



ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

<https://asce.tamus.edu>

THE OPEN SOURCE MEDIA SUMMARY

November 30, 2022

HOW CHINA IS TRYING TO TURN THE US CHIPS ACT TO ITS FAVOR

SZ Tan and Peter W. Singer | Defense One | November 16, 2022

When the Chips and Science Act (frequently referred to as the CHIPS Act) was signed into law in August, President Biden and Congressional lawmakers celebrated. The legislation included subsidies to bolster America's domestic semiconductor industry and tackle supply chain vulnerabilities, addressing key national security concerns with China. The Biden administration boasted that the CHIPS Act would lower costs, create jobs, strengthen supply chains, and counter China. But China has not taken the news lying down. The PRC has mobilized a strategic communications campaign to undermine support for the Act. "A perfect example of overreacting and coercion," tweeted Hua Chunying, a spokesperson for the PRC's Ministry of Foreign Affairs, shortly after the bill became law. Hua drew an analogy of the world as a classroom, where everyone is studying hard to get good grades, and suddenly, one student cuts the electricity and threatens the other students in the name of upholding classroom order. "Anyone like this guy? Seriously?" she added. As Hua's tweet suggests, the PRC counter-offensive aims to depict the U.S. as a fading global hegemon trying to tip the global playing field back in its favor.

Read the full article [here](#).

CHINESE GOVERNMENT INTELLIGENCE OFFICER SENTENCED TO 20 YEARS IN PRISON FOR ESPIONAGE CRIMES, ATTEMPTING TO STEAL TRADE SECRETS FROM CINCINNATI COMPANY

U.S. Department of Justice | U.S. Attorney's Office, Southern District of Ohio | November 16, 2022

The first Chinese government intelligence officer ever to be extradited to the United States to stand trial was sentenced today in federal court in Cincinnati. Yanjun Xu was sentenced to 20 years in prison. Xu targeted American aviation companies, recruited employees to travel to China, and solicited their proprietary information, all on behalf of China. "This case sends a clear message: we will hold accountable anyone attempting to steal American trade secrets," said U.S. Attorney Kenneth L. Parker. "Xu conspired to steal American science and technology. Thanks to the diligent work of the FBI, GE Aviation, and our trial team, he'll spend decades in federal prison. The historic sentencing of a Chinese government official for committing espionage against the U.S. is a significant achievement and also should serve as a warning to foreign governments that the U.S. will not tolerate this type of illegal activity," stated FBI Cincinnati Special Agent in Charge J. William Rivers. "The FBI and our partners will continue to investigate and prosecute those who attempt to steal the sophisticated technologies of U.S. companies, our military, and our government."

Read the full article [here](#).



ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

MATHEMATICAL THEOREM USED TO CRACK US GOVERNMENT ENCRYPTION ALGORITHM

Catarina Chagas | Queen's University | Phys.org | November 23, 2022

In the digital era and moving towards quantum computing, protecting data against hack attacks is one of our biggest challenges—and one that experts, governments, and industries worldwide work hard to address. While this is an effort to build a more connected and safe future, it can certainly learn from the past. In July, the US National Institute of Standards and Technology (NIST) selected four encryption algorithms and posed some challenge problems to test their security, offering a \$50,000 reward for whomever managed to break them. It happened in less than an hour: one of the promising algorithm candidates, named SIKE, was hacked with a single personal computer. The attack did not rely on a powerful machine, but on powerful mathematics based on a theorem developed by a Queen's professor decades ago. Ernst Kani has been researching and teaching since the late 1970s—first at the University of Heidelberg, in Germany, and then at Queen's, where he joined the Department of Mathematics and Statistics in 1986. His main research focus is arithmetic geometry, an area of mathematics that uses the techniques of algebraic geometry to solve problems in number theory. The problems Dr. Kani works to solve stretch back to ancient times.

Read the full article [here](#).

ACADEMIC RESEARCH SECURITY

U.S. Department of Defense | Office of the Under Secretary of Defense for Research & Engineering

The Department of Defense greatly values its partnership with the academic community. Of paramount importance to the integrity and effectiveness of the academic research community has been the open, transparent, and merit-based nature of research collaborations. In recent years the Department, along with other federal research funding agencies, has become concerned that foreign governments may try to undermine the integrity of the academic research enterprise. This site is a resource for the actions that the Department and the interagency are taking to ensure the integrity of fundamental research in academia as well as steps that the academic community has taken. This site does not cover security measures for research that is not designated as fundamental research, which may include CUI or classified research that require additional protection. The Department welcomes dialogue with our partners in academia about ways to mitigate risks to academic research.

Read the full article [here](#).

UNIVERSITY ENGAGEMENT WITH CHINA: AN MIT APPROACH

Richard Lester and Lily Tsai (co-chairs), Suzanne Berger, Peter Fisher, M. Taylor Fravel, David Goldston, Yasheng Huang, and Daniela Rus | The MIT China Strategy Group | November 2022

The subject of this report is MIT's future relationship with China. The question it addresses is how the Institute and other American research universities should engage with organizations and individuals in countries whose political leaders are pursuing policies that are irreconcilable with basic human rights and values and that pose security risks to the United States. While China is the focus of this report, some of the findings apply to MIT's relations with other countries, too. The outlook for the China relationship is increasingly uncertain because of the harsher political climate in China, the intensifying geopolitical and strategic rivalry between China and the United States, and concerns over attempts by Chinese interests to gain advantage over the United States by exploiting American university research. MIT has flourished because it has been a magnet for the world's most talented students, scholars, and innovators, many of them from China.

