ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

June 9, 2021

DESANTIS SIGNS LAWS TO COMBAT CHINESE INFLUENCE AT FLORIDA UNIVERSITIES

Gray Rohrer | Orlando Sentinel | June 7, 2021

Gov. Ron DeSantis signed two bills into law Monday designed to combat foreign influence in Florida's universities from countries deemed hostile to the U.S., especially China, and crack down on theft of trade secrets and intellectual property. "If you look right now, there is no single entity that exercises a more pervasive nefarious influence across a wide range of American industries and institutions than the Communist Party of China," DeSantis said at a bill signing ceremony at a Florida National Guard facility in Miami. "Academia is permeated with its influence." DeSantis bashed China for its handling of the COVID-19 virus, asserting it leaked from a lab, and decried the country's influence among U.S. entertainment companies, two issues that have made headlines recently. But the bills he signed, HB 7017 and HB 1523, were spurred by incidents over the past decade of Chinese nationals working at Florida colleges stealing sensitive materials and designs of military equipment. Under HB 7017, Florida universities must report donations or gifts worth $50,000 or more from seven "foreign countries of concern" – China, Cuba, Iran, North Korea, Russia, Syria and Venezuela – twice each year, on Jan. 31 and July 31. Those that don't disclose gifts must pay 105% of the value of the gift to the state.

Read the full article here.

TRAINING OPPORTUNITY: CMMC FACT VS FICTION: WHAT'S AHEAD FOR GOVERNMENT CONTRACTORS

Derek White and Heather Engel

It's been two years since the Cybersecurity Maturity Model Certification (CMMC) was first announced. Since then, the model has gone through some updates and will continue to emerge as the Department of Defense and other agencies look to implement the verification method for cybersecurity requirements within the Government Contracting industry. This webinar will cover what's fact vs fiction in regard to CMMC, as well as discuss what contractors should be aware of and focused on between now and when CMMC is fully in place across the Defense Industrial Base (DIB). Attendees will have the opportunity to ask questions throughout. Join us for this complimentary, live webinar on Tuesday, June 22, 2021 at 2:00 PM ET. Save your spot by filling out the form on this page. We hope to see you there!

Register for the Webinar here.

TRIAL BEGINS FOR UNIVERSITY OF TENNESSEE, KNOXVILLE SCIENCE PROFESSOR ALLEGEDLY HIDING CHINESE RESEARCH AFFILIATIONS

Corinne Murdock | The Tennessee Star | June 8, 2021

A previously tenured science professor from University of Tennessee, Knoxville (UTK) faced trial Monday for allegedly covering up his research affiliations with China. The professor, Anming Hu, was first indicted last February by the U.S. Department of Justice (DOJ). His trial is a part of the DOJ's "China Initiative," an investigative effort by the DOJ's National Security Division (NSD) to identify and prosecute individuals engaged in trade secret theft, hacking, economic espionage, foreign direct investment threats, and supply chain compromises to benefit the Chinese government. The trial, United States v. Anming Hu, began Monday at 9 a.m. EST in the Eastern. According to court documents, the hearing is scheduled to continue Tuesday morning at 9 a.m. In addition to facing charges for false statements about his affiliations with the Beijing University of Technology (BJUT), Hu is facing charges of wire fraud. According to the DOJ press release, Hu was arrested because he didn't disclose his relationship to BJUT while receiving NASA funding. The press release also noted that UTK cooperated with the investigation.

Read the full article here.

DEPARTMENT OF JUSTICE SEIZES $2.3 MILLION IN CRYPTOCURRENCY PAID TO THE RANSOMWARE EXTORTIONISTS DARKSIDE

U.S. Department of Justice | June 7, 2021

The Department of Justice today announced that it has seized 63.7 bitcoins currently valued at approximately $2.3 million. These funds allegedly represent the proceeds of a May 8, ransom payment to individuals in a group known as DarkSide, which had targeted Colonial Pipeline, resulting in critical infrastructure being taken out of operation. The seizure warrant was authorized earlier today by the Honorable Laurel Beeler, U.S. Magistrate Judge for the Northern District of California. "Following the money remains one of the most basic, yet powerful tools we have," said Deputy Attorney General Lisa O. Monaco for the U.S. Department of Justice. "Ransom payments are the fuel that propels the digital extortion engine, and today's announcement demonstrates that the United States will use all available tools to make these attacks more costly and less profitable for criminal enterprises. We will continue to target the entire ransomware ecosystem to disrupt and deter these attacks.

