ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

November 17, 2021

CHINA STILL STEALS COMMERCIAL SECRETS FOR ITS OWN FIRMS' PROFIT

The Economist* | *November 11, 2021

Earlier this year Microsoft found that a group of hackers, which it called Hafnium, had broken into hundreds of thousands of computer servers around the world that were running the firm's mail and calendar software. The cyber-thieves were stealing emails, documents and other data from small businesses, ngos and local governments in an enormous, seemingly indiscriminate, cyber-attack. In July America, Britain, other members of nato and the European Union all blamed China. America was more specific. It named China's civilian intelligence agency, the Ministry of State Security (mss). Such co-ordinated condemnation condemnation of the Chinese government for allegedly hacking into foreign computer systems was unprecedented. But it was no surprise in the West that China appeared to be responsible (as always in such cases, it denied involvement).

Read the full article here.

OPINION: WE SPENT A YEAR INVESTIGATING WHAT THE CHINESE ARMY IS BUYING. HERE'S WHAT WE LEARNED.

Ryan Fedasiuk* | *Politico* | *November 10, 2021

Last week, the U.S. Department of Defense released its annual report on Chinese military power, mentioning "artificial intelligence" 20 separate times. The report echoed longstanding concerns that the Chinese People's Liberation Army is investing heavily in "intelligentized warfare" — a strategy based on making weapons systems and military operations more networked and autonomous — and that artificial intelligence may be "changing the future of warfare faster than expected." The so-called arms race for AI has come to define debates about the competition between the United States and China. The idea that the two nations are racing to dominate in AI — and, in particular, that China is surging ahead in this race — has garnered high-profile supporters as well as skeptics. But while much discussion, including the DoD report, has focused on China's longer-term grand plans to become an AI superpower, it has been less clear what the country is doing in the short term to make those ambitions a reality. Over the past year, I was part of a team of researchers at the Center for Security and Emerging Technology that sifted through 350 Chinese military equipment contracts related specifically to AI. The sample we analyzed is part of a larger, publicly available dataset of 66,000 procurement records published between April and November 2020.

Read the full article here.

EXCLUSIVE CHINESE EMBASSY LOBBIES U.S. BUSINESS TO OPPOSE CHINA BILLS - SOURCES

Michael Martina | Reuters | November 15, 2021

China has been pushing U.S. executives, companies and business groups in recent weeks to fight against China-related bills in the U.S. Congress, four sources familiar with the initiative told Reuters, in letters to and meetings with a wide range of actors in the business community. China's embassy in Washington had sent letters pressing executives to urge members of Congress to alter or drop specific bills that seek to enhance U.S. competitiveness, according to the sources and the text of a letter sent by the embassy's economic and commercial office seen by Reuters. Chinese officials warned companies they would risk losing market share or revenue in China if the legislation becomes law, according to the text of the letter. The sources said China's request also left some individuals who received a letter concerned that they could be seen as violating the Foreign Agents Registration Act (FARA) if they lobbied lawmakers on similar issues in the future. As a result, none of the sources wanted to be identified as having received or seen the letter.

Read the full article here.

FBI: IRANIAN THREAT ACTOR TRYING TO ACQUIRE LEAKED DATA ON US ORGANIZATIONS

Catalin Cimpanu | The Record | November 12, 2021

The US Federal Bureau of Investigation says that a threat actor known to be associated with Iran is currently seeking to acquire data from organizations across the globe, including US targets. The actor has demonstrated interest in leaked data sets in various locations, including web forums and the dark web. The FBI judges this actor may attempt to leverage information in these leaked data sets, such as network information and email correspondence, to conduct their own cyber operations against US organizations. The FBI said the threat actor wasn't interested in a particular industry vertical but was seeking data in bulk. "This actor has also demonstrated interest in obtaining unauthorized access to SCADA systems using common default passwords," the agency added. The FBI is now asking companies that have been at the center of a past hack where the data was leaked online to ensure that the leaked data can't be abused to breach them again.

Read the full article here.

U.S. OFFICIALS WARN TECH COMPANIES OF FOREIGN THREATS IN FIVE KEY AREAS

Sabri Ben-Achour, Alex Schroeder and Rose Conlon | Market Place | November 12, 2021

The U.S. intelligence community has some advice for American tech companies: If you're going to do business with foreign partners like China and Russia, be smart about it. In recent weeks, U.S. intelligence officials launched a campaign to warn American companies in emerging industries — artificial intelligence, quantum information systems, biotechnology, semiconductors and autonomous systems — about their interactions with business partners in countries like China and Russia. The goal is to make American firms aware of what they might be getting themselves into when they work with foreign investors and collaborators. Part of the worry is illegal attempts to steal intellectual property, like cyber attacks and data theft. Michael Orlando, acting director of the National Counterintelligence and Security Center, a branch of the U.S. intelligence community that focuses on threats from foreign powers, also cautions about legal interactions where companies may be unknowingly putting themselves, their data and their intellectual property at risk.

