ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

January 4, 2023

U.S. SLAPS RESTRICTIONS ON CHINESE CHIPMAKER AND OTHER COMPANIES OVER NATIONAL SECURITY WORRIES

Kevin Breuninger | CNBC | December 15, 2022

The Biden administration said Thursday it was "severely" restricting dozens of mostly Chinese organizations, including at least one chipmaker, over their efforts to use advanced technologies to help modernize China's military. The 36 entities will face "stringent license requirements" that hamper their access to certain U.S.-produced commodities, software, and technologies — including artificial intelligence and advanced computing, the Commerce Department's Bureau of Industry and Security said in a press release. The Bureau's latest action comes more than two months after the Biden administration imposed new curbs on China's access to advanced semiconductors. The new designations also take aim at Russia-linked entities supporting that country's military invasion of Ukraine, the agency said. The actions will protect U.S. national security by squelching Beijing's ability to "leverage artificial intelligence, advanced computing, and other powerful, commercially available technologies for military modernization and human rights abuses," Alan Estevez, undersecretary of Commerce for Industry and Security, said in the press release.

Read the full article here.

CISA RESEARCHERS: RUSSIA'S FANCY BEAR INFILTRATED US SATELLITE NETWORK

Christian Vasquez | CyberScoop | December 16, 2022

Researchers at the Cybersecurity and Infrastructure Security Agency recently discovered suspected Russian hackers lurking inside a U.S. satellite network, raising fresh concerns about Moscow's intentions to infiltrate and disrupt the rapidly expanding space economy. While details of the attack are scant, researchers blamed the incident on the Russian military group known as Fancy Bear, or APT28. It involved a satellite communications provider with customers in U.S. critical infrastructure sectors. Responding to a tip about suspicious network behavior, CISA researchers found hackers inside the satellite network earlier this year. MJ Emanuel, a CISA incident response analyst who discussed the incident at the CYBERWARCON cybersecurity conference last month, said it appeared that Fancy Bear was in the victim's networks for months. Space security is a growing global concern, especially as key industries and militaries around the world increasingly rely on satellites for vital communications, GPS and internet access. A cyberattack against the U.S. telecom company Viasat, which provides internet service in Europe, disrupted internet service in Ukraine just before the Russian invasion in February.

Read the full article here.

UPDATES ON RESEARCH SECURITY POLICIES AND PRACTICES IN THE U.S. GOVERNMENT

Executive Office of the President | Office of Science and Technology Policy | October 2022

The primary purpose of NSPM-33 (National Security Presidential Memorandum) is to strengthen protections of U.S. government-supported research while maintaining an open environment in which to foster research discoveries and innovation. Practical application of NSPM-33 includes developing a series of actions for Federal research funding agencies, emphasizing standardized policies for disclosures, and supporting transparency, researcher responsibility, and training for Federal researchers and those funded by Federal taxpayer dollars, especially through research security programs. NSPM-33 implementation guidance goals are to reaffirm core values of openness, transparency, honesty, equity, fair competition, objectivity, and democratic values, acknowledge the seriousness of the challenge, communicate and apply policies in a clear and uniform way, and continue welcoming international students, scholars, and collaborations.

Read the full article here.

'A SEA CHANGE': BIDEN REVERSES DECADES OF CHINESE TRADE POLICY

Gavin Bade | Politico | December 26, 2022

After decades of U.S. efforts to engage China with the prospect of greater development through trade, the era of cooperation is coming to a screeching halt. The White House and Congress are quietly reshaping the American economic relationship with the world's second-largest economic power, enacting a strategy to limit China's technological development that breaks with decades of federal policy and represents the most aggressive American action yet to curtail Beijing's economic and military rise. The new federal rules, executive orders and pending legislation aimed at China's high-tech sectors, which began this fall and will continue in 2023, are the culmination of years of debate spanning three administrations. Taken together, they represent an escalation of former President Donald Trump's tariffs and trade disputes against Beijing that could ultimately do more to slow Chinese technological and economic development — and divide the two economies — than anything the 45th president did while in office. "You really have seen a sea change in the way that they're looking at the relationship with China," said Clete Willems.

Read the full article here.

PENTAGON'S CMMC PROGRAM LAUNCH FACES DELAY AS OMB RULEMAKING REVIEW SHIFTS TO JANUARY

Sara Friedman | Inside Cybersecurity | December 21, 2022

The Pentagon is planning to submit the first rulemaking under its cyber certification program in January for review by the Office of Management and Budget, according to a Defense Department spokeswoman, shifting the official launch timeframe farther down the road than previously expected. The Defense Department is in the process of making changes to its Cybersecurity Maturity Model Certification program following an internal review in 2021. There will be two rulemakings, according to a 2021 notice posted in the Federal Register. The first rule will change Title 32 of the Code of Federal Regulations, followed by an update to the 2020 interim final rule that amended Title 48 of the CFR and put in place regulations for the initial CMMC program. CMMC director Stacy Bostjanick announced earlier this year that the 32 CFR rule would be sent over to OMB's Office of Information and Regulatory Affairs in July. The expectation was to release an interim final rule in March 2023 with a 60-day public comment period and CMMC requirements to start in showing up in DOD contracts the following May.