Read the full article here.

COLONIAL PIPELINE HACKED VIA INACTIVE ACCOUNT WITHOUT MFA

Michael Novinson | CRN | June 5, 2021

The Darkside ransomware gang broke into Colonial Pipeline through an inactive account that didn't use multifactor authentication, according to a consultant who investigated the attack. The ransomware group took advantage of a compromised password for a virtual private network (VPN) account April 29 to get into the network of the Alpharetta, Ga.-based pipeline giant, said Charles Carmakal, SVP and CTO of FireEye's Mandiant division. The VPN account was no longer in use at the time of the attack but still provided hackers with access to Colonial's network, according to Carmakal. Carmakal and Colonial Pipeline CEO Joseph Blount spoke with Bloomberg Friday afternoon, and their comments were subsequently confirmed to CRN by spokespeople for FireEye and Colonial. The ransomware attack promoted Colonial to shut down its 5,500-mile natural gas pipeline for five days, resulting in more than 10,000 gas stations across the Southeastern United States being out of fuel.

Read the full article here.

CHINA IS STEALING OUR TECHNOLOGY AND INTELLECTUAL PROPERTY. CONGRESS MUST STOP IT

Dan Blumenthal and Linda Zhang | National Review | June 2, 2021

The Senate is moving fast to pass the U.S. Innovation and Competition Act (USICA), which will spend significant taxpayer dollars to help Washington compete technologically with China. The bill must include strong "research security" provisions to stop China's rapacious program of acquiring science and technological know-how. U.S. science and technology programs have not been well protected from Beijing to date, and as Congress pumps more government funding into the U.S. research enterprise, such laxity in protecting American intellectual property (IP) can no longer be tolerated. While other costs to U.S. national power are more difficult to measure, the U.S. Trade Representative estimated in 2018 that Chinese theft of American IP costs U.S. firms between $225 billion and $600 billion every year. General Keith Alexander, a former National Security Agency director, has called China's technology theft "the greatest transfer of wealth in human history."

Read the full article here.

BIDEN'S NEW SCIENCE ADVISER SHARES VIEWS ON FOREIGN INFLUENCE, RESEARCH BUDGETS, AND MORE

Jeffrey Mervis | Science | June 3, 2021

President Joe Biden's newly installed science adviser says he understands why scientists are baffled by rules intended to prevent other nations from unfairly benefiting from U.S. science. In recent years, the U.S. government has cracked down on requiring federally funded scientists to report any sources of foreign funding—and has even prosecuted some who failed to follow the rules. But the effort has forced them to navigate a mélange of requirements, and Eric Lander thinks the government can do better. "It's very hard to figure out what you're supposed to be disclosing," Lander told ScienceInsider yesterday during a wide-ranging interview conducted on his first day on the job as director of the White House Office of Science and Technology Policy (OSTP). "Agencies have different rules, and their definitions also vary." Lander believes researchers would be happy to comply with a simpler system of disclosure—such as a digital record of their research activities updated on a quarterly basis.

Read the full article here.

ALL ROADS LEAD TO INTELLECTUAL PROPERTY IN THE U.S. – CHINA RIVALRY

Noelle Borao | EIN Presswire | June 4, 2021

While there is no official acknowledgment, there is little doubt that the "Quad" of U.S., Australia, India, and Japan was designed to thwart China's aims in the Indo-Pacific region. The Quad discussed not only producing and delivering COVID vaccinations in the March meeting, but also explored building a supply chain for producing rare-earth minerals to counter China's 60% dominance in that market. However, Beijing's ambitions extend beyond dominating the global supply infrastructure for strategic goods relevant for U.S. security. Its road to power over Western allies would likely come from misappropriation of commercial technology innovations—or intellectual property (IP) theft—that also have public, military uses. It is therefore critical that the Biden administration calibrate its strategy toward China's IP theft, in particular. U.S. officials have long warned about the Chinese Party-State's practice of military-civil fusion of science and research activities, intended to either develop or acquire technologies explicitly for bolstering its military power.

Read the full article here.

TO COUNTER CHINA, ALLIED NATIONS MUST COOPERATE ON TECHNOLOGY INNOVATION

Jamil N. Jaffer | The Hill | June 1, 2021

America and our allies are in the midst of the fight of a generation. China's rise as a technological juggernaut seems inexorable. Across the globe, there is an appearance that the U.S. and our allies' power and influence is on the wane, supplanted by massive Chinese technology deployment and resource distribution. In parallel to China's rise, the potential of our core alliances may be waning, as some allies saw America walking away from commitments and, as a result, have grown skeptical of our leadership and staying power. Yet there remains time to alter our current trajectory, as the Biden administration seeks to rebuild frayed relationships with key allies and partners in Europe, Asia and other regions. This effort could not be more critical or timely, particularly as our nations look to come out of economic and social challenges presented by the COVID-19 pandemic and address the supply chain revealed in the context of this crisis through onshoring and ally-shoring.

Read the full article here.

CYBER ATTACKS REVEAL THE TRUTH ABOUT NETWORK VULNERABILITY

Government Technology | June 4, 2021

The cyber attack on Colonial Pipeline Co. and similar recent attacks such as the SolarWinds breach (which impacted several government agencies) revealed major vulnerabilities in government cybersecurity protocols and critical infrastructure systems, resulting in immediate action taken by the White House. If there's one lesson to be learned from these breaches, it's that organizations of all sizes and industries must do everything they can to protect their infrastructure, environments and networks. Organizations deal with threats to their environments every day, whether it's employee remote access to internal systems or access granted to third-party vendors who perform outsourced business operations. There's no shortage of avenues for hackers to exploit — especially for large and susceptible targets like the government and critical infrastructure. That's why the new executive order is a change agent in the cybersecurity industry. Organizations are apt to stick to what they know when it comes to cybersecurity, which tends to be old security methods and legacy systems.

Read the full article here.

SENATE PUSHES FINAL RESEARCH COMPETITIVENESS BILL VOTE TO WEEK OF JUNE 8

Christa Wagner | AAMC | June 4, 2021

After more than a week of Senate floor debate on the Endless Frontier Act (S. 1260), a bipartisan proposal to provide more than $200 billion to enhance the United States' global research competitiveness, support domestic manufacturing, and address foreign government influence in research, the Senate postponed further consideration of the package until after the Memorial Day recess. Republicans voiced objections on May 27 to last-minute additions to the bill, forcing the chamber to delay a final vote on the more than 1,400-page bill to the week of June 7. Objections arose after senators introduced more than 600 amendments for consideration during the open amendment process throughout the week of May 24, including an amendment in the nature of a substitute from Senate Majority Leader Chuck Schumer (D-N.Y.), co-lead of the Endless Frontier Act.

Read the full article here.

AS THE U.S.-CHINA TRADE WAR CONTINUES, CAREER TRAINING IS AMERICA'S BEST DEFENSE

Shaun McAlmont | Real Clear Education | June 4, 2021

Amid the ongoing trade war between China and the United States, lawmakers are moving to pass a comprehensive new bill to boost economic competition, minimize reliance on China, and promote investment in the American workforce. With our economy beginning to recover, we need to focus on preparing young people to fill vital roles in the years ahead and decrease our reliance on tech and talent from abroad. China has the world's second-largest economy and a faster-growing and more lucrative tech industry that "is poised to come out ahead" of the U.S., according to an analysis by The Wall Street Journal last year. It's winning the 5G race, contributes more to AI research, and because its population is so large, it has more data to feed to machine-learning and transportation technologies like self-driving vehicles. If the U.S. wants to prevail in the tech race, we have to start with education.

Read the full article here.

CHINESE CYBERSPIES UNC2630 TARGETING US AND EU ORGANIZATIONS

Cyware | June 3, 2021

China-sponsored threat groups, tracked as UNC2630 and UNC2717, are deploying new malware strains on compromised networks. Recently, the groups have targeted dozens of U.S. and EU organizations after abusing vulnerable Pulse Secure VPN appliances. What has happened? A month ago, threat actors were abusing a recently patched zero-day in Pulse Connect Secure gateways. They deployed malware to gain access to networks, collect credentials, and steal proprietary data. UNC2630 installed four new malware strains, bringing the total to 16 malware families custom-tailored for targeting Pulse Secure VPN appliances. These new malware families are Bloodmine, Bloodbank, Cleanpulse, and Rapidpulse. Moreover, old malware families identified as SlowPulse, SlightPulse, and HardPulse, among others, were also put to use. Many of the targeted organizations operate in defense, government, high-tech, transportation, and financial sectors aligning with Beijing's strategic goals mentioned in China's recent 14th Five Year Plan.

Read the full article here.

OPINION: TO COMPETE WITH CHINA, WASHINGTON MUST FIX ITS OWN DYSFUNCTION

Josh Rogin | The Washington Post | June 3, 2021

Everyone in Washington seems to agree that strategic competition with China is the most important U.S. foreign policy issue, but there's no agreement on how to address it. As Congress works on its biggest-ever bipartisan package of China-related legislation, worrying signs suggest our government and politics might be too broken to rise to this massive and complex challenge. Last week, the Biden administration's "Asia czar," Kurt Campbell, publicly announced the United States would embrace, not turn away from, the Trump administration's decision to fundamentally reorient U.S. foreign policy toward China. "The period that was broadly described as engagement has come to an end," he said, adding that the United States will operate under a "new set of strategic parameters" and "the dominant paradigm is going to be competition." In Congress, Democrats and Republicans are working on a huge piece of legislation that is meant to put America's money where Campbell's mouth is. And next Tuesday, after months of delay, the Senate is set to finally pass what it calls comprehensive legislation to compete with China.

Read the full article here.

NET CLOSES IN ON CHINESE 'SPIES' IN UK UNIVERSITIES WHERE ACADEMICS ARE SUSPECTED OF PASSING PIONEERING BRITISH TECHNOLOGY TO BEIJING

Glen Owen and Jake Ryan | The Daily Mail | May 22, 2021

A high-level probe into Chinese 'spies' working in British universities could lead to arrests within weeks, The Mail on Sunday has been told. Specialists at the Foreign Office, Special Branch and HMRC have drawn up a list of academics suspected of passing sensitive information to Beijing, including pioneering British technology that could be used to aid the repression of minorities and dissidents. Investigators are understood to have 'established a correlation' between universities which earn significant income from students from China and the activities of staff which have prompted suspicion. Universities under scrutiny include Manchester and Imperial College, which earn 26 per cent of their income from students from China; Liverpool and Sheffield (28 per cent); and Oxford and Cambridge (10 per cent). There is no suggestion any of the institutions are aware of, or complicit in, any wrongdoing. Last year it was revealed that a third of non-EU university students in the UK come from China, with 120,000 paying a total of £2.1 billion in fees.

Read the full article here.

EXCHANGE SERVERS TARGETED BY 'EPSILON RED' MALWARE

Elizabeth Montalbano | Threat Post | June 3, 2021

Threat actors have deployed new ransomware on the back of a set of PowerShell scripts developed for making encryption, exploiting flaws in unpatched Exchange Servers to attack the corporate network, according to recent research. Researchers from security firm Sophos detected the new ransomware, called Epsilon Red, in an investigation of an attack on a U.S.-based company in the hospitality sector, Sophos Principal Researcher Andrew Brandt wrote in a report published online. The name – coined by the attackers themselves, who may be the same crew behind the REvil ransomware – is a reference to an obscure enemy character in the X-Men Marvel comics. The character is a "'super soldier' alleged to be of Russian origin" armed with four mechanical tentacles – which seems to represent the way the ransomware spreads its hooks into a corporate network, Brandt wrote.

Read the full article here.

APPLIED RESEARCH GETS STARRING ROLE IN BIDEN'S 2022 BUDGET

Jeffrey Mervis and David Malakoff | Science | June 1, 2021

Last week, President Joe Biden unveiled a proposed 2022 budget for the U.S. government that would boost federal spending on R&D by 9%, or $13.5 billion, including what he calls "the biggest increase in non-defense [R&D] spending on record." The plan puts an unprecedented emphasis on translating scientific discoveries into practical tools for fighting climate change and disease, bolstering the economy, and tackling other issues. Although Congress is certain to reject or revise parts of the proposal, its support for even a portion of Biden's ambitious vision might lead to numerous new funding entities and alter how the government invests in academic research. The $6 trillion spending blueprint released on 28 May adds greater detail to a skeletal plan Biden presented in early April. It asks Congress to boost spending on a wide swath of nondefense science (see table, below), with increases of 20% or more for research programs at the National Institutes of Health (NIH), the National Science Foundation (NSF), the U.S. Department of Agriculture (USDA), and other agencies. It also includes a 30% boost for clean energy R&D. At the same time, Biden wants an 11% cut in basic research spending by the military, which is a key funder of academic research in math, computer science, and engineering.

Read the full article here.

HOW U.S. GOVERNMENT AGENCIES HAVE RESPONDED TO CHINESE NATIONALS EXPLOLITING U.S. R&D

Synthetic | May 31, 2021

American taxpayers contribute over $150 billion each year to scientific research. Through entities like the National Science Foundation, the National Institutes of Health and the Department of Energy's National Labs, taxpayers fund innovations that contribute to national security and innovation. America built this successful research enterprise on certain values: reciprocity, integrity, merit-based competition, and transparency. These values foster a free exchange of ideas, encourage the most rigorous research results to flourish, and ensure that researchers receive the benefit of their intellectual capital. The open nature of research in America encourages our researchers and scientists to "stand on the shoulders of giants." In turn, America attracts the best and brightest. Foreign researchers and scholars travel to the U.S. just to participate in the advancement of science and technology. Some countries, however, seek to exploit America's openness to advance their own national interests.

Read the full article here.

THE INTENSE CYBER STRUGGLE OVER INTELLECTUAL PROPERTY THREATENS THE GLOBAL ORDER

Ruth Taplin | Barron's | June 1, 2021

Are companies and governments prepared for cyberattacks on intellectual property, infrastructure, and the full suite of cyberwarfare? Judging from recent events, not really. The list of examples from the very recent past is alarming. In December, it came to light that the Russian state had apparently launched a cyberespionage attack on the U.S. software firm SolarWinds, giving hackers access to a mine of data on U.S. government and private company IP and personnel. In March, we learned that Chinese state-affiliated criminal gangs hacked into thousands of private companies' emails through Microsoft Exchange Server, gaining sensitive IP, legal and negotiation data. In May, Colonial Pipelines was successfully targeted by the nonstate Russian hacking group DarkSide, out for monetary gain through ransomware. And last week, Microsoft said the Russian state-backed attacker behind SolarWinds had launched a new attack on government agencies and think tanks. It is clear that cyberattacks on IP, trade secrets, and intelligence information emanating from China and Russia will in the coming years present the greatest threat to democracy globally—not to mention to intellectual property rights in general. Consider one more recent example of such a cyberespionage alliance: the case of Turbine Panda, a name given by researchers to a Chinese-affiliated group that allegedly carried out cyberattacks on U.S. aeronautics companies with the intention of stealing the blueprints of the components for an aircraft engine.

Read the full article here.