ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

September 21, 2022

MID-DECADE CHALLENGES TO NATIONAL COMPETITIVENESS

Special Competitive Studies Project | September 2022

Today Americans need a new unity of purpose. Three decades of American beliefs about themselves, their government, and their place in the world have been shaken. In the midst of a wave of technological change, we are left with questions about the future of democracy, rising geopolitical danger, and disorientation about where we are heading. We created the Special Competitive Studies Project (SCSP) to develop an agenda that can help Americans recapture the confidence to face these challenges with a shared sense of national purpose. SCSP's mission is to make recommendations to strengthen America's long-term competitiveness for a future where artificial intelligence (AI) and other emerging technologies reshape our national security, economy, and society. The premise of our work is straightforward. Strategic competition between the United States and the People's Republic of China (PRC) is the defining feature of world politics today. The epicenter of the competition is the quest for leadership and dominant market share in a constellation of emerging technologies that will underpin a thriving society, growing economy, and sharper instruments of power.

Read the full article here.

NATIONAL INSIDER THREAT AWARENESS MONTH 2022

Security Staff | Security | September 8, 2022

September is National Insider Threat Awareness Month, which emphasizes the importance of safeguarding enterprise security, national security and more by detecting, deterring and mitigating insider risk. The risks of espionage, violence, unauthorized disclosure and unknowing insider threat actions are higher than ever; therefore, maintaining effective insider threat programs is critical to reducing any security risks and increasing operational resilience. National Insider Threat Awareness Month is an opportunity for enterprise security, national security and all security leaders to reflect on the risks posed by insider threats and ensure that an insider threat prevention program is in place and updated continuously to reflect the evolving threat landscape. Recent examples of insider threats include: In August 2022, a federal jury in California convicted Ahmad Abouammo, a former manager at Twitter, of acting as an unregistered agent of Saudi Arabia and other violations. In July 2022, a federal jury in New York convicted former CIA programmer Joshua Schulte of violations stemming from his theft and illegal dissemination of highly classified information. Harboring resentment toward the CIA, the programmer had used his access at CIA to some of the country's most valuable intelligence-gathering cyber tools to covertly collect these materials and provide them to WikiLeaks, making them known to the public and to U.S. adversaries.

Read the full article here.

DEPARTMENT OF DEFENSE ISSUES INTERIM RULE REQUIRING DISCLOSURE OF CHINESE WORKFORCE AND FACILITIES

Cara Lasley, Kevin Maynard, Hon. Nazak Nikakhtar, and Lisa Rechden | Wiley Rein LLP | JD Supra | August 31, 2022

The Department of Defense (DoD) issued an interim rule requiring certain Defense contractors and subcontractors to disclose the use of workers and facilities in People's Republic of China (PRC). The rule, which implements Section 855 of the FY22 NDAA, amends the Defense Federal Acquisition Regulation Supplement (DFARS) to add clauses requiring pre-award and post-award disclosures, as well as award restrictions, on covered entities who maintain facilities or employ one or more individuals who perform work in the PRC in connection with covered DoD contracts. The new DFARS clauses require disclosures by a "covered entity"—that is, a company performing work on a DoD contract or subcontract with a value over $5 million, excluding contracts for commercial products or commercial services, that performs work in the PRC. ursuant to the interim rule, covered entities (and their subcontractors) must disclose (1) the number of individuals that will or do perform work in the PRC and (2) a description of the entity's physical presence (or proposed physical presence) in the PRC.

Read the full article here.

TIKTOK WON'T COMMIT TO STOPPING US DATA FLOWS TO CHINA

Brian Fung | CNN Business | September 14, 2022

TikTok repeatedly declined to commit to US lawmakers on Wednesday that the short-form video app will cut off flows of US user data to China, instead promising that the outcome of its negotiations with the US government "will satisfy all national security concerns." Testifying before the Senate Homeland Security Committee, TikTok Chief Operating Officer Vanessa Pappas first sparred with Sen. Rob Portman over details of TikTok's corporate structure before being confronted — twice — with a specific request. "Will TikTok commit to cutting off all data and data flows to China, China-based TikTok employees, ByteDance employees, or any other party in China that might have the capability to access information on US users?" Portman asked. The question reflects bipartisan concerns in Washington about the possibility that US user data could find its way to the Chinese government and be used to undermine US interests, thanks to a national security law in that country that compels companies located there to cooperate with data requests.

