ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

# THE OPEN SOURCE MEDIA SUMMARY

## September 21, 2023

## 5 EARLY WARNING INDICATORS THAT ARE KEY TO PROTECTING NATIONAL SECRETS

*Kellie Roessler | Dark Reading | August 23, 2023*

The US Department of Defense (DoD) will create an insider threat office to monitor employees following a review into the leak of classified Pentagon intelligence on Discord. A June 30 memo signed by the Secretary of Defense calls for the establishment of a Joint Management Office for Insider Threat and Cyber Capabilities to "oversee user activity monitoring (UAM)." While any effort to stop insiders from leaking data is promising, there is a bigger issue at play that has everything to do with the UAM requirements, as defined by the Committee on National Security Systems Directive (CNSSD) 504 in 2014. In brief, current UAM data requirements are insufficient for proactively stopping insider risks from becoming threats that turn into data-loss incidents ("proactively" being the key word). On hearing about the Joint Management Office for Insider Threat and Cyber Capabilities, many insider-risk practitioners likely experienced a good spell of déjà vu. And within reason.

Read the full article here.

## THE U.S. IS GETTING HACKED. SO THE PENTAGON IS OVERHAULING ITS APPROACH TO CYBER

*Maggie Miller and Lara Seligman | Politico | September 12, 2023*

A series of high-profile cyberattacks from Russia, China and criminal networks in recent years have served as a wake up call to the Defense Department that cyberwarfare has changed. And that reckoning has forced one of its most secretive branches-U.S. Cyber Command-to come to an unusual conclusion: Going it alone is no longer an option. Hackers are increasingly infiltrating private companies and government agencies far outside the Pentagon's usual purview, and the hacks are being perpetrated by cybercriminals who honed their strategies abroad before striking the United States. So Pentagon leaders have started opening up communications with other federal agencies and the private sector on cyber threats to elections and other critical systems, and increasing assistance to foreign allies. They've codified the changes in a new cyber strategy released Tuesday, first reported by POLITICO. It's "a more calibrated thinking about cyber, and realistic thinking about cyber," said Mieke Eoyang, DOD deputy assistant secretary for cyber policy, in an interview ahead of the strategy rollout.

Read the full article here.

## CISA WARNS GOVT AGENCIES TO SECURE IPHONES AGAINST SPYWARE ATTACKS

*Sergiu Gatlan | Bleeping Computer | September 11, 2023*

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) ordered federal agencies today to patch security vulnerabilities abused as part of a zero-click iMessage exploit chain to infect iPhones with NSO Group's Pegasus spyware. This warning comes after Citizen Lab disclosed that the two flaws were used to compromise fully-patched iPhones belonging to a Washington DC-based civil society organization using an exploit chain named BLASTPASS that worked via PassKit attachments containing malicious images. Citizen Lab also warned Apple customers to apply emergency updates issued on Thursday immediately and urged individuals susceptible to targeted attacks due to their identity or occupation to enable Lockdown Mode. "Apple is aware of a report that this issue may have been actively exploited," the company said when describing the two Image I/O and Wallet vulnerabilities, tracked as CVE-2023-41064 and CVE-2023-41061.

Read the full article here.

## NSA, U.S. FEDERAL AGENCIES ADVISE ON DEEPFAKE THREATS

*National Security Agency-Central Security Service | September 12, 2023*

The National Security Agency (NSA) and U.S. federal agency partners have issued new advice on a synthetic media threat known as deepfakes. This emerging threat could present a cybersecurity challenge for National Security Systems (NSS), the Department of Defense (DoD), and DIB organizations. They released the joint Cybersecurity Information Sheet (CSI) "Contextualizing Deepfake Threats to Organizations" to help organizations identify, defend against, and respond to deepfake threats. NSA authored the CSI with contributions from the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA). The term "deepfake" refers to multimedia that has either been synthetically created or manipulated using some form of machine or deep learning (artificial intelligence) technology. Other terms used to describe media that have been synthetically generated and/or manipulated include Shallow/Cheap Fakes, Generative AI, and Computer Generated Imagery (CGI).

