ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

May 26, 2021

U.S. A TOP TARGET FOR FOREIGN AND DOMESTIC INFLUENCE OPERATIONS, SAYS NEW FACEBOOK REPORT

Elizabeth Culliford | Financial Post | May 26, 2021

The United States topped a list of the countries most frequently targeted by deceptive foreign influence operations using Facebook between 2017 and 2020, the social media company said in a new report released on Wednesday. It also came second on a list of countries targeted by domestic influence operations in that same time period. Facebook Inc said one of the top sources of coordinated inauthentic behavior networks targeting the United States in the year leading up to the 2020 presidential election was domestic campaigns originating in the United States itself, as well as foreign operations from Russia and Iran. The tallies were based on the number of "coordinated inauthentic behavior" networks removed by Facebook, a term it uses for a type of influence operations that relies on fake accounts to mislead users and manipulate the public debate for strategic ends.

Read the full article here.

SENATE WEIGHING NEW CONTROLS ON FOREIGN INVOLVEMENT IN US RESEARCH

Mitch Ambrose | American Institute of Physics | May 20, 2021

Senators are proposing major expansions to federal research security policies through provisions attached to the Endless Frontier Act, which the full Senate began debating this week. Proponents of the measures argue that if the U.S. is to substantially increase R&D funding, it must do more to ensure that rival governments, principally China's, do not reap the benefits. The bill emerged from the Senate Commerce, Science, and Transportation Committee already bearing blanket restrictions on federal funds supporting researchers who are participating in certain nations' "talent recruitment programs." Now, the bill has been bundled into a broader legislative package titled the U.S. Innovation and Competition Act, which contains additional security measures developed by other committees. These new provisions include ones enabling the federal government to block U.S. universities from accepting certain foreign funding and to deny visas to individuals who are deemed to present a risk of misappropriating "sensitive or emerging technologies." University groups successfully advocated to modify some provisions before they were added to the bill, but they have warned the addition of other, little-debated measures could undermine support for the legislation.

Read the full article here.

ALBERTA ASKS UNIVERSITIES TO STOP PURSUING PARTNERSHIPS WITH LINKS TO CHINESE GOVERNMENT

Rob Drinkwater | Vancouver Sun | May 24, 2021

Alberta's advanced education minister has sent a letter to four of the province's universities asking them to pause their pursuit of new or renewed partnerships with organizations linked with China or the Chinese Communist Party. A ministry spokesman says in an email that Demetrios Nicolaides has also asked the four comprehensive academic and research institutions to thoroughly review their relationships with entities that are potentially linked with the People's Republic of China and its governing party. The letter asks that the review ensures "these ongoing partnerships follow stringent risk assessments and due diligence." "I am deeply concerned about the potential theft of Canadian intellectual property and further concerned that research partnerships with the People's Republic of China may be used by Chinese military and intelligence agencies," Nicolaides said in a statement. "More needs to be done to curb foreign state infiltration into our research and innovation centres, including our post-secondary institutions."

Read the full article here.

A WARNING TO DOD: RUSSIA ADVANCES QUICKER THAN EXPECTED ON AI, BATTLEFIELD TECH

Andrew Eversden | C4ISRNET | May 24, 2021

The Russian military is more technologically advanced than the U.S. realized and is quickly developing artificial intelligence capabilities to gain battlefield information advantage, an expansive new report commissioned by the Pentagon warned. The federally funded Center for Naval Analyses examined the Kremlin's whole-of-government approach for artificial intelligence development and found it is largely driven by the perceived threat from the United States, combined with lessons learned from its continuing conflicts in Syria and Ukraine about what the future battlefield will look like, the report released Monday said. However, the Russian government faces limitations because its AI efforts are primarily government funded, and it lacks a strong defense industrial base, noted the report, written on behalf of the Pentagon's Joint Artificial Intelligence Center. Still, analysts cautioned Pentagon leadership not to underestimate the Russia's technological advances as the U.S. pivots its strategic focus to the Indo-Pacific. The Russian military has been undergoing modernization since 2009.

