RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE
THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary

November 7, 2024

REGISTRATION NOW OPEN FOR THE ASCE 2025 ANNUAL SEMINAR FEBRUARY 25-27, TO BE HELD AT TEXAS A&M UNIVERSITY

Born from a commitment to safeguarding the integrity of academic research, the Academic Security and Counter Exploitation (ASCE) program, spearheaded by The Texas A&M University System's RISC Institute, fosters a sense of community among university research security professionals, uniting them in a collaborative defense against emerging threats. Since its inception in 2016, ASCE has been a beacon in the fight against foreign influence, equipping academic institutions with the knowledge and tools needed to protect their invaluable research. Now in its ninth year, the annual ASCE Seminar stands as the preeminent gathering for training, networking, and collaboration, laser-focused on fortifying the academic research enterprise.

View the full resource here.

ASCE 2025 CALL FOR PROPOSALS

If you would like to present, please submit your proposal by clicking on the link below.
The seminar committee will review all proposals, and the selection will be based on relevance to the seminar theme, quality of the abstract, and potential audience engagement. Presenters will be notified of acceptance or rejection no later than December 15, 2024.

The submission deadline is November 15, 2024.

View the full resource here.

TOP US OFFICIAL WARNS OF 'LARGE UPTICK' IN FOREIGN SPIES TARGETING TECH COMPANIES, THREATENING NATIONAL SECURITY

Mike Levine | ABC News | October 29, 2024

The nation's chief counterintelligence officer, Mike Casey, is warning of a "large uptick" in foreign spies trying to secretly infiltrate tech companies in the United States so they can steal America's latest innovations. According to Casey, America's own economy and national security -- even democracy itself -- are at stake, with China in particular looking to use stolen technologies to crush U.S. competitors, squeeze civil liberties inside China, and boost China's military might. "We're not perfect, but I don't want to live in the dystopian version of the [People's Republic of China]," joked Casey, who as director of the U.S. National Counterintelligence and Security Center coordinates and guides the nation's counterintelligence activities. Casey said that over the past two years, as U.S. companies began to heed warnings about questionable investments from China, the U.S. intelligence community has seen a spike in China's use of front companies and other proxies to access start-up companies and then steal their new technologies. By Casey's own description, at least some of what drives his concern is classified U.S. intelligence, which presents a "huge challenge" for U.S. officials who want to persuade start-up executives with no security clearance -- and little money -- to be very careful in choosing investors and partners.

Read the full article here.

EXCLUSIVE: CHINESE RESEARCHERS DEVELOP AI MODEL FOR MILITARY USE ON BACK OF META'S LLAMA

James Pomfret and Jessie Pang | Reuters | November 1, 2024

Top Chinese research institutions linked to the People's Liberation Army have used Meta's publicly available Llama model to develop an AI tool for potential military applications, according to three academic papers and analysts. In a June paper reviewed by Reuters, six Chinese researchers from three institutions, including two under the People's Liberation Army's (PLA) leading research body, the Academy of Military Science (AMS), detailed how they had used an early version of Meta's Llama as a base for what it calls "ChatBIT". The researchers used an earlier Llama 13B large language model (LLM) from Meta (META.O), opens new tab, incorporating their own parameters to construct a military-focused AI tool to gather and process intelligence, and offer accurate and reliable information for operational decision-making. ChatBIT was fine-tuned and "optimised for dialogue and question-answering tasks in the military field", the paper said. It was found to outperform some other AI models that were roughly 90% as capable as OpenAI's powerful ChatGPT-4.

Read the full article here.

NEW-ERA POLICIES AIM TO HALT EROSION OF ACADEMIC FREEDOM

Peter Maassen | University World News | October 30, 2024

Faced with growing worries about academic freedom in the European Union, the European Parliament launched an Academic Freedom Forum (EP Forum for Academic Freedom) in 2022. The studies undertaken for the forum show that academic freedom is eroding in practically all EU member states. The EP Forum contributes to a wider set of initiatives aimed at getting a better understanding of the threats to academic freedom, and ways in which the promotion and protection of academic freedom in Europe can be enhanced. In most societies around the world, academic freedom is acknowledged and legally protected as a fundamental value and principle in higher education and is seen as a necessary condition for attaining high quality academic education and research.