Read the full article here.

FINAL REPORT: NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

National Security Commission on Artificial Intelligence

No comfortable historical reference captures the impact of artificial intelligence (AI) on national security. AI is not a single technology breakthrough, like a bat-wing stealth bomber. The race for AI supremacy is not like the space race to the moon. AI is not even comparable to a general-purpose technology like electricity. However, what Thomas Edison said of electricity encapsulates the AI future: "It is a field of fields … it holds the secrets which will reorganize the life of the world." Edison's astounding assessment came from humility. All that he discovered was "very little in comparison with the possibilities that appear." The National Security Commission on Artificial Intelligence (NSCAI) humbly acknowledges how much remains to be discovered about AI and its future applications. Nevertheless, we know enough about AI today to begin with two convictions.

Read the full article here.

FINISH UNIVERSITIES PREPARE GUIDELINES ON POTENTIAL CHALLENGES WHEN COOPERATING WITH CHINA

Gregers Moller | ScandAsia | November 9, 2021

Finland's Ministry of Education and Culture in cooperation with Finnish universities and the Ministry for Foreign Affairs are preparing its own guidelines for the university and science community due to the risks and threats regarding espionage involved in university and research collaboration with Chinese partners, YLE reports. China is world-leading in several scientific disciplines and for universities wanting to stay at the cutting edge, collaboration with Chinese partners is important. At the same time, the EU has several projects underway to ensure safer cooperation with China, and the first EU-wide recommendations are set to be published soon. According to the Finnish Security Intelligence Service (Supo), the level of risk related to China has increased in the Nordic country as well and Finland's guidelines are expected to be published in December. Mari-Anna Suurmunne, a senior specialist in education and science at Finland's Embassy in Beijing says to YLE that the guidelines aim to raise awareness of the potential challenges related to cooperation with China.

Read the full article here.

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) 2.0 UPDATES AND WAY FORWARD

Federal Register Notice from the Department of Defense | November 17, 2021

This document provides updated information on DoD's way forward for the approved Cybersecurity Maturity Model Certification (CMMC) program changes, designated as ''CMMC 2.0.'' CMMC 2.0 builds upon the initial CMMC framework to dynamically enhance Defense Industrial Base (DIB) cybersecurity against evolving threats. The CMMC framework is designed to protect sensitive unclassified information that is shared by the Department with its contractors and subcontractors and provide assurance that Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) will be protected at a level commensurate with the risk from cybersecurity threats, including Advanced Persistent Threats. Under the CMMC program, DIB contractors will be required to implement certain cybersecurity protection standards, and, as required, perform self-assessments or obtain third-party certification as a condition of DoD contract award.

Read the full article here.

MINISTRY SHUTS CAMPUS OFFICE FOR POACHING TECH TALENT FOR CHINA

Mimi Leung | University World News | November 11, 2021

The Ministry of Education stepped in to prevent the poaching of high technology talent in Taiwan, as it shut down a campus office at a major university this week that it said was being used to recruit semiconductor workers for China. The ministry warned universities that "non-academic exchanges" with mainland China were unlawful. Amid heightened geopolitical tensions between Beijing and Taipei, and global competition for scientific talent in advanced technologies such as semiconductors, as well as China's own efforts to become self-sufficient in high tech, the ministry's move highlighted the sensitivity of research and talent in these areas. In September the Taiwan government proposed tightening existing laws governing its relations with Beijing to prevent China stealing "national core technology", including through industrial espionage and talent poaching. It did not define national core technology, but Taiwan is a global leader in semiconductor technology and production. Education Minister Pan Wen-chung responded to questions during a 9 November legislative hearing, after media reports that an office on the campus of Taiwan's National Tsing Hua University (NTHU) in Hsinchu City was set up as a 'cover' to recruit talent from Taiwan for China's lagging semiconductor industry.

Read the full article here.

AUSTRALIAN UNIVERSITIES' ALLURE DIMS FOR CHINESE, INDIAN STUDENTS

John Power | Al Jazeera | November 10, 2021

Before the COVID-19 pandemic hit, Raj Kiran Grewal, who lives in Mohali in India's Punjab state, saw Australia as the ideal place to do her MBA. But after spending 20 months trying to get around the country's ultra-strict border controls, Grewal is so sick of "false hopes" that she is considering studying in the United States or Canada instead. "Australia is definitely not the right option as they just want the money from international students and they do not care about the rest," Grewal said. "I am really frustrated with the way the college and immigration treated the stranded overseas people including international students, and family members of the people living in Australia as well," she added, explaining how she deferred her course when Australia shut its borders in early 2020 only for her university to cancel her enrollment after she declined to accept the option of studying online. Grewal is one of many international students who have looked elsewhere during Australia's self-imposed isolation, raising fears of long-lasting damage to one of the country's most lucrative industries. Students from China, India and other Asian countries have long been drawn to Australia to study due to its high-ranking universities, English-speaking environment and comfortable lifestyle. Before the pandemic, international education contributed 40 billion Australian dollars ($29.5bn) to the economy, making the sector the fourth-largest export after iron ore, coal and gas.

Read the full article here.

OPEN LETTER TO DR. ERIC LANDER RE: NSPM-33

Asian American Scholar Forum | November 9, 2021

In November 2021, AASF sent the following letter to Dr. Eric Lander, Director of the Office of Science and Technology Policy and Science Advisor to the President, to express the importance of open science and academic freedom, and to submit our comments regarding the implementation of National Security Presidential Memorandum-33 (NSPM-33), "Presidential Memorandum on United States Government Support Research and Development National Security Policy."

Read the full article here.

UNIVERSITIES TELL STRANDED INTERNATIONAL STUDENTS TO PREPARE FOR RETURN TO CAMPUS IN CHINA

Mimi Lau | South China Morning Post | November 11, 2021

Two international universities in China have told their overseas students to prepare for a return to campus as early as March, after they were shut out of the country because of the pandemic. While there has been no official announcement on when China's borders will reopen to foreign students, Duke Kunshan University in Suzhou and New York University Shanghai have both sent out emails saying they could be allowed back on campus in time for the next semester. China's borders have been closed to most foreigners since March 2020, with special exemptions granted for work or family reasons, as part of its zero-tolerance strategy to Covid-19. That has left many of the country's half a million international students stranded overseas and unable to attend classes in person. International students have taken to social media to appeal to Chinese authorities to grant them visas so they can return to the country to continue their university studies, including via the Twitter campaign #TakeUsBackToChina.

Read the full article here.

CONTROLLED UNCLASSIFIED INFORMATION

Defense Counterintelligence and Security Agency

What is CUI?CUI is government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide policies. CUI is not classified information. It is not corporate intellectual property unless created for or included in requirements related to a government contract. Why is it important? Because there are fewer controls over CUI as compared to classified information, CUI is the path of least resistance for adversaries. Loss of aggregated CUI is the one of the most significant risks to national security, directly affecting lethality of our warfighters. How is CUI management changing? In March 2020, DoD Instruction 5200.48 directed DCSA with eight responsibilities related to CUI. During the first half of 2021, DCSA developed an implementation plan to execute these responsibilities and will be utilizing a phased approach to operationalize its CUI responsibilities beginning October 1, 2021.

Read the full article here.

SUPPLY-CHAIN VULNERABILITIES AND 4 OTHER THREATS TO THE US THAT THE FBI DIRECTOR IS WORRIED ABOUT

Stavros Atlamazoglou | Business Insider | November 9, 2021

During a Senate hearing in September, the FBI director described what the agency sees as the top four threats facing the US. FBI Director Christopher Wray told the Senate Committee on Homeland Security and Governmental Affairs that foreign terrorist organizations, homegrown violent extremists, cyberattacks, and malign foreign influence present the biggest threats to the US. In addition to the four threats the FBI has identified, the wider intelligence community and the Department of Defense have also highlighted that supply-chain vulnerabilities pose an additional threat to US national security and private industry. The threats come from both state and non-state actors, with China and Russia behind some of the challenges. Domestic terrorists are high on the FBI's threat list. The FBI categorizes Domestic Violent Extremists (DVEs) as individuals who commit violent criminal acts to further socio-political goals and who have been influenced by domestic factors, including racial, ethnic, anti-government, or anti-authority views.

Read the full article here.

OFFICIAL SAYS DOD, WITH HELP FROM PARTNERS, ON CUSP OF CUTTING-EDGE INNOVATIONS

David Vergun | U.S. Department of Defense | November 8, 2021

Artificial intelligence, quantum computing, bioengineering and other leap-ahead technologies were topics addressed by the undersecretary of defense for research and engineering. Heidi Shyu provided keynote remarks today at the virtual Carnegie Mellon University Software Engineering Institute's Research Review 2021. "The challenges facing our military are both diverse and complex, ranging from sophisticated cyberattacks to supply chain risks, to defense against hypersonic missiles, to responding to biothreats. To address these challenges, the department must harness the incredible innovation ecosystem, both domestically and globally, in order to stay ahead of our adversaries," Shyu said. "I believe the way to build confidence amidst the technology disruptions is to embrace these changes and move forward rapidly. Furthering science, technology and innovation across the department could not be more important than it is today. Many potential adversaries will have greater access to commercial state-of-the-art technologies than ever before, and that could greatly disrupt our nation. We cannot afford a leveling of technology advantage," she said.

Read the full article here.

THE TEXAS A&M
UNIVERSITY SYSTEM

The Academic Security and Counter Exploitation Program is coordinated by The Texas A&M University System Research Security Office as a service to the academic community.
https://rso.tamus.edu