Read the full article here.

TARGETING U.S. TECHNOLOGIES: A REPORT OF FOREIGN TARGETING OF CLEARED INDUSTRY

Briefing from the Defense Counterintelligence and Security Agency

FY19 cleared industry submitted 6,121 reports that the Defense Counterintelligence and Security Agency (DCSA) assessed as likely an attempt to obtain unauthorized access to classified or sensitive information and technology. These suspicious contact reports (SCR) from cleared industry represent an incident of a likely foreign entity attempting to illicitly obtain access to information or technology at a facility. This presentation is not a holistic assessment of foreign intelligence targeting of cleared industry; DCSA cannot assess the volume foreign collection attempts that go unidentified or unreported.

View the presentation slides here.

32 CODE OF FEDERAL REGULATION PART 117, NISPOM

Defense Counterintelligence and Security Agency | May 25, 2021

May 24 marks the halfway point in the National Industrial Security Program Operating Manual (NISPOM) rule implementation period ending August 24, 2021. DCSA is here to help you "get ready for the rule." In addition to changing from a DOD operating manual (5220.22-M) to a federal rule (32CFR Part 117), the NISPOM Rule includes a number of contractor requirements. DCSA has created and published resources to assist cleared industry in better understanding what is required for compliance. More than 5,000 users have visited the NISPOM Rule webpage, close to 2,000 people have watched the "Ready for the Rule" video, and more than 3,000 users have used the NISPOM Cross Reference Tool as a desk-side aid offering the ability to select a link in the familiar NISPOM table of contents and find the corresponding section of the NISPOM Rule. DCSA is also soliciting questions about the NISPOM Rule and has posted Frequently Asked Questions (FAQs) to the NISPOM Rule webpage. NISPOM Rule FAQs address the top questions asked during engagements with cleared industry.

Read the full article here.

CENSORSHIP, SURVEILLANCE AND PROFITS: A HARD BARGAIN FOR APPLE IN CHINA

Jack Nicas, Raymond Zhong, and Daisuke Wakabayashi | The New York Times | May 17, 2021

On the outskirts of this city in a poor, mountainous province in southwestern China, men in hard hats recently put the finishing touches on a white building a quarter-mile long with few windows and a tall surrounding wall. There was little sign of its purpose, apart from the flags of Apple and China flying out front, side by side. Inside, Apple was preparing to store the personal data of its Chinese customers on computer servers run by a state-owned Chinese firm. Tim Cook, Apple's chief executive, has said the data is safe. But at the data center in Guiyang, which Apple hoped would be completed by next month, and another in the Inner Mongolia region, Apple has largely ceded control to the Chinese government. Chinese state employees physically manage the computers. Apple abandoned the encryption technology it used elsewhere after China would not allow it. And the digital keys that unlock information on those computers are stored in the data centers they're meant to secure.

Read the full article here.

COMBATTING INSIDER THREATS WITH KEYBOARD SECURITY

Dale Ludwig | Threat Post | May 25, 2021

As cyberattacks snowball and insider threats become an ever-larger part of the problem, it may be time to move beyond purely software-based cyber-defenses. Implementing hardware-based security, like secure keyboards, can be an important part of the mix. Those in IT-leadership roles are well aware that the attention and spending on security and tightening computer networks against cyberattacks has never been higher. Motivations for nefarious activity can range from espionage and financial gain to just plain business disruption. Whatever the motivation, cybersecurity threats continue to grow in numbers and complexity, and have significant effects on all facets of the day-to-day business of running a large organization. Beyond the significant financial issues they can cause, cyberattacks can also lead to lawsuits, regulatory penalties and reputational damage. Just like the motives behind cyber-threats, the actual attacks themselves can be incredibly varied. Today's large organizations must be on the lookout to combat all types of threats, including malware, denial of service (DoS) attacks, zero-day exploits, ransomware, DNS attacks and many more. Overall, most companies have done a very good job policing these attacks from outsiders.