Read the full article here.

STRUGGLING HUAWEI RUNS OUT OF ADVANCED IN-HOUSE-DESIGNED CHIPS FOR SMARTPHONES AMID US TRADE SANCTIONS, COUNTERPOINT REPORT SAYS

Iris Deng | South China Morning Post | December 21, 2022

Huawei Technologies Co has finally run out of in-house-designed semiconductors for its smartphones after US trade sanctions effectively cut the company's access to advanced new chips, according to a report by Counterpoint Research. Shenzhen-based Huawei, which briefly surpassed Samsung Electronics to lead global smartphone shipments in early 2020, has struggled to get new in-house-designed integrated circuits (ICs) manufactured by a major chip foundry after Washington tightened trade restrictions in August 2020, covering the firm's access to semiconductors developed or produced using US technology, from anywhere. Privately-held Huawei and chip design arm HiSilicon were added to the US government's trade blacklist, known as the Entity List, in 2019. At the time, HiSilicon said it had a backup plan to ensure the group's survival, while research firms Haitong and Canalys indicated that Huawei had been stockpiling critical US components for almost a year.

Read the full article here.

THE TOP 20 AMERICAN UNIVERSITIES FOR R AND D FUNDING IN ENGINEERING

Michael T. Nietzel | Forbes | January 2, 2023

Where is cutting-edge engineering research being conducted in the U.S.? What are our leading universities for sponsored research in engineering subfields such as chemical engineering, electrical engineering, and mechanical engineering? One answer to those questions can be found in the Higher Education Research and Development (HERD) Survey, released in December by the National Science Foundation (NSF). That survey measures the dollars spent annually on research and development (R and D) at American colleges and universities. The latest HERD Survey, sponsored by the National Science Foundation's National Center for Science and Engineering Statistics, presents R&D expenditure data for fiscal year 2021, collected from 910 universities and colleges that grant a bachelor's degree or higher and spent at least $150,000 in R&D in the prior fiscal year. The HERD survey summarizes the federal, state, industry and other funds a university spends on all its research activities, and it also breaks those expenditures out by ten major fields.

Read the full article here.

2022 RESEARCH HIGHLIGHTS — PROMISING MEDICAL FINDINGS

National Institutes of Health | U.S. Department of Health & Human Services | December 20, 2022

With NIH support, scientists across the United States and around the world conduct wide-ranging research to discover ways to enhance health, lengthen life, and reduce illness and disability. Groundbreaking NIH-funded research often receives top scientific honors. In 2022, these honors included two NIH-supported scientists who received Nobel Prizes. Here's just a small sample of the NIH-supported promising medical findings in 2022. For more health and medical research findings from NIH, visit NIH Research Matters. The underlying causes of multiple sclerosis, a devastating autoimmune disease that affects the central nervous system, have been unclear. Using blood samples from more than 10 million people, researchers found that previous infection with Epstein-Barr virus dramatically increased the odds of developing multiple sclerosis. The finding suggests that vaccines against Epstein-Barr could help prevent the disease. Vaccines and treatments have lowered the risk of severe disease and death from SARS-CoV-2, the virus that causes COVID-19, but new variants continue to pose challenges.

Read the full article here.

CYBER CRIMINALS IMPERSONATING BRANDS USING SEARCH ENGINE ADVERTISEMENT SERVICES TO DEFRAUD USERS

Federal Bureau of Investigation | Internet Crime Complaint Center (IC3) | December 21, 2022

The FBI is warning the public that cyber criminals are using search engine advertisement services to impersonate brands and direct users to malicious sites that host ransomware and steal login credentials and other financial information. Cyber criminals purchase advertisements that appear within internet search results using a domain that is similar to an actual business or service. When a user searches for that business or service, these advertisements appear at the very top of search results with minimum distinction between an advertisement and an actual search result. These advertisements link to a webpage that looks identical to the impersonated business's official webpage. In instances where a user is searching for a program to download, the fraudulent webpage has a link to download software that is actually malware. The download page looks legitimate and the download itself is named after the program the user intended to download.

Read the full article here.

10 AMAZING AFOSR RESEARCH PROJECTS FOR 2022

Air Force Research Laboratory (AFRL)

Let's count down the new year with 10 amazing Air Force Office of Science Research (AFOSR) projects. The Air Force Research Laboratory accomplished a ton in 2022. As the year comes to a close we wanted to highlight some of that work at AFOSR. As a component of AFRL, AFOSR's mission focuses on investing in basic research efforts for the Air Force in relevant scientific areas to support the Air Force goals of control and maximum utilization of air, space, and cyberspace. AFOSR works with the academic community to support their basic research and its development for industry. Let us send off 2022 with 10 research efforts from AFOSR that are worth celebrating. Nothing says the holidays more than a warm cup of eggnog or hot chocolate to kickstart the new year. Engineers at the University of California, Irvine looked at a squid-skin-inspired cup cozy's, or covering's that will keep your hands cool and your drinks hot. Drawing inspiration from cephalopod skin, engineers at the UCI invented an adaptive composite material that can insulate beverage cups, restaurant to-go bags parcel boxes and even shipping containers.