Read the full article here.

FEARS GROW OF RUSSIAN SPIES TURNING TO INDUSTRIAL ESPIONAGE

Alexander Martin | The Record | September 14, 2022

Russia acknowledged this week that parts of its technology industry are dependent on foreign knowledge and lagging competitors by more than a decade, raising concerns that the country's cyber spies will be used for industrial espionage. Experts told The Record that Western companies should be on "full alert" for attacks from Moscow's intelligence services. President Vladimir Putin has suggested in recent months that the country's Foreign Intelligence Service (SVR) should support technological development as the country deals with mounting sanctions. The admission about the state of Russia's microelectronics industry is contained in a new strategic policy document from the Ministry of Industry and Trade, reported Tuesday by Kommersant. It lists a number of acute problems facing Russia's domestic technology industry, including its dependence on foreign intellectual property; its lack of production capacity; and Russia being unattractive to investors.

Read the full article here.

WILL MORE STUDIES BE CLASSIFIED?

Kent Anderson | The Geyser | September 14, 2022

One of the more intriguing details in the recent OSTP guidance comes when you follow a footnote. The OA and open science enthusiasts writing the OSTP materials may have framed this citation incorrectly. In essense, this misreading and other hints at a less robust embrace of "open" may hint at unintended consequences. First, a refresher. In the "Economic Landscape of Federal Public Access Policy" document submitted to Congress at the time the OSTP statement was released, there is a citation to a document from the Reagan Administration. This document was cited to justify the claim that the US government has wanted "unrestricted access" to scientific research for a long time. Unfortunately, that's not what the cited document says. Written at the height of the Cold War, this 1985 unclassified "national security decision" states that fundamental scientific and engineering research funded by the US government should remain "unrestricted" to "the maximum extent possible."

Read the full article here.

A CHINESE SPY WANTED GE'S SECRETS, BUT THE US GOT CHINA'S INSTEAD

Jordan Robertson and Drake Bennett | Bloomberg | September 14, 2022

In January 2014, Arthur Gau, an aerospace engineer who was nearing retirement age, received an unexpected email from a long-lost acquaintance in China. Years before, Gau had made a series of trips from his home in Phoenix to speak at the Nanjing University of Aeronautics and Astronautics, or NUAA, one of China's most prestigious research institutions. The original invitation had come from the head of a lab there studying helicopter design. Increasingly, however, Gau had heard from someone else, a man who worked at the university in a vague administrative capacity. Little Zha, as the man called himself, was the one who made sure Gau never had to pay his own airfare when he came to give talks. When Gau brought his mother on a 2003 visit, Zha arranged and paid for them to take a Yangtze cruise to see the river's dramatically sculpted middle reaches before they were flooded by the Three Gorges Dam. The relationship had ended awkwardly, though, when Zha offered Gau money to come back to China with information about specific aviation projects from his employer, the industrial and defense giant Honeywell International Inc. Gau ignored the request, and the invitations stopped.

Read the full article here.

PROFESSOR IN LENGTHY TRIAL OVER IRANIAN SCIENTISTS' VISITS

Jan Petter Myklebust | University World News | September 14, 2022

A former tenured professor who invited four Iranian scientists to work at his university in Trondheim in Norway is currently on trial for a string of charges including violation of the new regulations on the export of scientific knowledge and a breach of the Iran sanctions. The trial, which started in the Oslo District Court on 5 September 2022, is expected to last 25 days. The scientist, who worked at the Norwegian University of Science and Technology (NTNU) at the time and is now based in Qatar, has pleaded not guilty to all charges. He faces up to 10 years in prison. The scientist was suspended, along with a colleague, in January 2020 after an investigation by the Norwegian Police Security Service (PST). At the time, both scientists were tenured staff members at NTNU. The charges against the second scientist were subsequently dropped. The former NTNU professor, who is of German and Iranian descent, is accused of inviting four Iranian citizens as guest academics to NTNU during the course of 2018 and 2019 without the consent of the university and giving them access to university facilities, which included a scanning electron microscope (SEM), without applying for the necessary licence from the Ministry of Foreign Affairs.

Read the full article here.

THE CYBER SECURITY HEAD GAME

Eric Haseltine | Psychology Today | September 12, 2022

Recently, the cyber arm of Homeland Security, CISA, announced a new, North Korean sponsored ransomware attack on health care systems, and the Center for Strategic and International Studies just listed 89 major international cyberattacks in 2022 alone, including a recent China-sponsored compromise of vital telecommunication systems. As if these incidents weren't sobering enough, CISA also warned that Russia, in retaliation for US support of Ukraine, could compromise vital US infrastructure such as mobile networks, banks, power and energy systems, in the same way Russian hackers took down the Colonial Pipeline system last year, causing severe fuel shortages. In sum, we find ourselves in a never-ending, low-level global cyber conflict that threatens to erupt into a major cyber war at any time… and we are not winning that conflict. As the former CTO of the US Intelligence Community and current Chairman of the Board of the US Technology Leadership Council, I can say with confidence that the problem isn't our technology. We invented the internet and still have the deepest technical resources of any country in the world, so our cyber defenses, including access controls, anti-malware, firewalls, secure computing platforms, intrusion/data loss detection systems and AI cyber defense systems are second to none.

Read the full article here.

FOREIGN INTELLIGENCE ENTITIES' RECRUITMENT PLANS TARGET CLEARED ACADEMIA

Defense Counterintelligence and Security Agency | April 2021

Foreign Intelligence entities (FIE)[i], specifically China and Russia, use academic talent recruitment plans and academic excellence initiatives to collect U.S. scientific research and technologies in a strategic effort to enhance their militaries and economies. China and Russia often utilize foreign students accepted to U.S. universities or at postgraduate research programs to collect sensitive U.S. Government information and/or technology. Additionally, Iran uses government-sponsored initiatives to persuade students studying abroad to return and share their knowledge. FIE target U.S. subject matter experts (SMEs), professors, and researchers in order to obtain sensitive U.S. Government information and technology. While foreign government-sponsored talent recruitment plans and academic excellence initiatives promote international cooperation in science and technology research, these programs are often part of a broader whole-of-government strategy to obtain U.S. scientific-funded research and/or technology through government-run or government-funded programs.

Read the full article here.

IMPERIAL COLLEGE TO CLOSE TWO RESEARCH VENTURES WITH CHINA

The Guardian | University World News | September 14, 2022

Imperial College London in the United Kingdom will shut down two major research centres sponsored by Chinese aerospace and defence companies amid a crackdown on academic collaborations with China, writes Hannah Devlin for The Guardian. The AVIC Centre for Structural Design and Manufacture is a long-running partnership with China's leading civilian and military aviation supplier, which has provided more than £6 million (US$7 million) to research cutting-edge aerospace materials. The second centre is run jointly with BIAM, a subsidiary of another state-owned aerospace and defence company, which has contributed £4.5 million for projects on high-performance batteries, jet engine components and impact-resistant aircraft windshields. The centres' stated goals are to advance civilian aerospace technologies, but critics have repeatedly warned that the research could also advance China's military ambitions.

Read the full article here.

CHINA IS RUNNING COVERT OPERATIONS THAT COULD SERIOUSLY OVERWHELM US

Nigel Inkster | The New York Times | September 14, 2022

In my three-decade career with Britain's Secret Intelligence Service, China was never seen as a major threat. If we lost sleep at night, it was over more immediate challenges such as Soviet expansionism and transnational terrorism. China's halting emergence from the chaotic Mao Zedong era and its international isolation after Chinese soldiers crushed pro-democracy demonstrations at Tiananmen Square in 1989 made it seem like an insular backwater. It's a different picture today. China has acquired global economic and diplomatic influence, enabling covert operations that extend well beyond traditional intelligence gathering, are growing in scale and threaten to overwhelm Western security agencies. The U.S. and British domestic intelligence chiefs — the F.B.I. director, Christopher Wray, and the MI5 director general, Ken McCallum — signaled rising concern over this with an unprecedented joint news conference in July to warn of, as Mr. Wray put it, a "breathtaking" Chinese effort to steal technology and economic intelligence and to influence foreign politics in Beijing's favor. The pace was quickening, they said, with the number of MI5 investigations into suspected Chinese activity having increased sevenfold since 2018.

Read the full article here.