Read the full article here.

CONTROLLED UNCLASSIFIED INFORMATION QUICK REFERENCE GUIDE

Department of Defense | April 1, 2021

For information to be considered CUI it must fall within a category, such as: Critical Infrastructure; Defense; Export Control; Financial & Tax; Immigration; Intelligence; International Agreements; Law Enforcement; Legal; Natural & Cultural Resources; NATO; Nuclear; Patent; Privacy; Procurement & Acquisition; Proprietary Business Information; Provisional (for DHS use only); Statistical; Transportation A complete list of categories, sub-categories, and descriptions can be found at https://www.dodcui.mil.

Read the full quick reference guide here.

HOW CISA LIMITED THE IMPACT OF THE SOLARWINDS ATTACK

Jason Miller | Federal News Network | May 19, 2021

Soon after the specifics about the SolarWinds attack came to light, the Department of Homeland Security went to work to limit the damage. Among the first things it did was put the attack signatures into the EINSTEIN toolset that is used by nearly every agency. "As part of the SolarWinds campaign, EINSTEIN was extremely useful in terms of identifying suspicious network traffic from a handful of federal civilian agencies that upon further investigation by those agencies helped identify additional victims of this campaign. It's worth noting that EINSTEIN didn't prevent the intrusion nor was it able to detect the intrusion until, in this case, we received threat information from private sector partners to inform our detection and prevention mechanisms," said Matt Hartman, the deputy executive assistant director for cyber at CISA, in an interview with Federal News Network. "As soon as CISA received indicators of this activity from industry partners, we immediately leveraged EINSTEIN to identify and notify agencies of anomalous activity on their networks, which helped accelerate response, remediation and recovery activities."

Read the full article here.

NATIONAL CYBER DEFENSE IS A "WICKED" PROBLEM: WHY THE COLONIAL PIPELINE RANSOMWARE ATTACK AND THE SOLARWINDS HACK WERE ALL BUT INEVITABLE

Terry Thompson | SciTechDaily | May 15, 2021

The ransomware attack on Colonial Pipeline on May 7, 2021, exemplifies the huge challenges the U.S. faces in shoring up its cyber defenses. The private company, which controls a significant component of the U.S. energy infrastructure and supplies nearly half of the East Coast's liquid fuels, was vulnerable to an all-too-common type of cyber attack. The FBI has attributed the attack to a Russian cybercrime gang. It would be difficult for the government to mandate better security at private companies, and the government is unable to provide that security for the private sector. Similarly, the SolarWinds hack, one of the most devastating cyber attacks in history, which came to light in December 2020, exposed vulnerabilities in global software supply chains that affect government and private sector computer systems. It was a major breach of national security that revealed gaps in U.S. cyber defenses. These gaps include inadequate security by a major software producer, fragmented authority for government support to the private sector, blurred lines between organized crime and international espionage, and a national shortfall in software and cybersecurity skills. None of these gaps is easily bridged, but the scope and impact of the SolarWinds attack show how critical controlling these gaps is to U.S. national security.

Read the full article here.

HOW SHOULD THE U.S. RESPOND TO CHINA'S MILITARY-CIVIL FUSION STRATEGY?

Elsa Kania, Tai Ming Cheung, Anja Manuel, Leo Carter, Peter Wood, Emily Weinstein, and Lorand Laskai
China File | May 22, 2021

During Donald Trump's presidency, the term "military-civil fusion" (MCF) came to feature prominently in U.S. officials' characterizations of their concerns about China. While efforts to integrate China's civilian and defense economies have been a goal of China's leaders for decades, Xi Jinping has elevated MCF as a priority and has expanded, intensified, and accelerated the effort across multiple domains, including to concentrate on more integrated development of emerging technologies. This strategy is regarded as critical to China's capacity to succeed in a confrontation of systems. During the Trump administration, U.S. officials expressed worries over the perceived threat of transfer of dual-use technologies, as well as about the long-term competitive challenge, should this initiative prove successful in improving synergies within China's innovation ecosystem.