Read the full article here.

BARGAINING CHIPS: US ALLIES AND EXPORT CONTROLS

Emily Benson | The Diplomat | January 1, 2023

A shift is occurring in U.S. policy on export controls, away from its "tall fence around a small yard" approach. The new strategy seeks a more expansive application of export controls more directly aimed at bringing about geopolitical objectives. On October 7, 2022, the Bureau of Industry and Security (BIS) at the U.S. Department of Commerce unveiled two new export control rules aimed at degrading Chinese AI capabilities. Typically, such announcements would have garnered enthusiasm mostly among a small community of export control experts, but these controls have frustrated U.S. allies and sent shockwaves throughout the global high-tech economy. These controls, if maintained, enforced, and ultimately supported by allies, have the potential to reshape the world's most consequential economic relationships, shuffle supply chains, and realign geoeconomic blocs. The new restrictions on exports of advanced semiconductors to China are particularly unique because they represent a return to a broad-based designation of export controls. This reflects the U.S. assumption that it is no longer possible to distinguish between military and non-military end-users in China, a consequence of Beijing's civil-military fusion doctrine.

Read the full article here.

AN UPDATE ON RESEARCH SECURITY: STREAMLINING DISCLOSURE STANDARDS TO ENHANCE CLARITY, TRANSPARENCY, AND EQUITY

Morgan Dwyer, Christina Ciocca Eller, and Ryan Donohue | Office of Science and Technology Policy | The White House | August 31, 2022

One of America's greatest strengths is its scientific and technological innovation, fueled over time by Federal investments in research and development (R&D). From the fundamental to the applied, U.S.-supported research has transformed our world and has made our communities safer, healthier, stronger, and more equitable. The American research culture is intentional in its strong commitment to openness. Yet maintaining that open research culture also requires being clear-eyed that certain governments seek to exploit our openness and disrupt the integrity of our research. Such threats require the Federal government, in collaboration with the research community, to take protective actions to mitigate research integrity risks without compromising the values that distinguish the U.S. research enterprise: openness, transparency, honesty, equity, fair competition, objectivity, and democratic participation.

Read the full article here.

U.S. CRACKS DOWN ON CHINESE COMPANIES FOR SECURITY CONCERNS

Ana Swanson | The New York Times | December 15, 2022

The Biden administration on Thursday stepped up its efforts to impede China's development of advanced semiconductors, restricting another 36 companies and organizations from getting access to American technology. The action, announced by the Commerce Department, is the latest step in the administration's campaign to clamp down on China's access to technologies that could be used for military purposes and underscored how limiting the flow of technology to global rivals has become a prominent element of United States foreign policy. Administration officials say that China has increasingly blurred the lines between its military and civilian industries, prompting the United States to place restrictions on doing business with Chinese companies that may feed into Beijing's military ambitions at a time of heightened geopolitical tensions, especially over Taiwan. In October, the administration announced sweeping limits on semiconductor exports to China, both from companies within the United States and in other countries that use American technology to make those products. It has also placed strict limits on technology exports to Russia in response to Moscow's invasion of Ukraine.

Read the full article here.

OPERATIONS SECURITY

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

NCSC executes the roles and responsibilities of the National Operations Security (OPSEC) Program Office, as described in National Security Presidential Memorandum (NSPM)-28 and will support department and agency implementation of OPSEC programs. NCSC/ETD will provide additional guidance, work with all Executive Branch departments and agencies to develop their programs, and will provide program development, training, and awareness materials. As set forth in NSPM-28, the National Operations Security Program (NOP) supports the establishment, implementation, and standardization of stakeholder OPSEC programs across the Executive Branch of the U.S. Government (USG) and, as appropriate, beyond to trusted partners. NSPM-28 requires all Executive Branch departments and agencies to implement OPSEC capabilities that identify and protect their most critical assets, identify and mitigate vulnerabilities, consider foreign adversarial threats in their organization's risk management activities, and apply sufficient threat mitigation practices to counter the threat. NOP requirements are set forth in NSPM-28.

Read the full article here.

EXPORT CONTROLS: ENFORCEMENT AGENCIES SHOULD BETTER LEVERAGE INFORMATION TO TARGET EFFORTS INVOLVING U.S. UNIVERSITIES

U.S. Government Accountability Office | June 14, 2022

Millions of foreign students and scholars study at U.S. universities, and many contribute to U.S. research. But, there's a risk that some may illegally access and share sensitive information, such as data or technology, with their home countries. Agencies involved in addressing this threat said that outreach and education increases university officials' awareness of research security threats and builds stronger relationships with university officials. To help prevent illegal transfers, we recommended that agencies determine which universities are at greater risk for such transfers and target outreach and education to them. According to U.S. government agencies, foreign entities are targeting sensitive research conducted by U.S. universities and other institutions. Releases or other transfers of certain sensitive information to foreign persons in the United States are subject to U.S. export control regulations. Such releases or transfers, which are considered to be exports, are commonly referred to as deemed exports. A U.S. Assistant Secretary of State wrote in 2020 that greater attention needed to be paid to deemed exports.

Read the full article here.