ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

May 24, 2023

FACT SHEET: BIDEN-HARRIS ADMINISTRATION ANNOUNCES NATIONAL STANDARDS STRATEGY FOR CRITICAL AND EMERGING TECHNOLOGY

The White House | May 4, 2023

Today, the Biden-Harris Administration released the United States Government's National Standards Strategy for Critical and Emerging Technology (Strategy), which will strengthen both the United States' foundation to safeguard American consumers' technology and U.S. leadership and competitiveness in international standards development. Standards are the guidelines used to ensure the technology Americans routinely rely on is universally safe and interoperable. This Strategy will renew the United States' rules-based approach to standards development. It also will emphasize the Federal Government's support for international standards for critical and emerging technologies (CETs), which will help accelerate standards efforts led by the private sector to facilitate global markets, contribute to interoperability, and promote U.S. competitiveness and innovation. The Strategy focuses on four key objectives that will prioritize CET standards development: Investment: Technological contributions that flow from research and development are the driving force behind new standards.

Read the full article here.

PENTAGON OUTLINES UPCOMING CONTRACTOR CYBERSECURITY PLAN

Lauren C. Williams | FCW | May 19, 2023

By November, Pentagon cybersecurity leaders aim to lay out just how private contractors will be expected to work with government agencies to safeguard data and ward off attacks. "We are working on a strategy—a [defense industrial base] cybersecurity strategy—that we hope to have out later this year," David McKeown, DOD's chief information and security officer, said at GovExec's Cyber Summit event Thursday. "Our strategy is bringing all of the pieces and parts within the department together…laying it out who's going to be doing what, and we overlay everything on top of the NIST cybersecurity framework." Lawmakers requested the strategy as a step toward reducing the vulnerabilities created by doing sensitive business with hundreds of thousands of private contractors. McKeown said the strategy would have several phases, starting with identifying what needs to be protected, then figuring out what measures are needed to protect data, detect intrusions, respond to attacks, and recover from them. For example, DOD's pending cyber certification program, CMMC, will fall under the "protect" phase.

Read the full article here.

JUSTICE DEPARTMENT FILES CRIMINAL CHARGES IN CASES OF AMERICAN TECH STOLEN FOR RUSSIA, CHINA AND IRAN

Hannah Rabinowitz | CNN | May 16, 2023

The Justice Department announced on Tuesday five criminal cases against people accused of stealing or illegally diverting American technology and materials for the Russian, Chinese and Iranian governments. The cases are the first enforcement actions by the department's Disruptive Technology Strike Force, which aims to counter efforts by "hostile nation-states" to illegally acquire sensitive US technology "to advance their authoritarian regimes and facilitate human rights abuses." Four arrests were made, but some defendants remain at large, according to the Justice Department. In one case, prosecutors said a Chinese citizen and former Apple Inc. engineer, who has been charged in northern California, allegedly stole "thousands of documents containing the source code for software and hardware pertaining to Apple's autonomous vehicle technology." The defendant, Weibao Wang, is now believed to be working for a China-based autonomous vehicle competitor. CNN has reached out to Apple for comment.

Read the full article here.

"THE COMPLEXITY OF TECHNOLOGY'S CONSEQUENCES IS GOING UP EXPONENTIALLY, BUT OUR WISDOM AND AWARENESS ARE NOT."

Tristan Harris and Sara Frueh | Issues in Science and Technology | May 16, 2023

Tristan Harris is a technology ethicist and the cofounder of the Center for Humane Technology. He'll be speaking at the Nobel Prize Summit 2023: Truth, Trust, and Hope at the National Academy of Sciences on May 24–26. In advance of the summit, Harris talked with Issues editor Sara Frueh about the challenge of online misinformation, ways to govern artificial intelligence, and a vision of technology that strengthens democracy. Oftentimes people think, "Well, I'll do it personally in a way that is nuanced and offers context, and if I can be one of the good actors, maybe I can set an example, and maybe other people will follow me, and then maybe it'll be a race to the top for who does that nuanced, context-driven thing better." But the fundamental problem is an engagement-based design paradigm in which, for example, social media algorithms rank which content we see, and the design choices reward shorter, bite-sized bits of information that prefer a lack of context and nuance. This is a side effect of sorting for what is engaging—and engaging is sticky and mimetic and simple.

