R&D funded by all other nonfederal sources increased in current dollars from FY 2019 to FY 2020 but were unchanged in constant dollars. The data discussed in this report are from the Higher Education Research and Development (HERD) Survey, sponsored by the National Center for Science and Engineering Statistics (NCSES) within the National Science Foundation. For more information on the survey, see "Data Sources, Limitations, and Availability."

Read the full article here.