ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

July 20, 2023

SAFEGUARDING OUR FUTURE

National Counterintelligence and Security Center | July 1, 2023

Since 2015, the PRC has passed or updated comprehensive national security, cybersecurity, and data privacy laws and regulations, expanding Beijing's oversight of domestic and foreign (including U.S.) companies operating within China. Beijing views inadequate government control of information within China and its outbound flow as a national security risk. These laws provide the PRC government with expanded legal grounds for accessing and controlling data held by U.S. firms in China. U.S. companies and individuals in China could also face penalties for traditional business activities that Beijing deems acts of espionage or for actions that Beijing believes assist foreign sanctions against China. The laws may also compel locally-employed PRC nationals of U.S. firms to assist in PRC intelligence efforts

Read the full article here.

CO-DIRECTOR OF THINK TANK INDICTED FOR ACTING AS UNREGISTERED FOREIGN AGENT, TRAFFICKING IN ARMS, VIOLATING U.S. SANCTIONS AGAINST IRAN, AND MAKING FALSE STATEMENTS TO FEDERAL AGENTS

U. S. Department of Justice | Press Release | July 10, 2023

A dual U.S.-Israeli citizen who serves as the co-director of a Maryland-based think tank was indicted today for allegedly engaging in multiple international criminal schemes. According to court documents, Gal Luft, 57, is charged in an eight-count indictment with offenses related to willfully failing to register under the Foreign Agents Registration Act (FARA), arms trafficking, Iranian sanctions violations and making false statements to federal agents. Luft was arrested on Feb. 17 in the Republic of Cyprus based on the charges in the indictment. Luft subsequently fled after being released on bail while extradition proceedings were pending and remains a fugitive. According to the allegations contained in the indictment, for years, Luft conspired with others in an effort to act within the United States to advance the interests of the People's Republic of China (China) as agents of China-based principals, without registering as foreign agents as required under U.S. law.

Read the full article here.

NATIONAL CYBER STRATEGY FACES MAJOR IMPLEMENTATION CHALLENGES, EXPERTS SAY

Chris Riotta and Natalie Alms | Nextgov/FCW | March 2, 2023

A depleted workforce, lack of funding and challenges with information sharing across the public and private sectors may severely hamper the federal government's implementation of a new sweeping cybersecurity strategy, experts told FCW. The White House is aiming to fundamentally transform how the federal government approaches cybersecurity with a new national strategy that both seeks to shift from a reactive to proactive posture and pushes for further accountability for software developers. The new strategy, released Thursday, is the first comprehensive cyber plan issued by the White House since 2018, and acknowledges the emerging risks and challenges across the cybersecurity landscape. Cybersecurity experts told FCW the strategy is long overdue and praised the administration's focus on shifting liability to software vendors for vulnerabilities found within their products. But some said the 35-page document lacked critical components that could hamper its successful implementation, namely the necessary funding, resources, and talent necessary to effectively secure U.S. interests in cyberspace.

Read the full article here.

NEW CHINESE COUNTERESPIONAGE LAW AIMED AT US TECH SECTOR

Jayant Chakravarti | BankInfoSecurity | July 5, 2023

China on July 1 set into motion a revamped Counter-Espionage Law that seeks to protect national security agencies and documents, data, and materials related to national security from foreign adversaries. The measure gives Chinese authorities sweeping powers to investigate and even seize property of companies doing business in China. China's National People's Congress first passed the Counter-Espionage Law in November 2014, signaling the Chinese Communist Party's intent to safeguard state secrets the party designated as critical to national security, giving security agencies the power to take proactive action against suspected espionage activities. The revised law, passed by the National People's Congress Standing Committee on April 26, went into effect on Saturday and covers all forms of cyberattacks that target government bodies and China's information infrastructure.

Read the full article here.