Read the full article [here](#).



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.

Read the full article [here](#).

INTERSECTIONS – TECHNOLOGY, NATIONAL SECURITY, AND US-CHINA STRATEGIC COMPETITION

The Center for Naval Analyses (CNA) | November 2022

With this issue, CNA's China and Indo-Pacific Security Affairs Division launches Intersections, a limited-series news digest describing the interplay between the People's Republic of China's (PRC's) technology acquisition efforts, US and partner nation responses to those efforts, and the critical and emerging technology risks for the US defense industrial base posed by the PRC's actions. CNA has documented a wide range of legal and illegal techniques to acquire foreign technologies that the PRC uses to achieve its national security objectives and build military capabilities (see graphic). Recognizing these techniques, and evaluating the evolving global technology landscape, is essential for understanding US-China strategic competition and devising technology protection policies. This newsletter highlights recent developments in PRC technology acquisition strategies, technology transfer risks, and government actions to protect critical and emerging technologies that have military applications.

Read the full article [here](#).

A WRONGFULLY TERMINATED CHINESE-AMERICAN SCIENTIST WAS JUST AWARDED NEARLY \$2 MILLION IN DAMAGES

Eileen Guo | MIT Technology Review | November 10, 2022

It's been almost a decade since the Chinese-American hydrologist Sherry Chen's life was turned upside down by an unfounded accusation of spying, and this week, she finally received something like justice. Today, Chen's lawyers announced that the scientist won a historic \$1.75 million settlement from the US Commerce Department for her wrongful prosecution and subsequent termination from the National Weather Service. "The government's investigation and prosecution of me was discriminatory and unjustified," Chen said in a statement. "The Commerce Department is finally being held responsible for its wrongdoing ... No one else should have to endure this injustice." Chen's case was an early instance of what would become a much bigger pattern of the US government's increasing suspicion of Chinese and Chinese-American scientists amid growing competition between the US and China. The settlement is a personal and symbolic victory after years of persecution.

Read the full article [here](#).



5 CYBERSECURITY TIPS SO YOU CAN SLEEP AT NIGHT

Jason Lee | Splunk | November 14, 2022

There's a joke I like to tell about what keeps C-level executives up at night. The shorthand version is that unlike the rest of the leadership team, the CISO's bed is made but no one sleeps in it. It's been almost two months since I joined Splunk as Chief Information Security Officer and my team has been focusing on Splunk's own foundational security and continuing our ongoing efforts to protect our customers – so security isn't the thing keeping them up at night. The reality is that it's not if a breach or exploit will occur, it's when. So organizations need to be ready to respond and recover when an incident occurs. Here are five tips on preparing for a cyberattack. The first line of defense is ensuring employees are informed and routinely trained on security policies.

Read the full article [here](#).

U.S. RESEARCH AND DEVELOPMENT FUNDING AND PERFORMANCE: FACT SHEET

Congressional Research Service | September 13, 2022

Research and development (R&D) in the United States is funded and performed by a number of sectors—including the federal government, state governments, businesses, academia, and nonprofit organizations—for a variety of purposes. This fact sheet begins by providing a profile of the U.S. R&D enterprise, including historical trends and current funding by sector and by whether the R&D is basic research, applied research, or development. The final section of this fact sheet includes data on R&D performance by sector. The United States became a global leader in R&D in the 20th century, funding as much as 69% of annual global R&D in the period following World War II.¹ Figure 1 shows the growth in total U.S. R&D expenditures from 1956 to 2020 in current dollars.² U.S. R&D in 2020 was 83 times higher than it was in 1956 in current dollars, and more than 11 times higher in constant dollars.³

Read the full article [here](#).

MIRATI THERAPEUTICS SUES CHINA'S INVENTISBIO FOR 99 MILLION RMB IN TRADE SECRET THEFT CASE

Aaron Wininger | The National Law Review | November 17, 2022

Per a securities filing by InventisBio Co (益方生物科技(上海)股份有限公司) on November 16, 2022, Mirati Therapeutics sued InventisBio for 99 Million RMB (~\$14 million USD) in a trade secret misappropriation case. Mirati requested an injunction, damages, and confirmation of ownership of certain patents and applications in a filing with the Shanghai Intellectual Property Court that was received by InventisBio on November 14, 2022. This case highlights the increased attention recently paid to trade secret misappropriation in China including a 60 million RMB settlement in a microelectronics case and a 159 million RMB verdict in a vanillin case. Mirati asserted that trade secrets of a certain preclinical research project of Mirati were the same or substantially the same as trade secrets used by InventisBio and a subsidiary and were being infringed. Mirati also alleged that the patents and applications obtained by InventisBio and a subsidiary should be owned by Mirati and its subsidiary.

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.tamug.edu>