Read the full article here.

## RESEARCHERS MUST NAVIGATE THORNY NEW DATA SECURITY LAWS

*Yojana Sharma | University World News | September 11, 2023*

In mid-August, when many economists, policy-makers and researchers were expecting yet another rise in the July figures for youth unemployment in China – which includes graduate unemployment – the government announced that it was suspending the release of the data. Analysts monitoring China, who were expecting another rise from a youth unemployment record set in June at 21.3%, have noted that other key economic indicators have become harder to find. Tightened control of key information has become more common in China. Academics and researchers overseas said recent laws controlling access to data and data exports have made it even more difficult to independently seek out or verify statistics on the ground, if information is withheld officially. Researchers – including China scholars seeking information about China but also researchers in scientific fields and who collaborate with Chinese partners – describe a new research environment in which even minimal connection or collaboration with China has to be handled with extreme care under several new laws.

Read the full article here.

## CISA OPEN SOURCE SOFTWARE SECURITY ROADMAP

*Cybersecurity and Infrastructure Security Agency | September 2023*

The federal government, critical infrastructure, and state, local, tribal, and territorial (SLTT) governments greatly depend upon open source software (OSS). OSS is software for which the humanreadable source code1 is made available to the public for use, study, re-use, modification, enhancement, and re-distribution. OSS is part of the foundation of software used across critical infrastructure, supporting every single critical infrastructure sector and every National Critical Function: one study2 found that 96% of studied codebases across various sectors contain open source code, and 76% of code in studied codebases was open source. Therefore, to fulfill CISA's mission of understanding, managing, and reducing risks to the federal government and critical infrastructure, we must understand and protect the open source software that we rely upon. As a public good, open-source software is supported by diverse and wide-ranging communities—which are composed of individual maintainers, non-profit software foundations, and corporate stewards.

Read the full article here.

## LEVERAGING METRICS TO ENHANCE YOUR INSIDER RISK MANAGEMENT PROGRAM

*Security Boulevard | September 5, 2023*

In today's dynamic cybersecurity landscape, organizations must proactively manage and monitor their Insider Risk. Effectively measuring the performance of an Insider Risk program and communicating its effectiveness and needs to senior leaders and the board is critical for continuous improvement and organizational buy-in. This blog is the first of a two-part series exploring the importance of using metrics to enhance your Insider Risk program from the start through maturity. In this blog, we will discuss the importance of program measurement, elucidate how to measure program activities and outcomes, and look at some example metrics for program evaluation. There are two ways to measure a program's effectiveness: Activity-focused numbers and program outcomes. Both metrics play a pivotal role in understanding and improving the effectiveness of an Insider Risk program. Capturing data on program activities and results provides tangible evidence of program performance, guides decision-making, and fosters a data-driven approach.

Read the full article here.

## HOW CHINA WEAPONIZES THE CAPITALIST SYSTEM AGAINST US

*Keith Krach | The Hill | August 6, 2023*

As we navigate the escalating threat posed by China – a nation guided by communist doctrine, yet peculiarly sustained by the tenets of global capitalism – the urgency to reassess our financial engagement becomes more pressing than ever. The Chinese Communist Party (CCP), the draconian ruler of the world's second-largest economy, has accumulated immense wealth from American investments. This wealth manifests itself through dollar-denominated Chinese bonds and a myriad of Chinese companies publicly traded on U.S. exchanges, including their shrewdly named subsidiaries, intricately woven into the fabric of index funds. In an alarming twist, the Chinese government has weaponized our own capitalist system against us. Through 401(k) retirement accounts and diverse investment vehicles, approximately 100 million Americans are unknowingly bolstering a predatory economic adversary and facilitating a military with global supremacy ambitions.

Read the full article here.

