ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

October 7, 2020

FBI AND NCSC RELEASE NEW MOVIE TO INCREASE AWARENESS OF FOREIGN INTELLIGENCE THREATS ON PROFESSIONAL NETWORKING SITES AND OTHER SOCIAL MEDIA PLATFORMS

U.S. Department of Justice Federal Bureau of Investigation and the Office of the Director of National Intelligence National Counterintelligence and Security Center | September 30, 2020

The FBI and the National Counterintelligence and Security Center (NCSC) today released a new movie to increase awareness of how foreign intelligence entities use fake profiles and other forms of deception on social media platforms to target individuals in government, business and academic communities for recruitment and information gathering. Inspired by true events, the 30-minute movie, called "The Nevernight Connection," details the fictional account of a former U.S. Intelligence Community official who was targeted by a foreign intelligence service via a fake profile on a professional networking site and recruited to turn over classified information. The movie can be accessed at: www.fbi.gov/nevernight.

Read the full article here.

REQUIRED SUBMISSION OF FINANCIAL CONFLICT OF INTEREST POLICY INTO THE ERA COMMONS INSTITUTION PROFILE (IPF) MODULE

National Institutes of Health | October 5, 2020

Effective November 12, 2020, NIH funded recipients will be required to submit their publicly assessible Financial Conflict of Interest policy to NIH via the eRA Commons Institution Profile (IPF) Module (IPF Module). A PDF of the FCOI policy must be submitted by the institutional signing official (SO) via the IPF Module under a new tab labeled, "Policy Documents". While the automated requirement goes into effect in November, NIH recognizes that recipients will need to modify their internal systems in order to comply. Therefore, applicants and recipients have until December 1, 2020, to comply with this requirement.

Read the full notice here.

CAUGHT IN THE CROSSFIRE: STRATEGIC COMPETITION, U.S.-CHINA SCIENCE COLLABORATION, AND U.S. UNIVERSITIES

Panel Discussion to be held October 28, 2020 featuring Arthur Bienenstock, Elsa B. Kania, Tim Stearns, and Susan Shirk | Stanford

Reports of Chinese espionage, IP theft and military-civil fusion strategy have all fueled concerns regarding U.S. universities' open research ecosystem, especially in STEM. Many of the concerns focus not only on research integrity but also on potential adverse consequences to U.S. military and economic security. This panel intends to deepen discussion on open access to U.S. universities, security risks involved, as well as the potential adverse consequences of limiting international access in science and technology (S&T) research. Questions that panel members will be asked to address include: What is our best estimate regarding the scale and scope of adverse influence in U.S. universities attributable to S&T collaboration with PRC personnel? Scientific collaboration and higher education have traditionally been immune to the ups-and-downs of U.S.-China politics. How did we get to where we are, and why? What are remedial measures that universities can consider, optimized to balance security and ethical concerns while ensuring pre-eminent scientific advancements and continued U.S. innovation?

Read the full announcement here.

DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT: ASSESSING CONTRACTOR IMPLEMENTATION OF CYBERSECURITY REQUIREMENTS (DFARS CASE 2019-D041)

U.S. Department of Defense | September 29, 2020

DoD is issuing an interim rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification framework in order to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain.

Read the full interim rule here.

CHARGES DROPPED AGAINST CHINESE RESEARCHER ACCUSED OF STEALING UVA TRADE SECRETS

Tyler Hammel | The Daily Progress | September 29, 2020

Charges against a University of Virginia researcher have been dropped after he was accused last month of stealing trade secrets and trying to take them to China. Haizhou Hu, a Chinese national, was arrested Aug. 28 as he attempted to board a flight from Chicago to China, according to a news release from the U.S. Department of Justice. He was charged with accessing a computer without authorization to obtain protected information, as well as theft of trade secrets, according to the court documents filed in the U.S. District Court for the Western District of Virginia. According to the release, Hu had been studying bio-mimics and fluid dynamics at UVa. A screening conducted by authorities revealed that Hu was alleged to be in possession of bio-inspired research simulation software code that he was not authorized to possess, and which represented the result of years of research and resources in its development by members of the UVa academic community.

Read the full article here.