Read the full article here.

EX-HARVARD PROFESSOR CHARLES LIEBER GETS HOUSE ARREST OVER CHINA TIES

Chloe Kim | BBC News | April 26, 2023

Former Harvard professor Charles Lieber was sentenced to six months of house arrest on Wednesday, according to US media. He was found guilty in 2021 of making false statements to authorities, filing false tax returns and failing to report a Chinese bank account. Critics say a US campaign to counter economic espionage from China hurts the academic community. Lieber's lawyers asked he be spared prison time because he has cancer. US District Judge Rya Zobel in Boston also sentenced him two years of supervised release and to one day in prison, which he has already served following his arrest. He must also pay a $50,000 (£40,100) fine, Bloomberg and Semafor reported. His lawyers said he was remorseful and had been punished enough because, they claimed, "his reputation has been ruined". Prosecutors recommended three months in prison, a year of probation and a $150,000 fine along with a $33,600 restitution to the Internal Revenue Service - which Lieber has already paid.

Read the full article here.

CHINESE FIRMS THAT THREATEN U.S. SECURITY CAN GET INVESTMENT FROM FEDERAL EMPLOYEES

Valerie Bauman and Didi Kirsten Tatlow | Newsweek | May 22, 2023

Millions of federal employees can invest in Chinese companies sanctioned by the U.S. government via its flagship retirement plan, even though these companies have been branded a danger to national security or are accused of profiting from forced labor or other human rights abuses, Newsweek has learned. Since June 2022, the federal government's employee retirement plan—the largest in the world with $720 billion in assets—has offered its 6.8 million members the option to invest some of their savings in an account containing about 5,000 mutual funds, some of which have holdings in Chinese companies that are on at least nine U.S. government sanctions or watch lists, according to an exclusive analysis for Newsweek by Washington D.C.-based consulting firm Kilo Alpha Strategies, using data from the Coalition for a Prosperous America. Among those companies are a leading developer of engines for fighter planes and turbines for naval ships, solar panel firms targeted for allegedly using forced labor by Uyghurs and others living in China's western Xinjiang region, as well as makers of surveillance systems seen as a threat to the U.S.

Read the full article here.

MALWARE TURNS HOME ROUTERS INTO PROXIES FOR CHINESE STATE-SPONSORED HACKERS

Dan Goodin | ARS Technica | May 17, 2023

Researchers on Tuesday unveiled a major discovery—malicious firmware that can wrangle a wide range of residential and small office routers into a network that stealthily relays traffic to command-and-control servers maintained by Chinese state-sponsored hackers. A firmware implant, revealed in a write-up from Check Point Research, contains a full-featured backdoor that allows attackers to establish communications and file transfers with infected devices, remotely issue commands, and upload, download, and delete files. The implant came in the form of firmware images for TP-Link routers. The well-written C++ code, however, took pains to implement its functionality in a “firmware-agnostic” manner, meaning it would be trivial to modify it to run on other router models. The main purpose of the malware appears to relay traffic between an infected target and the attackers’ command and control servers in a way that obscures the origins and destinations of the communication.

Read the full article here.

20 WAYS TO ENSURE SECURITY REMAINS/BECOMES EVERYONE’S RESPONSIBILITY

Steve Prentice | CISO Series | May 17, 2023

Every security department has a limitation: it can’t be on the front lines of every business activity all the time. The charge to make security everyone’s responsibility is vital for a security program to succeed.‟ As technology becomes more ubiquitous and the threat landscape continues to evolve, organizations can no longer rely solely on their security teams to protect against cyberattacks. Everyone within an organization is a potential target and must be prepared to respond,” said Rama Balla, cloud/cyber security architect, Macquarie Group. Art Ocain (@ArtIsGrowth), CIO and CISO, Airiam, added, “In an era where cunning insider-threat attacks like Lapsus$ prey on corporate employees, it’s crucial to foster a culture that not only raises security awareness but also motivates people to actively safeguard the organization.” We asked our community of experts for their suggestions for getting everyone onboard and committed to a positive security culture.

