ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

July 13, 2023

AUSTIN DIRECTS DOD COMPONENTS TO REINFORCE CLASSIFIED SAFEGUARDS FOLLOWING SECURITY REVIEW

U.S. Department of Defense | July 5, 2023

Secretary of Defense Lloyd J. Austin III has tasked Defense Department components with implementing a series of recommendations aimed at improving classified information safeguards. This action follows the Pentagon's review of departmentwide security programs and policies undertaken after the unauthorized disclosure of sensitive information discovered online in the spring. The secretary's directive follows his approval of the initial findings of the 45-day review led by the undersecretary of defense for intelligence and security and the DOD chief information officer and director of administration and management. "While the review found that a majority of DOD personnel with access to classified national security information, or as we call it CNSI, comply with security policies, procedures and processes, and recognize the importance of that information and maintaining our national security, the review also identified a number of areas where the department should seek to improve its security posture and accountability measures," a senior defense department official said today.

Read the full article here.

DOD LOOKS TO BLOCK CHINESE AND RUSSIAN INFLUENCE ON US ACADEMIA

Jonathan Lehrfeld | MilitaryTimes | July 5, 2023

The Pentagon just released a black list of mostly Chinese and Russian research institutes that it says have engaged in "problematic activity," including trying to infiltrate sensitive Defense Department research at U.S. colleges and universities. The Pentagon partners with hundreds of U.S. universities and research institutions, a relationship malign actors have been able to reportedly hijack to steal U.S. defense technology. When those U.S. institutions also get funding from the black-listed entities, the foreign partners have in the past used the research relationship to try to access and even steal sensitive defense research. "The publication of these foreign entities underscores our commitment to ensuring the responsible use of federal research funding and safeguarding our critical technologies from exploitation or compromise," Heidi Shyu, the undersecretary of defense for research and engineering, said in a June 30 release. The statement went on to encourage U.S. universities and industry to "review the list and exercise caution when engaging with entities listed."

Read the full article here.

PENTAGON TO STRENGTHEN INSIDER THREAT MONITORING AND VETTING PROCEDURES FOLLOWING MAJOR INTEL LEAK

Haley Britzky, Natasha Bertrand, and Oren Liebermann | CNN Politics | July 5, 2023

Chinese companies utilize a variety of methods—many of them covert or coercive—to acquire valuable technology, intellectual property (IP), and knowhow from U.S. firms. These efforts are often made at the direction of and with assistance from the Chinese government, part of Beijing's larger effort to develop its domestic market and become a global leader in a wide range of technologies. These acquisition attempts frequently target advanced technologies such as artificial intelligence, biotechnology, and virtual reality, which are still in the early stages of development but could provide dual military and civilian capabilities in the future. This report explores six methods used by Chinese companies to acquire U.S. technology and IP, including (1) foreign direct investment, (2) venture capital investment, (3) joint ventures, (4) licensing agreements, (5) cyber espionage, and (6) talent acquisition programs. It then examines the effectiveness of existing U.S. regulations to assess and address the risks of increased technology transfers to China.

Read the full article here.

HOW CHINESE COMPANIES FACILITATE TECHNOLOGY TRANSFER FROM THE UNITED STATES

Sean O'Connor | The U.S.-China Economic and Security Review Commission | May 6, 2019

Chinese companies utilize a variety of methods—many of them covert or coercive—to acquire valuable technology, intellectual property (IP), and knowhow from U.S. firms. These efforts are often made at the direction of and with assistance from the Chinese government, part of Beijing's larger effort to develop its domestic market and become a global leader in a wide range of technologies. These acquisition attempts frequently target advanced technologies such as artificial intelligence, biotechnology, and virtual reality, which are still in the early stages of development but could provide dual military and civilian capabilities in the future. This report explores six methods used by Chinese companies to acquire U.S. technology and IP, including (1) foreign direct investment, (2) venture capital investment, (3) joint ventures, (4) licensing agreements, (5) cyber espionage, and (6) talent acquisition programs. It then examines the effectiveness of existing U.S. regulations to assess and address the risks of increased technology transfers to China.

Read the full article here.

NEW TOOL EXPLOITS MICROSOFT TEAMS BUG TO SEND MALWARE TO USERS

Bill Toulas | BleepingComputer | July 5, 2023

A member of U.S. Navy's red team has published a tool called TeamsPhisher that leverages an unresolved security issue in Microsoft Teams to bypass restrictions for incoming files from users outside of a targeted organization, the so-called external tenants. The tool exploits a problem highlighted last month by Max Corbridge and Tom Ellson of UK-based security services company Jumpsec, who explained how an attacker could easily go around Microsoft Teams' file-sending restraints to deliver malware from an external account. The feat is possible because the application has client-side protections that can be tricked into treating an external user as an internal one just by changing the ID in the POST request of a message.

Read the full article here.

RECENT CHINESE CYBER INTRUSIONS SIGNAL A STRATEGIC SHIFT

Pukhraj Singh | Australian Strategic Policy Institute (The Strategist) | July 5, 2023

On 25 May, Australia and its partners in the Five Eyes intelligence-sharing network—Canada, New Zealand, the UK and the US—made a coordinated disclosure on a state-sponsored cyber hacking group dubbed 'Volt Typhoon'. The group has been detected intruding on critical infrastructure since 2021, but the nature of recent intelligence on its behaviour hints at worrying developments in the Chinese cyber establishment. While the Five Eyes' disclosure is direct in its attribution of Volt Typhoon to the Chinese government, there are many layers that need to be peeled away to reveal the true nature, and implications, of the threat. State-aligned or state-sponsored cyber threats emerging from China can be grouped under two broad government structures: the Ministry of State Security and the Strategic Support Force. The MSS is China's peak foreign intelligence, counterintelligence and political security agency, and the SSF is the joint information warfare command of the People's Liberation Army's, akin to US Cyber Command. While its US counterpart focuses solely on military cyber operations, the SSF has a broader mandate covering electronic warfare, strategic military cyber operations and political warfare. The SSF was founded in 2015 as part of structural reforms to the PLA spearheaded by Chinese President Xi Jinping.

Read the full article here.

OPEN SCIENCE IN HORIZON EUROPE

European Research Executive Agency

Did you know that open science is a legal obligation under Horizon Europe. Its purpose is to foster greater transparency and trust for the benefit of scientific research and for the benefit of EU citizens. Confused or unsure about how to comply with open science principles when applying for EU funding and when implementing your project? Fear not! REA has prepared an information package and series of Q&As below. This may help you to successfully implement open science practices in your proposals and during your project if your proposal is selected for funding. What does "as open as possible, as closed as necessary" mean? Results and data may be kept closed if making them public in open access is against the researcher's legitimate interests. Examples include to commercially exploit their research results, or if it is against any obligations mentioned in the Grant Agreement (e.g. personal data protection).

Read the full article here.

HOW TO MAKE YOUR SCIENTIFIC DATA ACCESSIBLE, DISCOVERABLE AND USEFUL

Jeffrey M. Perkel | Nature | June 27, 2023

Miguel Acevedo typically gets two questions about his research on malaria in lizards. "Do lizards really get malaria?" (The answer is yes.) And, "Will I get malaria from a lizard?" (Not likely.) Lizard malaria is a model for vector-borne disease ecology and evolution1. A colleague had been pursuing the same problem, at the same site in Puerto Rico, since the 1990s, and Acevedo, a wildlife ecologist at the University of Florida in Gainesville, wanted to combine those older data with his own to perform a long-term analysis. It was easier said than done. Whereas Acevedo's data were logged using a standardized data-entry template, the colleague's data were recorded in a mix of paper notebooks, Excel spreadsheets and hand-drawn maps. "It was some of the most organized data of that era, but we didn't have the standards then that we have today," he says. Columns weren't necessarily consistent from sheet to sheet, nor did they use the same units, and it wasn't always clear which sampling sites were being measured.

Read the full article here.

CHINA CRAFTS WEAPONS TO ALTER BRAIN FUNCTION; REPORT SAYS TECH MEANT TO INFLUENCE GOVERNMENT LEADERS

Bill Gertz | The Washington Times | July 6, 2023

China's People's Liberation Army is developing high-technology weapons designed to disrupt brain functions and influence government leaders or entire populations, according to a report by three open-source intelligence analysts. The weapons can be used to directly attack or control brains using microwave or other directed energy weapons in handheld guns or larger weapons firing electromagnetic beams, adding that the danger of China's brain warfare weapons prior to or during a conflict is no longer theoretical. "Unknown to many, the Chinese Communist Party (CCP) and its People's Liberation Army (PLA) have established themselves as world leaders in the development of neurostrike weapons," according to the 12-page report, "Enumerating, Targeting and Collapsing the Chinese Communist Party's Neurostrike Program." The Washington Times obtained a copy of the study. The U.S. Commerce Department in December 2021 imposed sanctions on China's Academy of Military Medical Sciences and 11 related entities the department said were using "biotechnology processes to support Chinese military end-uses and end-users, to include purported brain-control weaponry. "Few public studies or discussions, however, have been held regarding the new advanced military capability.

Read the full article here.

AUDIT OF THE DOD'S IMPLEMENTATION AND OVERSIGHT OF THE CONTROLLED UNCLASSIFIED INFORMATION PROGRAM

Inspector General | Department of Defense | June 1, 2023

The objective of this audit was to determine the extent to which the DoD developed guidance, conducted training, and oversaw the implementation of the DoD Controlled Unclassified Information (CUI) Program. We also reviewed a sample of documents that were identified by the DoD Components and contractors as containing CUI to determine whether the documents had CUI headers and footers, a designation indicator, and portion markings as required by DoD guidance (referred to as the required markings throughout this report). CUI is information created or possessed for the Government that requires safeguarding or dissemination controls according to applicable laws, regulations, and Government-wide policies. We will continue to explore opportunities for additional oversight on the implementation of the DoD CUI Program. Background Executive Order 13556, "Controlled Unclassified Information," established a Government-wide program to standardize the way the Executive Branch handles unclassified information that requires safeguarding or dissemination controls. DoD Instruction 5200.48, "Controlled Unclassified Information," established the DoD CUI Program requirements for designating, marking, handling, and decontrolling CUI and establishes a requirement for CUI training.

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