Read the full article here.

CHINESE AISI COUNTERPARTS

Karson Elmgren and Oliver Guest | IAPS | October 2024

In late 2023, the US and UK established AI Safety Institutes (AISIs)— government-backed technical institutions that focus on the safety of advanced AI systems. Other jurisdictions, such as Japan and Singapore, have followed in establishing AISIs with varying degrees of similarity. There is also an "International Network of AISIs", bringing together various AISIs and "equivalent government-backed scientific office[s]." The first meeting of this network is scheduled for November 2024. While there have been rumors that an AISI will be established in China, the country has not joined the trend. China is also not part of the International Network, though Commerce Secretary Raimondo has implied that individual Chinese scientists might be invited to the November meeting.

Read the full article here.

MITIGATING AUSTRALIA'S CLOUD-COMPUTING RISKS IS STILL WORK IN PROGRESS

Andrew Horton | ASPI | October 28, 2024

The appeal of cloud computing is undeniable. It provides remarkable scalability, cost-efficiency and agility, qualities that attract government and business. However, for all its benefits, there are also risks, not least of which is maintaining sovereignty over Australian data. The Australian government is working on mitigating the risks but needs to do more. Further necessary measures include improving cloud-computing regulation and encouraging development of entirely Australian services. Data sovereignty is the principle that information is subject to the laws and regulations of the country in which it is collected and stored, ensuring that individuals and organisations maintain control over their data within national boundaries. It's important because, as former prime minister Malcolm Turnbull said, 'Data is the new oil. It's the currency of the digital age, and we need to make sure that it's controlled by Australians for the benefit of Australians'. Relying on foreign cloud providers raises serious concerns about who ultimately controls our data and the systems that host it.

Read the full article here.

NEW TRADECRAFT OF IRANIAN CYBER GROUP ARIA SEPEHR AYANDEHSAZAN AKA EMENNET PASARGAD

Joint Cybersecurity Advisory | October 30, 2024

The Federal Bureau of Investigation (FBI), U.S. Department of Treasury, and Israel National Cyber Directorate are releasing this Cybersecurity Advisory (CSA) to warn network defenders of new cyber tradecraft of the Iranian cyber group Emennet Pasargad, which has been operating under the company name Aria Sepehr Ayandehsazan (ASA) and is known by the private sector terms Cotton Sandstorm, Marnanbridge, and Haywire Kitten. The group exhibited new tradecraft in its efforts to conduct cyber-enabled information operations into mid-2024 using a myriad of cover personas, including multiple cyber operations that occurred during and targeting the 2024 Summer Olympics – including the compromise of a French commercial dynamic display provider. ASA has also undertaken a project to harvest content from IP cameras and used online resources related to Artificial Intelligence. Since 2023, the group has exhibited new tradecraft including the use of fictitious hosting resellers to provision operational server infrastructure to its own actors as well as to an actor in Lebanon involved in website hosting. Recently released reporting from Microsoft indicates this group has demonstrated interest in election-related websites and media outlets, suggesting preparations for future influence operations.

Read the full article here.

PRC ADAPTS META'S LLAMA FOR MILITARY AND SECURITY AI APPLICATIONS

Sunny Cheung | The Jamestown Foundation | October 31, 2024

In September, the former deputy director of the Academy of Military Sciences (AMS), Lieutenant General He Lei (何雷), called for the United Nations to establish restrictions on the application of artificial intelligence (AI) in warfare (Sina Finance, September 13). This would suggest that Beijing has an interest in mitigating the risks associated with military AI. Instead, the opposite is true. The People's Republic of China (PRC) is currently leveraging AI to enhance its own military capabilities and strategic advantages and is using Western technology to do so. The military and security sectors within the PRC are increasingly focused on integrating advanced AI technologies into operational capabilities. Meta's open-source model Llama (Large Language Model Meta AI) has emerged as a preferred model on which to build out features tailored for military and security applications. In this way, US and US-derived technology is being deployed as a tool to enhance the PRC's military modernization and domestic innovation efforts, with direct consequences for the United States and its allies and partners.

Read the full article here.