## US, CHINA MAY END SCIENCE AND TECH AGREEMENT

*Caroline Wagner | Ohio State News | September 12, 2023*

A decades-old science and technology cooperative agreement between the United States and China expires on Aug. 27, 2023. On the surface, an expiring diplomatic agreement may not seem significant. But unless it's renewed, the quiet end to a cooperative era may have consequences for scientific research and technological innovation. The possible lapse comes after U.S. Rep. Mike Gallagher, R-Wis., led a congressional group warning the U.S. State Department in July 2023 to beware of cooperation with China. This group recommended to let the agreement expire without renewal, claiming China has gained a military advantage through its scientific and technological ties with the U.S. The State Department has dragged its feet on renewing the agreement, only requesting an extension at the last moment to "amend and strengthen" the agreement. The U.S. is an active international research collaborator, and since 2011 China has been its top scientific partner, displacing the United Kingdom, which had been the U.S.'s most frequent collaborator for decades.

Read the full article here.

## NSF SEEKS TO TACKLE FOREIGN PARTNERSHIP FEARS

*Paul Basken | Times Higher Education | August 23, 2023*

The US National Science Foundation is making a concerted effort to resolve high-stakes debates over US research security by creating a formal network of scientists to study the best ways of handling the problem. As both Republicans and Democrats in the US grow increasingly antagonistic towards China and other countries they regard with suspicion, the NSF initiative aims to precisely identify and study the threat to the US from foreign misuse of the nation's research enterprise. "At NSF, we're very data-driven," Rebecca Keiser, the NSF's chief of research security strategy and policy, said in announcing the plan. "And so what we wanted to do was explore what was occurring here." The idea follows years of rising complaints from politicians and national security officials aimed at the US research community over perceptions that Chinese partners are stealing ideas of economic and military value. University leaders generally have acknowledged the concern but argued that the collaborations provide the US with a net benefit.

Read the full article here.

## AMERICAN UNIVERSITIES SHOULDN'T CUT ALL TIES WITH CHINA

*L. Rafael Reif | Foreign Affairs | September 13, 2023*

Since the United States and China reopened diplomatic relations in the late 1970s, the leaders of both countries have recognized the value of having their universities work together in research and education, to promote prosperity and friendship. Today, however, U.S. policymakers are so concerned about the potential transfer of advances in science and technology from American university laboratories to China that, step by step, sometimes intentionally, sometimes inadvertently, they are discouraging academic exchanges. Research papers authored jointly by U.S. and Chinese scientists fell in 2021 for the first time in decades, the number of American scientists of Chinese descent leaving the United States for China has ticked upward, and surveys of Chinese students thinking of studying abroad suggest that the United States is becoming a less desirable destination for many of them. In late August, the U.S. government continued to signal its wariness about academic engagements with China by waiting until the last minute to renew the landmark U.S.-China Science and Technology Cooperation Agreement, which dates back to 1979.

Read the full article here.

## CONGRESS MUST SECURE AN AMERICAN MANUFACTURING BASE FOR VITAL TECH

*L. Rafael Reif | The Hill | September 9, 2023*

During the global semiconductor shortage brought on by the pandemic, many Americans were shocked to learn that over 90 percent of the world's most sophisticated semiconductor chips are manufactured in Taiwan, which is increasingly menaced by China. Since leading American companies rely on these chips, any sustained disruption in their supply would be disastrous to our economy. In recent decades, financial markets have encouraged such geographical specialization. They have rewarded U.S. companies for outsourcing and offshoring even high-tech manufacturing to countries with lower costs, greater scale, or greater production expertise — and more generous government subsidies underpinning all these advantages. Now, with rising geopolitical tensions beginning to fragment global supply chains, it has become clear that the U.S. should have at least some state-of-the-art manufacturing presence in technologies critical to our economy.

Read the full article here.