CISA AND FBI RELEASE CYBERSECURITY ADVISORY ON ENHANCED MONITORING TO DETECT APT ACTIVITY TARGETING OUTLOOK ONLINE

The Cybersecurity and Infrastructure Security Agency | July 12, 2023

The Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) have released a joint Cybersecurity Advisory (CSA), Enhanced Monitoring to Detect APT Activity Targeting Outlook Online, to provide guidance to agencies and critical infrastructure organizations on enhancing monitoring in Microsoft Exchange Online environments. In June 2023, a Federal Civilian Executive Branch (FCEB) agency observed unexpected events in Microsoft 365 (M365) audit logs. After reporting the incident to Microsoft, network defenders deemed the activity malicious. As a response, Microsoft released this guidance:

Microsoft: Microsoft Mitigates China-based Threat Actor Storm-0558 Targeting of Customer Email
Microsoft: Mitigation for China-Based Threat Actor Activity
Microsoft: Analysis of Storm-0558 Techniques for Unauthorized Email Access

Read the full article here.

CHINESE SPIES ARE TARGETING THE UK 'AGGRESSIVELY' WITH BEIJING 'PENETRATING EVERY SECTOR OF THE ECONOMY' AND FEARS OVER INFLUENCE IN UNIVERSITIES, WARNS PARLIAMENT'S INTELLIGENCE WATCHDOG

James Tapsfield | DailyMail | July 13, 2023

Chinese spies are targeting the UK 'prolifically and aggressively' with Beijing managing to penetrate 'every sector of the economy', a watchdog warned today. The alarming picture was revealed in a long-awaited report by Parliament's intelligence watchdog. It raises concerns about Chinese influence in UK universities and the country's intention to become a 'permanent and significant player' in the civil nuclear energy industry. The Intelligence and Security Committee (ISC) is also critical of the UK Government's response, questioning the trade-off between economic interest and security concerns. The 207-page report, published this morning, said the UK is of 'significant interest to China when it comes to espionage and interference', placing the country 'just below China's top priority targets'. It said: 'China's state intelligence apparatus – almost certainly the largest in the world with hundreds of thousands of civil intelligence officers…. targets the UK and its interests prolifically and aggressively, and presents a challenge for our Agencies to cover.'

Read the full article here.

HOW CHINA EXPORTS SECRECY

Christopher Walker | Foreign Affairs | July 11, 2023

Beijing's Global Assault on Transparency and Open Government China thrives on secrecy. Beijing's approach to governance, which relies on surveillance and control rather than openness and deliberation, requires secrecy. And to sustain it, the Chinese government suppresses independent journalism, censors digital information, and closely guards the kind of information that democracies freely disclose. This commitment to secrecy and censorship is a long-standing feature of the Chinese Communist Party's rule. But under President Xi Jinping, whose ideas about governance may shape the world for years to come, the CCP has grown even more furtive.

Read the full article here.

US-CHINA RELATIONS HAVE ENTERED A FRIGHTENING NEW ERA

Martin Wolf | Financial Times | April 25, 2023

The relationship between the US and China is likely to determine humanity's fate in the 21st century. It will determine whether there will be peace, prosperity and protection of the planetary environment, or the opposites. Should it be the latter, future historians (if any such actually exist) will surely marvel at the inability of the human species to protect itself against its own stupidity. Yet today, happily, we can still act to prevent disaster. That is true in many domains. Among these is economics. How then are economic relations to be best managed in the increasingly difficult future we confront? Janet Yellen, US Treasury secretary, and Ursula von der Leyen, president of the European Commission, have both recently made thoughtful statements on this topic. But do they set out a workable future? On that I am, alas, doubtful. Yellen sets out a plan for what she calls "constructive engagement".

Read the full article here.

FOREIGN-FUNDED LANGUAGE AND CULTURE INSTITUTUES AT U. S. INISTITUTIONS OF HIGHER EDUCATION

Philip J. Hanon, Jayathi Y. Murthy, and Sarah M. Rovito | The National Academies | June 2023

Foreign-funded language and culture institutes exist on U.S. campuses beyond Confucius Institutes (CIs)—Chinese government-funded centers established by the Chinese Communist Party to extend the reach of Chinese language and culture and to enhance worldwide opinion of China through offering classes in Mandarin Chinese and highlighting positive aspects of Chinese culture. Regardless of the sponsoring nation, foreign-funded language and culture institutes may pose risks for U.S. host institutions regarding academic freedom, freedom of expression, governance, and national security. This is particularly true if the values of the sponsoring nation do not align with the democratic values held in the United States and if the sponsoring nation is suspected of engaging in activities adversely affecting human rights, academic freedom, freedom of expression, association, dissent, and U.S. national security.