AMERICANS, YOUR CALLS AND TEXTS CAN BE MONITORED BY CHINESE SPIES

Josh Rogin | The Washington Post | November 2, 2024

Last week, the Chinese hacking and spying operation known as "Salt Typhoon" was revealed to have targeted former president Donald Trump and his running mate, Sen. JD Vance of Ohio, as well as staffers for Vice President Kamala Harris's campaign and for Congress. The Post has reported that the hackers were able to collect audio and text messages from their targets in a wide-ranging espionage operation, which likely began several months ago. But what is less well understood, according to six current and former senior U.S. officials I spoke with from both parties, all of whom were briefed by the U.S. intelligence community on the operation, is that the threat is much broader. The Chinese hackers, who the United States believes are linked to Beijing's Ministry of State Security, have burrowed inside the private wiretapping and surveillance system that American telecom companies built for the exclusive use of U.S. federal law enforcement agencies — and the U.S. government believes they likely continue to have access to the system. Millions of mobile-phone users on the networks of at least three major U.S. carriers could thus be ongoingly vulnerable to Chinese government surveillance.

Read the full article here.

FBI WARNS GMAIL, OUTLOOK, AOL AND YAHOO USERS—HACKERS GAIN ACCESS TO ACCOUNTS

Zak Doffman | Forbes | November 3, 2024

"Cybercriminals are gaining access to email accounts," the FBI warned this week, even when accounts are protected by multifactor authentication (MFA). Attacks begin when users are lured into "visiting suspicious websites or click on phishing links that download malicious software onto their computer." Email access itself comes by way of cookie theft. Not the devilish tracking cookies that we read so much about, and which caused havoc when Google reversed its promise to eradicate them from Chrome. These are session cookies or security cookies or "remember me" cookies. They store credentials to stop you having to log in every time you visit a website or access one of your accounts.

Read the full article here.

DEFENSIVE MEASURES AGAINST CHINA: TIME FOR A REEVALUATION

Scott Kennedy | Center for Strategic & International Studies (CSIS) | October 29, 2024

On a recent trip to China, I visited a Chinese firm that is on the U.S. Department of Commerce's Entity List. When discussion turned to their designation, they claimed utter disbelief and surprise; they could not fathom what prompted Washington's action. It is possible that their claims of innocence are genuine, but given their place in an important high-tech sector, likely links to the Chinese party-state, and the nature of some of their customers, one can also see why the U.S. government would have taken this step. In fact, it may be difficult to disagree with most, if not every, individual decision the U.S. government has taken in the last five years to protect itself in the face of the broad national security challenge China presents to the United States, its allies, and the rules-based global order. Nevertheless, the cumulative effect of all of this action deserves careful evaluation. And where the result is not as intended, Washington needs to recalibrate its policy approach. There are now around 1,000 Chinese companies and institutions blacklisted by the United States for national security or human rights reasons. The list of "controlled items" that require a license to be exported to China has ballooned, and in the case of advanced semiconductors and semiconductor equipment, the restrictions are country-wide.

Read the full article here.

US TREASURY RESTRICTS INVESTMENT IN CHINESE QUANTUM INDUSTRY

Jacob Taylor | American Institute of Physics (AIP) | October 30, 2024

The Treasury Department finalized a rule on Monday that bars U.S. persons from making certain investments in China-based entities that are working on semiconductors, AI systems, or quantum information technologies. The rule takes effect on Jan. 2, 2025, and builds upon other restrictions the U.S. has placed on strategic technologies, including new export controls on quantum computers implemented in September and export restrictions on specific quantum labs in China implemented in May. The rule is currently limited to China (including Hong Kong and Macau) but the department notes that more countries could be added in the future. It applies to transactions involving Chinese citizens who are not also U.S. citizens or permanent residents, entities located in China, or entities majority-owned by Chinese citizens, among other cases. The transactions covered by the rule include joint ventures, greenfield investments, certain forms of debt financing, and acquisition of equity, among others. Examples of activities exempted from the rule include investments in publicly traded securities and equity-based compensation.

Read the full article here.