Read the full article here.

THE FULL STORY OF THE STUNNING RSA HACK CAN FINALLY BE TOLD

Andy Greenberg | Wired | May 20, 2021

Amid all the sleepless hours that Todd Leetham spent hunting ghosts inside his company's network in early 2011, the experience that sticks with him most vividly all these years later is the moment he caught up with them. Or almost did. It was a spring evening, he says, three days—maybe four, time had become a blur—after he had first begun tracking the hackers who were rummaging through the computer systems of RSA, the corporate security giant where he worked. Leetham—a bald, bearded, and curmudgeonly analyst one coworker described to me as a "carbon-based hacker-finding machine"—had been glued to his laptop along with the rest of the company's incident response team, assembled around the company's glass-encased operations center in a nonstop, 24-hours-a-day hunt. And with a growing sense of dread, Leetham had finally traced the intruders' footprints to their final targets: the secret keys known as "seeds," a collection of numbers that represented a foundational layer of the security promises RSA made to its customers, including tens of millions of users in government and military agencies, defense contractors, banks, and countless corporations around the world.

Read the full article here.

DOD CLEARS PATH FOR FIRST ASSESSOR TO ENTER CMMC MARKET

Jackson Barnett | FedScoop | May 13, 2021

The Department of Defense's cyber inspectors approved the first company to become a certified assessor for the department's new contractor cybersecurity standards, clearing a critical hurdle in the process. The DOD's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) approved the first company, which was not named, to move forward in the Cybersecurity Maturity Model Certification (CMMC) process, a spokesperson told FedScoop. Now, it is up to the CMMC Accreditation Body (CMMC-AB) to grant the company Certified Third Party Assessment Organization (C3PAO) status, meaning that it can officially assess the maturity of defense contractors' cybersecurity in compliance with new CMMC requirements. "[W]e can say the first C3PAO has been certified by the agency. Keep in mind, the certification process is multi-tiered and [Defense Contract Management Agency's] role is to verify and validate the ability of a C3PAO to protect the data that will be entrusted to them," Matthew Montgomery, spokesperson for the DCMA, the agency that houses DIBCAC, told FedScoop.

Read the full article here.

MINIMIZING DAMAGE FROM A DATA BREACH: A CHECKLIST

Susan Bradley | CSO | May 12, 2021

Once a breach occurs, you'll want to identify what the attackers accessed and how they accessed the data. This information helps you identify if you need to notify users that their data has been breached and learn how to protect yourself from the next attack. First, make sure you have the necessary resources and preparations in place to investigate. The process of identifying how an attacker entered the network is often based on the evidence and timeline analysis. Knowing how best to handle the evidence and having a plan in place before an intrusion occurs are key to properly handling the investigation. The Cybersecurity Unit for the US Department of Justice has several resources to help with planning ahead. This task checklist will make it easier to respond to a data breach or limit its damage.

Read the full article here.

US PUBLIC HAS MIXED VIEWS ON FOREIGN STUDENT RECRUITMENT

Mary Beth Marklein | University World News | May 17, 2021

Americans are more likely than not to say students from other countries have a positive impact on United States higher education and society, but offer mixed views about whether they would like universities to step up efforts to reverse recent enrolment declines, a study suggests. The study, which is based on three iterations of surveys of registered voters conducted between March 2017 and February 2021, paints what it calls a "complex, evolving and nuanced public view" of how US voters perceived international students during perhaps the most volatile and politicised period of higher education policy-making since the September 2001 terrorist attacks. It was sponsored by the American Council on Education (ACE), the primary representative in Washington for university leaders. Overall, US international enrolments declined 1.8% in 2019, according to the Institute of International Education (IIE), which has tracked student mobility trends for decades. IIE data also show that international students contributed an estimated US$44 billion to the US economy that year. But the US's global share has diminished in recent years as more countries are competing in the recruitment of students from outside their borders.