## I'M NOT A CHINESE SPY, INSISTS PARLIAMENTARY RESEARCHER ARRESTED OVER ESPIONAGE CLAIMS

*Andy Gregory | Independent | September 12, 2023*

A parliamentary researcher who was arrested on suspicion of spying for China has insisted he is "completely innocent". In a statement released through his lawyers, the man denied being a "Chinese spy" and said he had spent his career trying to "educate others" about the "threats presented by the Chinese Communist Party". The researcher, who had links with senior Tories including security minister Tom Tugendhat and foreign affairs committee chair Alicia Kearns, was arrested back in March – but this went undisclosed until Saturday. The arrest, under the Official Secrets Act, led to Rishi Sunak confronting Chinese premier Li Qiang at the G20 summit in India on Sunday over what he alleged was "unacceptable" interference in democracy. Mr. Sunak told MPs on Monday night he had been "emphatically clear" in his engagement with China "that we will not accept any interference in our democracy and parliamentary system".

Read the full article here.

## SECURITY RAID ON CHINESE ACADEMIC FUELS CONCERN OVER AUSTRALIA-CHINA EXCHANGES

*Kirsty Needham | Reuters | September 11, 2023*

A Chinese university scholar had equipment seized and was questioned by Australia's security agency and police in Western Australia last month in an incident that has prompted some Australian academics to reconsider their travel plans to China for fear of reprisals. The Chinese academic, who specialises in foreign affairs research at a Beijing university, had visited universities in three Australian states in July and August. The Guardian first reported on Monday that the man had his accommodation raided and his laptop taken by the Australian Security Intelligence Organisation and Australian Federal Police in Perth, and was told his visa was being assessed for security reasons. He returned to China. Three sources with knowledge of the matter confirmed some of the details of the Guardian story to Reuters. The Chinese national had previously studied in Australia and now worked for a Beijing university where he specialised in foreign policy research, one of the sources added.

Read the full article here.

## CODE REINS IN TOP SCIENTISTS, WHO MUST 'SERVE NATIONAL SECURITY'

*Mimi Leung | University World News | September 14, 2023*

Members of the prestigious Chinese Academy of Sciences (CAS) have been barred from publicly expressing academic opinions 'unrelated to their field of expertise', amid tightened restrictions to ensure the nation's top scientists abide by 'national security' goals. A new code of conduct released by the CAS in August also has rules that seek to curb the use of 'academician' titles for non-academic purposes, including those for business ventures and promotions. 'Academician' is the highest title bestowed on scientists in China, which members retain for life. The latest version is the first change in the CAS code of conduct for approximately a decade. The new rules also lay down that academicians must be open to 'supervision from society' – a blanket term which usually means adhering to Communist Party of China control and not provoking public criticism. The code specifically states that academicians must ensure their public statements are in line with the general policies of the Communist Party's Central Committee.

Read the full article here.

# USEFUL RESOURCES

## DON'T BE A PAWN OF REPESSIVE FOREIGN GOVERNMENTS

*National Counterintelligence and Security Center | March 2023*

Foreign intelligence entities (FIEs) and elements working on behalf of repressive regimes have sought to use U.S.-based persons to facilitate their efforts to threaten or harm perceived critics and opponents in the United States. For instance, FIEs from the People's Republic of China, the Islamic Republic of Iran, and other nations have used U.S.-based persons to conduct surveillance against and collect personal information on individuals their regimes were targeting in the United States.

View the full resource here.

## PREVENTING VIOLENT ATTACKS:BEST PRACTICES FOR BYSTANDER INTERVENTION

*The Threat Lab*

In the weeks and months prior to a violent act, perpetrators may engage in communication and/or behaviors that could signal imminent violence. Some of their behaviors may be intentionally concealed, while others are observable. Many targeted violent acts are preventable through recognition and reporting. This brochure aims to help you prevent violent attacks by providing information on what, when, and where to report.

View the full resource here.

## 15 TYPES OF CYBER ATTACKS

*Cyber Risk Advisory and Consulting Services*

View the full resource 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*