Read the full article here.

THE STATE OF U.S. SCIENCE AND ENGINEERING 2022

Amy Burke, Abigail Okrent, and Katherine Hale | National Science Foundation | January 18, 2022

The State of U.S. Science and Engineering shows that strengthening the U.S. S&E enterprise is critical to maintaining the U.S. position as a lead performer and collaborator of S&T activities globally (see Glossary section for definition of terms used in this report). Currently, the United States leads the world on several S&E fronts. The successful development of COVID-19 vaccines demonstrates that the U.S. S&E enterprise is strong and can effectively collaborate internationally across sectors. Globally, the United States performed the most R&D ($656 billion, preliminary estimate) in 2019. However, the United States' role as the world's foremost performer of R&D is changing as Asia continues to increase its investments. Growth in R&D and S&T output by other countries, including China, outpaced that of the United States. Consequently, even as U.S. R&D has increased, the U.S. share of global R&D has declined, and the relative position of the United States in some S&T activities has either not changed or decreased even as absolute activities increased.

Read the full article here.

DESPITE RISKS, EU CONTINUES TO FUND RESEARCH WITH CHINESE MILITARY-LINKED UNIVERSITIES

David Matthews and Richard L. Hudson | Science Business | May 16, 2023

Despite efforts to prevent EU technology leaking to China's military, the European Commission is continuing to fund at least five research projects involving some of China's top military-linked universities. The projects, research by Science|Business finds, involve heat transfer, data security and other technologies that could have dual civilian and military use. China's participation includes four of its so-called Seven Sons of National Defence, top-ranked universities controlled by the industry ministry and producing most technical graduates that work for its state defence industry. Under standard EU rules, the Chinese get their own funding for their work in the projects, but as official "participants" they can share in the European research, meetings and staff exchanges. The projects in question are five on-going Marie Skłowdowska Curie Actions (MSCA), that facilitate staff exchanges and network-building among research institutions. Four of the five were started under the EU's old Horizon 2020 programme, but a fifth began only this March under the Horizon Europe programme.

Read the full article here.

U.S. TECH ESPIONAGE TEAM UNVEILS FIRST CASES INVOLVING CHINA AND RUSSIA

Ana Swanson | The New York Times | May 16, 2023

The Biden administration announced arrests and criminal charges on Tuesday in five cases involving sanctions evasion and technology espionage efforts linked to Russia, China and Iran. Two Russian nationals were taken into custody last week under accusations of sending aircraft parts to Russia in violation of sanctions imposed after the invasion of Ukraine. In another case, a former Apple engineer is accused of stealing the company's autonomous vehicle technology to provide it to a Chinese competitor. The announcements were the work of a recently established "technology strike force," which aims to protect critical American technology or data from theft by hostile nations. The strike force was set up in February and brings together agents with the Commerce and Justice Departments, as well as the F.B.I. and local attorneys offices. Federal agents are working to trace the global movement of U.S. goods and data, as well as the funds used to pay for them.

Read the full article here.

SAFEGUARDING OUR FUTURE – BEWARE OF FOREIGN GIFTS WITH STRINGS ATTACHED

The National Counterintelligence and Security Center | June 19, 2020

City-to-city partnership agreements could be used by foreign powers to advance a political goal or influence government decisions. What seems good for your city or state may undermine strategic U.S. interests. You may be manipulated to support a foreign malign narrative or hidden agenda. A foreign power may seek your support to gain a political or economic advantage. May receive sub-par donations while the donor receives a propaganda boon. Be aware of the consequences of your actions-locally and nationally. Understand your role and the potential press coverage your acceptance will draw. Beware of those who would ask you to advance a position or lobby on behalf of another nation or group. Beware of gifts of "smart" technology with potential for storing/transferring sensitive data.

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