ACADEMICS' TIME INCREASINGLY TAKEN UP WITH RESEARCH SECURITY

Helen Parker | Times Higher Education | October 28, 2024

More than half of academics and university leaders who responded to a survey expect to spend more time on research security in the coming years as concerns about international collaborations grow. Digital Science's survey of 380 academics, researchers and university staff from 70 countries revealed that security is a key concern for the global research community, with 58 per cent of respondents expecting to have to dedicate more time to research security in five years. Forty-five per cent said they already spend more time on research security than they did five years ago.

Read the full article here.

CHINA–US SCIENTIFIC COLLABORATION ON SUSTAINABLE DEVELOPMENT AMIDST GEOPOLITICAL TENSIONS

Rongrong Li, Feng Ren and Qiang Wang | Nature | October 31, 2024

This study aims to investigate whether growing geopolitical competition has affected international collaboration in sustainable development research, with a particular focus on structural changes in bilateral research collaboration between China and the United States. Three datasets have been created and compared using bibliographic information provided by the Web of Science core collection: before the Trump administration, during the Trump administration, and during the Biden administration. The results indicate that countries worldwide have conducted extensive research in sustainable development, and the United States, China, and the United Kingdom have produced the most publications, demonstrating a high level of scientific research productivity. Concerning the collaborative patterns of sustainable development research, China and the United States are each other's largest collaborative partners.

Read the full article here.

US APPROACH TO RESEARCH COOPERATION WITH CHINA

Gisela Grieger | European Parliamentary Research Service (EPRS) | March 2022

China and the US are each other's number one research partner Recent data using co-authored research articles and joint patents as a proxy for research cooperation show that China and the US are each other's most important long-standing research partner. China has become an increasingly prominent research cooperation partner for Australia, Canada, and the United Kingdom (UK), while this is less the case for Germany (Figure 1). Japan has lost its earlier role as a major research partner for China to Australia, whereas China has retained its crucial role for Japan, ranking second to the US.

Read the full article here.

CHINA'S STRIDES IN ACADEMIC RESEARCH SEEN TO NARROW US LEAD IN MEDICAL SCIENCE

Zhang Tong | South China Morning Post | September 25, 2024

China is rapidly narrowing the gap with the United States in medical research publications, a trend fuelled by both government policies and the development of artificial intelligence (AI), according to a top scientific publisher. Marie Souliere, head of editorial ethics and quality assurance at Frontiers, one of the biggest academic publishers in the world, said she had seen China's overall research output slowly overtake that of the US, and the lead was most striking in the field of medicine. China overtook the US in share of medicine-related articles in 2019, with 22 per cent of our published content in those fields, versus 19 per cent for the US. Since then, the China share has grown, and maintains around 40 per cent," Souliere said in an interview with the Post this month.

Read the full article here.

USEFUL RESOURCES

YOUR PERSONAL INFORMATION: PROTECTING IT FROM EXPLOITATION

Office of the Director of National Intelligence | September 2016

According to US financial sector estimates, the global space economy is projected to grow from $469 billion in 2021 to more than $1 trillion by 2030. The United States is the main driver of this growth through its role as a global leader in space investment, research, innovation, and production.

Read the full article here.

MAKING PREVENTION A REALITY: IDENTIFYING, ASSESSING, AND MANAGING THE THREAT OF TARGETED ATTACKS

Federal Bureau of Investigation | February 2017

Those responsible for threat assessment and management should recognize that both male and female persons of concern for targeted violence will come to their attention. There may be a tendency for stakeholders to view the potential threat posed by females as less worrisome, e.g. dismissing threatening writings by females as mere fantasy or attention-seeking material.

View the full resource here.

MULTI-FACTOR AUTHENTICATION: TOP 10 HIGH FAVLUE CONTROLS

National Defense ISAC

Multifactor authentication (MFA) to an information system, as described by The DoD, uses two or more methods of authentication involving something you know (e.g., password); something you have (e.g., a One-Time Password (OTP) generating device like a fob, smart-card, or a mobile app on a smart-phone); and something you are (e.g., a biometric like a fingerprint or iris).

View the full resource here.

WHIAANHPI & DCSA: NAVIGATING THE FEDERAL SECURITY CLEARANCE PROCESS

August 21, 2024

How prospective and current federal employees can effectively explore government careers.

View the video here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute