



<https://asce.tamus.edu>

THE OPEN SOURCE MEDIA SUMMARY

October 12, 2022

AN UPDATE ON RESEARCH SECURITY: STREAMLINING DISCLOSURE STANDARDS TO ENHANCE CLARITY, TRANSPARENCY, AND EQUITY

Morgan Dwyer, Christina Ciocca Eller, and Ryan Donohue | Office of Science and Technology Policy | The White House | August 31, 2022

One of America's greatest strengths is its scientific and technological innovation, fueled over time by Federal investments in research and development (R&D). From the fundamental to the applied, U.S.-supported research has transformed our world and has made our communities safer, healthier, stronger, and more equitable. The American research culture is intentional in its strong commitment to openness. Yet maintaining that open research culture also requires being clear-eyed that certain governments seek to exploit our openness and disrupt the integrity of our research. Such threats require the Federal government, in collaboration with the research community, to take protective actions to mitigate research integrity risks without compromising the values that distinguish the U.S. research enterprise: openness, transparency, honesty, equity, fair competition, objectivity, and democratic participation. The Biden-Harris Administration is committed to strengthening research security without compromising these core values. "Research security" here refers to safeguarding the U.S. research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference.

Read the full article [here](#).

NSA, CISA, FBI REVEAL TOP CVEs EXPLOITED BY CHINESE STATE-SPONSORED ACTORS

National Security Agency/Central Security Service | October 6, 2022

In a Cybersecurity Advisory released today, the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) exposed the "Top Common Vulnerabilities and Exposures (CVEs) Actively Exploited by People's Republic of China State-Sponsored Cyber Actors" since 2020. The report highlights how PRC cyber actors continue to exploit these weaknesses to gain unauthorized access into sensitive networks, establish persistence, and move laterally to other internally connected networks. The actors have targeted government and critical infrastructure networks with an increasing array of new and adaptive techniques — some of which pose a significant risk to Information Technology Sector organizations (including telecommunications providers), Defense Industrial Base (DIB) Sector organizations, and other critical infrastructure organizations.

Read the full article [here](#).



AN INFLECTION POINT FOR THE CREATION OF NEW CYBERSECURITY OPERATING MODELS IN HIGHER EDUCATION

Hernan Londono | EDUCAUSE Review | October 4, 2022

I can't claim that I was "there" when cybersecurity was finally recognized as a discrete branch of higher education operations. I have, however, been involved in cybersecurity in the higher education and health care fields for about fifteen years—long enough to have witnessed some evolutionary changes. Recently, I have been particularly interested in understanding the different elements that contribute to the current situation in higher education: a sense that colleges and universities aren't making much progress in their quest to improve their cybersecurity postures. Of course, the journey, budget, size, and complexity of every institution is different, and some institutions have surely improved their positions. But the conversations I have had at nearly every cybersecurity conference, panel discussion, and social event lead me to believe that, overall, things are not getting better.

Read the full article [here](#).

I WAS A PRESIDENTIAL SCIENCE ADVISER – HERE ARE THE MANY CHALLENGES ARATI PRABHAKAR FACES AS SHE TAKES OVER PRESIDENT BIDEN'S SCIENCE POLICY OFFICE

Neal Lane, Emeritus Professor | Nextgov | October 7, 2022

Arati Prabhakar has been sworn in as director of the Office of Science and Technology Policy and assistant to the president for science and technology after being confirmed by the U.S. Senate, two months following her nomination by President Joe Biden. As the director of OSTP and assistant to the president, she now serves as the confidential science adviser to the president and is also accountable to Congress. Prabhakar is both the first woman and first person of color to hold this role. I had the pleasure of getting to know Prabhakar during the Clinton administration when she was the director of the National Institute for Standards and Technology and I was director of the National Science Foundation. In 1998, President Bill Clinton selected me to be his director of OSTP and assistant to the president for science and technology, a position I held until the end of the administration in 2001.

Read the full article [here](#).

U.S. IMPOSES TOUGH RULES TO LIMIT CHINA'S ACCESS TO HIGH-TECH CHIPS

Ellen Nakashima, Jeanne Whalen and Cate Cadell | The Washington Post | October 7, 2022

The Biden administration on Friday announced its most aggressive measures to date aimed at limiting China's access to advanced computer chips and chip-making equipment, saying that the technology is supporting China's military modernization and even its development of weapons of mass destruction. The administration said it was focusing solely on the chips, activities and entities of "greatest national security concern" in China to minimize harm to the American chip industry — foundational to the U.S. economy — and disruptions to the global supply chain. The move represents a clear flexing of U.S. muscle in its competition with China, with analysts saying it amounts to a new strategy of high-tech containment. But officials also acknowledged the effort could backfire without buy-in from foreign partners and allies. "We recognize that the unilateral controls we're putting into place tomorrow will lose effectiveness over time if other countries don't join us, and we risk harming U.S. technology leadership if foreign competitors are not subject to similar controls," said a senior administration official who spoke on the condition of anonymity to preview the rules with reporters.

Read the full article [here](#).



U.S. ADDS CHINA'S YMTC AND 30 OTHER FIRMS TO 'UNVERIFIED' TRADE LIST

Karen Freifeld and Alexandra Alper | Reuters | October 7, 2022

The United States on Friday added China's top memory chipmaker YMTC and 30 other Chinese entities to a list of companies that U.S. officials have been unable to inspect, ratcheting up tensions with Beijing and starting a 60 day-clock that could trigger much tougher penalties. The new listings were the first of a slew of new restrictions announced on Friday on exports of technology to China aimed at blocking military advances. The crackdown included curbs on access to chipmaking tools for Chinese firms including Yantze Memory Technologies Co (YMTC), as reported by Reuters a day earlier. U.S. senators from both parties have been calling for YMTC, China's fast-growing chip manufacturer, to be placed on a trade blacklist known as the "entity list." The company, founded in 2016, poses a "direct threat" to U.S. chip companies, according to the Biden administration. YMTC and the Chinese embassy in Washington did not respond to requests for comment.

Read the full article [here](#).

HOUSE GOP DEMANDS INVESTIGATION INTO CHINESE TIES TO TOP US NUCLEAR AND WEAPONS SITE

Jerry Dunleavy | Restoring America | Washington Examiner | October 6, 2022

House Republicans are calling on the Biden administration to investigate the Chinese government's economic espionage efforts at U.S. research labs following a damning report about Beijing's apparent extensive efforts at the Los Alamos National Laboratory. The Republicans wrote to "express our serious concerns" about a new report seeming to show decadeslong Chinese government-linked infiltration into New Mexico's Los Alamos National Laboratory, a U.S. weapons and nuclear research site, "and to learn what steps your offices are taking to protect our critical research from malign talent recruitment programs." The Tuesday letter, led by Rep. Michael Waltz (R-FL) and 10 other House Republicans, was addressed to Secretary of Energy Jennifer Granholm and White House Office of Science and Technology Policy Director Arati Prabhakar. Waltz told the Washington Examiner, "The Chinese Communist Party, particularly under Xi Jinping, explicitly aims to become the dominant world superpower in the next decade, and they aim to do it through technology."

Read the full article [here](#).

IS OUR COMPETITOR 'CHINA' OR THE CHINESE COMMUNIST PARTY?

Jimmy Chien | Defense One | October 3, 2022

Words, chosen deliberately, can strengthen or weaken nations. Too often, we conflate "China" and the "Chinese Communist Party," bolstering the authoritarian regime at the expense of our own strategic goals. Understanding why requires a bit of linguistic and cultural history. "China," written 中國, was likely first used during the Warring States period (475-221 BCE) to refer to the central states of the Yellow River valley. During the Song Dynasty (960-1279 CE), it came to describe the civilization at large. The nation-state, however, was not called 中國, but took the name of whichever dynasty was in power at the time. The dynasties are gone, but this tradition endures. In 1949, control of the traditional territory of "China" passed to the People's Republic of China (中華人民共和國), a state ruled by the Chinese Communist Party. As understood by Chinese people, the PRC is the political power that controls the civilizational territories of China. Many Chinese-language speakers refer to the PRC as 中共 (pronounced *zhong-gong*), not 中國 (*zhong-guo*), emphasizing the second character 共, because it denotes the Communist Party.

Read the full article [here](#).



MICHAEL WALTZ WARNS BIDEN ADMINISTRATION ABOUT CHINESE RESEARCH THEFT

Kevin Derby | Florida Daily | October 7, 2022

This week, U.S. Rep. Michael Waltz, R-Fla., warned the Biden administration about “malign foreign talents programs in U.S. federal research.” Waltz sent a letter to U.S. Energy Sec. Jennifer Granholm and Arati Prabhakar, the director of the White House Office of Science and Technology Policy, on the matter. Ten other Republicans on the U.S. House Science, Space and Technology (SST) Committee, including U.S. Rep. Bill Posey, R-Fla., signed the letter. In the letter, Waltz insisted the Chinese Communist Party’s (CCP) Thousand Talents Program was a threat and pointed to “Republican efforts to prevent further Chinese exploitation of American research and technology sectors.” The congressman also pointed to reports from Strider Technologies, Inc., “which found that at least 162 scientists formerly employed at the Los Alamos National Laboratory in New Mexico had returned to China to support the CCP in various domestic and military research and development programs.” Waltz weighed in on the letter this week.

Read the full article [here](#).

6 STEPS COLLEGES AND UNIVERSITIES CAN TAKE TO PROTECT AGAINST CYBER ATTACKS: PART 2

Peggy Bresnick | Fierce Education | March 17, 2021

The U.S. education system ranks last for cybersecurity among U.S. industries, particularly in areas of application security, network security and patching cadence. This is bad news for universities, good news for cyber criminals. Higher education institutions are prime targets for a number of reasons, according to security ratings company SecurityScorecard. Security investments are often put off, especially during the pandemic, when many students are learning remotely even if they live on campus, universities want to make it easy for students and professors to access a wide variety applications and data. Student awareness of cyber safety can be spotty, and students may become easy targets. What’s more, college students typically come to campus with their own laptops, desktops, smart phones and tablets, providing a huge volume and assortment of devices for criminals to attack. And finally, it’s often easy for nefarious strangers to walk through a large campus environment unnoticed, entering research labs and planting USBs.

Read the full article [here](#).

CHINA’S CANDIDATE TO COVERTLY SEED INTO THE U.S. ARMY MAVNI PROGRAM FOUND GUILTY

Christopher Burgess | ClearanceJobs | September 27, 2022

Today, a federal jury convicted Ji Chaoqun of being an illegal agent of China. Readers will recall that we highlighted his attempt to seed himself into the U.S. Army and his connection, via those within the MSS who were being subjected to an FBI counterespionage investigation which led to the identification and ultimate arrest, deportation from Belgium and conviction of MSS officer Yanjun Xu. As it was Yanjun Xu poor operational tradecraft that ultimately allowed for the identification of Ji. All part of a greater effort targeting U.S. aviation industry on behalf of China. Sentencing will occur at a later date.” In May 2016 a recent recipient of a graduate degree in electrical engineering from the Illinois Institute of Technology (IIT) applied to join the U.S. Army Reserves as part of the MAVNI (Military Accessions Vital to the National Interest) program. The graduate, identified as Ji Chaoqun (Ji), a Chinese citizen who came to the U.S. under a student visa. As part of the enlistment process, he was asked to fill out an SF-86, which he submitted on June 6, 2016.

Read the full article [here](#).



'MALIGN INFLUENCE': CHINA'S CULTURAL INSTITUTES UNDER GROWING SCRUTINY

Today | October 9, 2022

Accused of peddling propaganda and even spying, Chinese cultural institutes are facing increasing resistance around the world, forcing some to close down and Beijing to make changes to their management. China has set up hundreds of Confucius Institutes — named after the ancient Chinese philosopher — in more than 150 countries in less than two decades, according to the body that oversees them. President Xi Jinping has called them "a symbol of China's unremitting efforts for world peace and international cooperation", and his administration has marked their "optimisation" and further promotion as an important plank of its education policy. Presented as China's answer to organisations such as Germany's Goethe-Institut or the British Council, they offer language lessons and cultural exchange programmes. Unlike most of their Western counterparts, they often sit within universities. But as relations with China have deteriorated and Mr Xi has taken a more aggressive foreign policy approach, an increasing number of critics in the West say the institutes have become a threat. In June, Germany's Education Minister Bettina Stark-Watzinger warned the language centres were being "used by the Communist Party for political ends".

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>*