Read the full article here.

DATA PROTECTION: EUROPEAN COMMISSION ADOPTS NEW ADEQUACY DECISION FOR SAFE AND TRUSTED EU-US DATA FLOWS

European Commission | Press Release | July 10, 2023

Today, the European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework. The decision concludes that the United States ensures an adequate level of protection – comparable to that of the European Union – for personal data transferred from the EU to US companies under the new framework. On the basis of the new adequacy decision, personal data can flow safely from the EU to US companies participating in the Framework, without having to put in place additional data protection safeguards. The EU-U.S. Data Privacy Framework introduces new binding safeguards to address all the concerns raised by the European Court of Justice, including limiting access to EU data by US intelligence services to what is necessary and proportionate, and establishing a Data Protection Review Court (DPRC), to which EU individuals will have access. The new framework introduces significant improvements compared to the mechanism that existed under the Privacy Shield. For example, if the DPRC finds that data was collected in violation of the new safeguards, it will be able to order the deletion of the data.

Read the full article here.

CHINA'S COGNITIVE AI RESEARCH

William Hannas, Huey-Meei Chang, Max Riesenhuber, and Daniel Chou | Center for Security and Emerging Technology | July 2023

An expert assessment of Chinese scientific literature validates China's public claim to be working toward artificial general intelligence (AGI). At a time when other nations are contemplating safeguards on AI research, China's push toward AGI challenges emerging global norms, underscoring the need for a serious open-source monitoring program to serve as a foundation for outreach and mitigation. China's intent to create broadly capable artificial intelligence, also called "artificial general intelligence" (AGI), was announced in its 2017 "New Generation AI Development Plan" and is championed by leading Chinese scientists and AI institutions. This study assesses the plausibility of these claims by examining Chinese scientific papers published in Chinese and English between 2018 and 2022 for evidence of related research. While most such papers are on routine AI applications, a significant body of research was found on AGI precursor technologies, indicating that China's claims to be working toward artificial general intelligence are genuine and must be taken seriously.

Read the full article here.

FOR EXPORT CONTROLS ON AI, DON'T FORGET THE "CATCH-ALL" BASICS

Emily S. Weinstein and Kevin Wolf | Center for Security and Emerging Technology | July 5, 2023

Existing U.S. government tools and approaches may help mitigate some of the issues worrying AI observers. This blog post describes long-standing "catch-all" controls, administered by the Department of Commerce's Bureau of Industry and Security (BIS), and how they might be used to address some of these threats. Recent advances in the field of artificial intelligence (AI) have put the world on edge. AI experts, policymakers, journalists, and others are expressing concern about the potential existential risks that AI may pose. These include those related to large language models (LLMs), such as ChatGPT and GPT-4. Experts across the policy and technology community who believe in the urgency for action, including OpenAI's Sam Altman and Senator Chuck Schumer, have called for regulation and controls on AI development and proliferation. Others in the broader tech policy community have expressed concerns about the existential risk posed by AI systems, even going as far as to argue that "mitigating the risk of extinction from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war."

Read the full article here.

SENATORS LEAVE CLASSIFIED AI BRIFING CONFIDENT BUT WARY

WallStreetPR | July 12, 2023

Senators left a classified briefing on artificial intelligence Tuesday with a deeper understanding of how AI is already being used to bolster U.S. national security and the looming threat China poses as it deploys its own AI capabilities. "I think, from a military perspective, it's very existential because China's playing for keeps," Sen. Eric Schmitt, R-Mo., told Fox News Digital after the closed-door session. "On the commercial side, there's a lot of innovation that's happening. So, it's moving quickly, but I think the best we can do right now is get a firm understanding." Tuesday afternoon's briefing was the first-ever classified meeting with senators and key Pentagon officials about AI. Discussion included how the U.S. is using AI to maintain its national security edge and how adversaries like China are using this emerging tool. Senate Majority Leader Chuck Schumer, D-N.Y., told reporters what he learned was "eye-opening." It comes after he told senators in a letter over the weekend that Congress is moving full steam ahead on his AI regulatory framework, which Schumer said Tuesday could take months to develop.

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