MITIGATING BRAIN DRAIN BY CONNECTING UNIVERSITIES

Peter van der Hijden and Marijk van der Wende | University World News | October 3, 2020

This week the European Commission published three policy communications with direct relevance for universities: one on the European Education Area, one on the European Research Area and one on a Digital Education Action Plan. A policy report, Towards a 2030 Vision on the Future of Universities in Europe, is to be released shortly. Earlier this summer, the commission published an equally interesting communication on a new European Skills Agenda. Excellence, sovereignty and inclusion figure prominently in these texts. So how does mobility fit into this agenda in a post-pandemic world? The COVID-19 recovery creates opportunities to align the European Union's green, digital and knowledge agendas. In order for universities to become leaner, cleaner and better employers and for their staff to find a better work-life balance, we need to rethink mobility. Mobility of students and staff is widely considered to have positive effects on the life and careers of the individuals concerned. It is part of the general EU objective of promoting the free movement of goods, persons, services and capital. Free movement is expected to allocate talent to the places where it is most productive to the benefit of all. Universities and research institutes will thus obtain the human resources they need to flourish.

Read the full article here.

ALERT (AA20-275A): POTENTIAL FOR CHINA CYBER RESPONSE TO HEIGHTENED U.S.–CHINA TENSIONS

U.S. Cybersecurity and Infrastructure Security Agency | October 1, 2020

In light of heightened tensions between the United States and China, the Cybersecurity and Infrastructure Security Agency (CISA) is providing specific Chinese government and affiliated cyber threat actor tactics, techniques, and procedures (TTPs) and recommended mitigations to the cybersecurity community to assist in the protection of our Nation's critical infrastructure. In addition to the recommendations listed in the Mitigations section of this Alert, CISA recommends organizations take the following actions.

1. Adopt a state of heightened awareness. Minimize gaps in personnel availability, consistently consume relevant threat intelligence, and update emergency call trees.

2. Increase organizational vigilance. Ensure security personnel monitor key internal security capabilities and can identify anomalous behavior. Flag any known Chinese indicators of compromise (IOCs) and TTPs for immediate response.

3. Confirm reporting processes. Ensure personnel know how and when to report an incident. The well-being of an organization's workforce and cyber infrastructure depends on awareness of threat activity. Consider reporting incidents to CISA to help serve as part of CISA's early warning system (see the Contact Information section below).

4. Exercise organizational incident response plans. Ensure personnel are familiar with the key steps they need to take during an incident. Do they have the accesses they need? Do they know the processes? Are various data sources logging as expected? Ensure personnel are positioned to act in a calm and unified manner.

Read the full alert here.

EC SETS OUT VISION FOR FUTURE OF EUROPEAN RESEARCH AREA

Brendan O'Malley | University World News | October 2, 2020

The European Commission has adopted a vision for a new European Research Area (ERA) to improve Europe's research and innovation landscape, accelerate the EU's transition towards climate neutrality and digital leadership, support its recovery from the societal and economic impact of the coronavirus crisis, and strengthen its resilience against future crises. It said the ERA, which was launched in 2000, should be "based on excellence" and be "competitive, open and talent-driven" and on 30 September 2020 set out key strategic objectives and actions which include improving access to facilities and infrastructure for researchers across the EU and strengthening the mobility of researchers and the free flow of knowledge and technology. The commission said the strategic objectives and actions would prioritise investments and reforms in research and innovation, improve access to excellence for researchers across the EU and enable research results to reach the market and the real economy. They would also promote skills and career development opportunities for researchers as well as gender equality and better access to publicly funded peer-reviewed science.

Read the full article here.

'SIGNIFICANT OVERREACH': UNIVERSITIES SAY AUSTRALIA'S FOREIGN VETO BILL ERODES AUTONOMY

Daniel Hurst | The Guardian | September 28, 2020

The Morrison government's proposed foreign veto laws are so broadly worded that universities may be required to hand over thousands of pages of documents every year to be checked, an inquiry has been told. Universities have also complained the legislation is so "extraordinarily wide" that it allows the foreign affairs minister to cancel agreements with international counterparts that may go against Australia's foreign policy, even if that policy isn't written down anywhere, publicly available or formally decided. In one of the most strongly worded submissions to an ongoing Senate inquiry into the proposal, the University of Western Australia said it had grave concerns about the bill, which should not be passed in its current form. UWA said institutional autonomy was "a central element of the free and vigorous higher education system which is essential to our economic and scientific progress and cultural enrichment". "It requires us to push back vigorously and without apology against proposals for the extension of executive power which may affect that autonomy without well-defined boundaries or limitations," UWA said.

Read the full article here.

DEPARTMENT OF DEFENSE COUNTER-INSIDER THREAT SOCIAL & BEHAVIORAL SCIENCE RESEARCH SUMMIT

The Threat Lab and the U.S. Department of Defense

The DoD C-InT SBS Summit is designed to deploy and share knowledge, strengthen relationships across the global C-InT Community of Practice, and integrate research into operations through delivery of relevant artifacts. This unique, virtual DoD C-InT SBS Summit will create meaningful match-ups among many stakeholders, including psychologists, analysts, researchers, law enforcement professionals, lawyers, HR personnel, and C-InT Program Managers.