Read the full article here.

CHINA'S COLLECTION OF GENOMIC AND OTHER HEALTHCARE DATA FROM AMERICA: RISKS TO PRIVACY AND U.S. ECONOMIC AND NATIONAL SECURITY

The National Counterintelligence and Security Center | February 2021

Would you want your DNA or other healthcare data going to an authoritarian regime with a record of exploiting DNA for repression and surveillance? For years, the People's Republic of China (PRC) has collected large healthcare data sets from the U.S. and nations around the globe, through both legal and illegal means, for purposes only it can control. While no one begrudges a nation conducting research to improve medical treatments, the PRC's mass collection of DNA at home has helped it carry out human rights abuses against domestic minority groups and support state surveillance. The PRC's collection of healthcare data from America poses equally serious risks, not only to the privacy of Americans, but also to the economic and national security of the U.S.

Read the full article here.

US PROFESSOR WITH CHINA TIES JAILED FOR LYING ON GRANT APPLICATIONS

Rebecca Trager | Chemistry World | May 20, 2021

A former Ohio State University rheumatologist and researcher who was arrested in May 2020 for his role in an immunology research fraud scheme has been sentenced to 37 months in prison. Last November, Song Guo Zheng pleaded guilty to lying on federal research grant applications so that he could use more than $4 million (£2.8 million) that his research group secured from the US National Institutes of Health (NIH) to develop rheumatology and immunology expertise for the Chinese government. As part of his 14 May sentence, Zheng is ordered to pay more than $3.4 million in restitution to the NIH and approximately $413,000 to Ohio State University. Zheng had been participating in the Chinese government's Thousand Talents programme – a scheme to recruit and cultivate high-profile scientists – since 2013, according to an affidavit filed with the criminal complaint. He was trying to hide his participation in the talent scheme and his affiliation with a Chinese university under Chinese government control, the US Department of Justice (DOJ) stated.

Read the full article here.

NELSON USES CHINESE MARS LANDING AS A WARNING TO CONGRESS

Jeff Foust | Space News | May 19, 2021

NASA Administrator Bill Nelson congratulated China for successfully landing a rover on Mars, but also used the milestone to warn Congress of China's competitive threat to American leadership in human spaceflight. In a statement May 19, hours after the China National Space Administration (CNSA) released the first images taken by the Zhurong rover since its May 14 landing on Mars, Nelson congratulated China for being only the second country, after the United States, to land a spacecraft on Mars and operate it there for more than a brief period. "As the international scientific community of robotic explorers on Mars grows, the United States and the world look forward to the discoveries Zhurong will make to advance humanity's knowledge of the Red Planet," Nelson said in the statement. "I look forward to future international discoveries, which will help inform and develop the capabilities needed to land human boots on Mars."

Read the full article here.

A BIPARTISAN VISION FOR THE FUTURE OF AMERICAN SCIENCE

Eddie Bernice Johnson | Issues in Science and Technology | April 27, 2021

A few weeks ago, I was joined by Science, Space, and Technology Committee Ranking Member Frank Lucas (R-OK), along with Research & Technology Subcommittee Chairwoman Haley Stevens (D-MI) and Ranking Member Michael Waltz (R-FL), in introducing the National Science Foundation for the Future Act (H.R.2225), the first comprehensive reauthorization of NSF since 2010. The bill is the culmination of a year's effort by members and bipartisan committee staff to gather input and feedback from what may be the largest and most diverse group of stakeholders to ever inform an NSF reauthorization. In the coming weeks, we will hold hearings on the legislation and bring it up for debate and amendment in committee.

Read the full article here.