Access the site here.

PREVENTING INSIDER THREATS: WHAT TO WATCH (AND WATCH OUT) FOR

Cynthia Brumfield | CSO | September 25, 2020

September is officially National Insider Threat Awareness Month (NIATM) and the theme of this year's NIATM is resilience. Of all the digital threats facing organizations, the insider threat can be the most vexing to tackle given how uncomfortable it can feel to suspect one's own colleagues of wrongdoing. It's challenging to set up systems and processes that might catch well-regarded peers or superiors in a harmful act. At last week's inaugural Insider Risk Summit, experts at corporations and cybersecurity firms gathered to talk about the top trends driving insider security threats and what security officers should know in trying to combat those threats. "There's not one type of threat but there is a common aspect, which is that [insiders] are looking to get at critical assets of the organization — people, information, technology and facilities," Michael Theis, chief engineer, Strategic Engagements at the US Community Emergency Response Team's (CERT's) National Insider Threat Center, said during his keynote talk.

Read the full article here.

IS THE US THE NEXT BIG MARKET FOR OUTBOUND STUDENTS?

Anthony C. Ogden and Denise Cope | University World News | October 3, 2020

There may be some major shifts under way in international student mobility patterns. The current upheavals in the United States higher education landscape appear to be driving greater numbers of US students to consider full degrees abroad. US universities and colleges were on the ropes prior to the COVID-19 pandemic, with many institutions already facing shrinking enrolments, budget crunches and stagnating public funding. Add COVID-19 to the mix and the challenges only get worse for US higher education. The cracks in the system are growing into chasms and the landscape may be forever changed. Over the past few years an energetic debate has emerged among educational leaders regarding the tenuous nature of US higher education. The range of opinions fall along two extremes: reassurance and panic. On the reassurance end, some are arguing for maintaining the status quo, offering polite mollifications that enrolment fluctuations and changes in disciplinary offerings are perfectly normal and there will be hardly any permanent disruption to higher education as we have known it. On the panic end, some are questioning the long-term viability of 'bricks and mortar' institutions and are calling for a broad rethinking of US higher education.

Read the full article here.

ZHENHUA DATA LEAK EXPOSES CHINA'S NEW 'HYBRID WARFARE'

Deutsche Welle | Taiwan News | September 29, 2020

More than 2 million people around the world have had their personal data collected on behalf of Chinese intelligence services, according to a leak of a dataset made public earlier this month by an Australian cybersecurity consultancy. The list includes prominent political figures like Boris Johnson and Narendra Modi and their families, business leaders like Ratan Tata, US military members of all ranks, senior diplomats, academics, celebrities, ordinary people, and even gangsters. The information was scraped mostly from open sources like social media profiles by a Chinese big-data harvesting company called Shenzhen Zhenhua Data Information Technology. Zhenhua provides data-based intelligence services. According to analysts, its two main clients are China's Ministry of State Security and the People's Liberation Army.

Read the full article here.

COMMUNIST CHINA'S INFLUENCE OPERATIONS: INDIA'S THINK-TANKS, POLITICIANS, INTELLECTUALS, ACADEMIA, MEDIA ARE TARGETS

Abhinav Pandya | Sunday Guardian Live | September 26, 2020

India's strategic experts, intelligence apparatus, political leadership, and the majority of the academic community failed and did so rather abysmally in understanding and preventing China's penetration in India's innards, i.e., our social, political, educational, and a plethora of other institutions. The consequent internal sabotage was evident in full steam during the ongoing India-China standoff. When China with its deceit and treachery in full bloom, was intruding into Indian territory, one could witness an entire brigade of security analysts, think tank community, academicians, politicians and media organisations promoting and protecting Chinese strategic interests with passionate zeal and fervour, which could only come if there is an uninterrupted flow of dollars from invisible foreign hands. Clive Hamilton and Mareike Ohlberg have exposed how the Chinese Communist Party is shaping the global order in their classic work, "Hidden Hand: Exposing How the Chinese Communist Party is Reshaping the World." They write, "The Party's program of influence and interference is well planned and bold, and backed by enormous economic resources and technological power.

Read the full article here.

UK TO EXCLUDE CHINESE STUDENTS FROM SENSITIVE SUBJECTS - TIMES

Reuters | October 1, 2020

Britain is to tighten rules about which subjects foreign students can study at its universities in a move to prevent the theft of intellectual property by Chinese students, the Times newspaper reported on Thursday. Under Britain's Academic Technology Approval Scheme (ATAS), postgraduate applicants from abroad already require security vetting to study subjects where their knowledge could be used in weapons programmes, according to a government website. The Times report said the list of subjects would be expanded to include areas related to cyber-security and aircraft, among others. Asked to comment on the report, the Foreign Office said the government had implemented a recent expansion of ATAS to cover military technology, to ensure Britain's safeguards were keeping up with ever-changing global threats.

Read the full article here.

AMERICAN LEADERS SOLD A DREAM OF CHANGING CHINA

Zachary Haver | Foreign Policy | September 29, 2020

After over 40 years of engagement, China has grown increasingly illiberal at home and assertive abroad. Beijing's deepening authoritarianism and aggressive nationalism have sparked a heated debate among policy analysts, former government officials, academics, and others about whether the United States got China wrong. At the heart of this conversation lies the contentious question of whether the United States even sought to change China in the first place. Defenders of engagement, many of whom built their own professional careers around the notion, claim that American politicians and officials never aimed to transform the People's Republic of China into a liberal democracy or a close partner of the United States. Some argue that "the goal was to shape Chinese policy to align more with U.S. objectives" in terms of "a more open society, reduced overseas disruptive behavior, increasingly transparent business operations."

Read the full article here.

DEFENSE INNOVATION IS FALLING SHORT

Christopher Zember and Peter Khooshabeh | War on Rocks | September 25, 2020

After six years of dedicated effort, the Pentagon's innovation initiatives are still far from meeting their goal. Despite some notable successes, the Defense Department is missing a key opportunity to deliver on its promise of putting transformational technologies into the hands of U.S. servicemembers. Over the past several years, there has been a significant increase in Defense Department offices and initiatives focused on engaging the commercial high-tech marketplace: the Defense Innovation Unit, MD5 (now the National Security Innovation Network), SOFWERX, AFWERX, NavalX — the list goes on. Meanwhile, the defense research enterprise has continued its practice of close collaboration with the academic community. While there are many similarities between the research and commercial high-tech communities, they tend to operate in parallel stovepipes, each with its own set of challenges and limitations. If we break down these stovepipes, we will find that each contains the means to address the shortcomings of the other. Researchers can help venture capitalists and startups access the most cutting-edge science.

Read the full article here.

NIST UNVEILS UPDATED GUIDE TO PRIVACY, SECURITY CONTROLS

Akshaya Asokan | Bank Info Security | September 24, 2020

The U.S. National Institute of Standards and Technology this week released a long-awaited guidance update, Special Publication 800-53 Revision 5, describing "next-generation security and privacy controls" and how to use them. It's the first time since 2013 that NIST has updated the document, which addresses the cybersecurity risks faced by federal government agencies as well as organizations in the private sector and offers guidelines on mitigating risks, protecting data and stopping breaches. "This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations and the nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities and privacy risks," according to the document. The update provides a list of security and privacy controls for managing IT systems, with a special emphasis on those that process or store personally identifiable information.

Read the full article here.

A CYBER CAUTIONARY TALE: UNNAMED AGENCY SUFFERS SOPHISTICATED, POSSIBLY NATION STATE, ATTACK

Jason Miller | Federal News Network | September 25, 2020

A virtual private network vulnerability that has been known since December. Stolen credentials of a power user. A poorly configured firewall. It didn't take long for the hacker to own this unnamed federal agency. In what was a matter of days, maybe weeks, this bad actor, possibly a nation state given how sophisticated the attack was, set up two remote command-and-control points, reviewed email and other documents to look for passwords and started networking hopping to find more valuable data and information. And now the Cybersecurity and Infrastructure Security Agency at the Homeland Security Department is laying out what happened with depth and specificity rarely seen in a public way. Without a doubt, CISA is telling other agencies, "Don't let this happen to you." The use case, gently titled "Federal Agency Compromised by Malicious Cyber Actor" is a detailed example of what happens when your agency's cyber hygiene is poor and exacerbated by the surge in remote workers.

Read the full article here.

U.S. PROBES OF CHINESE RESEARCHERS DRAW MORE ORGANIZED OPPOSITION

Aruna Viswanatha | The Wall Street Journal | October 1, 2020

The Justice Department's effort to prosecute some Chinese researchers in the U.S. accused of hiding their ties to the Chinese government is facing increasing pushback from some academics and Chinese-American groups. New York University's Brennan Center and several Asian-American groups hosted a panel discussion on Wednesday night described as the first in a series titled: "The Human and Scientific Costs of the 'China Initiative'," referring to a broader Justice Department push that includes the university cases.

Read the full article here.