ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

April 19, 2023

THE PRECARIOUS BALANCE BETWEEN RESEARCH OPENNESS AND SECURITY

E. William Colglazier | Issues in Science and Technology | Spring 2023

The United States is in the middle of a debate on the appropriate balance between openness and security for scientific research and development—a balance that has shifted significantly since the end of the Cold War. The COVID-19 pandemic, competition between the United States and China, the Russian invasion of Ukraine, increasing deglobalization, fraying supply chains, and current economic stresses have dramatically increased US political leaders' concerns with international scientific and technological collaboration. This shift has bridged deep political divides to create a growing consensus among elected officials. The CHIPS and Science Act, approved by large majorities in the House and Senate in August 2022, along with new regulations from the Biden administration in October 2022, not only advance the US semiconductor industry but also limit China's ability to acquire certain advanced chips and manufacturing technologies. In January 2023, a bipartisan vote in the House of Representatives approved the creation of the Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party to investigate issues such as the origin of SARS-CoV-2 and to recommend policy changes.

Read the full article here.

PROTECTING U.S. TECHNOLOGICAL ADVANTAGE

National Academies of Sciences, Engineering, and Medicine | 2022

U.S. leadership in technology innovation is central to our nation's interests, including its security, economic prosperity, and quality of life. Our nation has created a science and technology ecosystem that fosters innovation, risk taking, and the discovery of new ideas that lead to new technologies through robust collaborations across and within academia, industry, and government, and our research and development enterprise has attracted the best and brightest scientists, engineers, and entrepreneurs from around the world. The quality and openness of our research enterprise have been the basis of our global leadership in technological innovation, which has brought enormous advantages to our national interests. In today's rapidly changing landscapes of technology and competition, however, the assumption that the United States will continue to hold a dominant competitive position by depending primarily on its historical approach of identifying specific and narrow technology areas requiring controls or restrictions is not valid. Further challenging that approach is the proliferation of highly integrated and globally shared platforms that power and enable most modern technology applications.

Read the full article here.

HOW TO EVALUATE AND IMPLEMENT THE NATIONAL CYBERSECURITY STRATEGY

Rebecca Sammons | Government Technology Insider | April 13, 2023

The Biden Administration recently released the National Cybersecurity Strategy, which provides both public and private sector with a higher-level policy document for securing cyberspace with a proactive approach to cybersecurity. While this strategy provides additional guidance to the 2021 Cybersecurity Executive Order, federal agencies will still likely face many challenges when it comes to implementation. We talked with Simon Szykman, Senior Vice President for Client Growth at Maximus, who was involved with the development of the National Strategy to Secure Cyberspace under the Bush Administration in 2003. We discuss anticipated challenges when trying to improve cybersecurity efforts and strategies for successful implementation of the policies introduced by the National Cybersecurity Strategy. The Executive Order is centered around the president directing federal agencies within the executive branch to do everything within their ability to improve cybersecurity. If you take a look at the Executive Order, you'll see a lot of direction assigned to the Office of Management and Budget (OMB), agencies and agency leadership to take on certain roles and responsibilities to improve cybersecurity within their missions.

Read the full article here.

FBI MAKES PROBABLE CAUSE ARREST IN CONNECTION WITH CLASSIFIED DOCUMENTS LEAK

Alexander Mallin, Jack Date, Luke Barr, Pierre Thomas, Matt Seyler, Aaron Katersky, and Alexandra Hutzler | ABC News | April 13, 2023

The FBI on Thursday made a probable cause arrest in North Dighton, Massachusetts, in connection with the leaked documents probe. Attorney General Merrick Garland announced Jack Teixeira was taken into custody in relation to the investigation into "alleged authorized removal, retention and transmission of classified national defense information." Teixeira, 21, is a member of the Massachusetts Air Force National Guard. "FBI agents took Teixeira into custody earlier this afternoon without incident," the attorney general said. "He will have an initial appearance at the U.S. District Court for the District of Massachusetts." Garland continued: "I want to thank the FBI, Justice Department prosecutors and our colleagues at the Department of Defense for the diligent work on this case. This investigation is ongoing. We will share more information at the appropriate time." The FBI said it was continuing to conduct law enforcement activity at the residence where Teixeira was arrested.

Read the full article here.

ZERO TRUST MATURITY MODEL

Cybersecurity and Infrastructure Security Agency

Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. The goal is to prevent unauthorized access to data and services and make access control enforcement as granular as possible. Zero trust presents a shift from a location-centric model to a more data-centric approach for fine-grained security controls between users, systems, data and assets that change over time; for these reasons. This provides the visibility needed to support the development, implementation, enforcement, and evolution of security policies. More fundamentally, zero trust may require a change in an organization's philosophy and culture around cybersecurity. CISA's *Zero Trust Maturity Model* is one of many roadmaps that agencies can reference as they transition towards a zero trust architecture.

Read the full article here.

AI TOOLS LIKE CHATGPT LIKELY TO EMPOWER HACKS, NSA CYBER BOSS WARNS

Colin Demarest | C4ISRNET | April 12, 2023

Generative artificial intelligence that fuels products like ChatGPT will embolden hackers and make email inboxes all the more tricky to navigate, according to the U.S. National Security Agency cybersecurity director. While much-debated AI tools will not automate or elevate every digital assault, phishing scheme or hunt for software exploits, NSA's Rob Joyce said April 11, what it will do is "optimize" workflows and deception in an already fast-paced environment. "Is it going to replace hackers and be this super-AI hacking? Certainly not in the near term," Joyce said at an event hosted by the Center for Strategic and International Studies think tank. "But it will make the hackers that use AI much more effective, and they will operate better than those who don't." U.S. officials consider mastery of AI critical to long-term international competitiveness — whether that's in defense, finance or another sector. At least 685 AI projects, including several tied to major weapons systems, were underway at the Pentagon as of early 2021.

Read the full article here.

ABANDONING THE US, MORE SCIENTISTS GO TO CHINA

David J. Bier | CATO Institute | April 11, 2023

The Organisation for Economic Co-operation and Development (OECD)—an intergovernmental organization with 38 member countries—has published new data showing that the United States is losing the race for scientific talent to China and other countries. China's strategy to recruit scientific researchers to work at China-affiliated universities is working. In 2021, the United States lost published research scientists to other countries, while China gained more than 2,408 scientific authors. This was a remarkable turnaround from as recently as 2017 when the United States picked up 4,292 scientists and China picked up just 116. As Figure 1 shows, the rest of the OECD and China have both surpassed the United States for net inflow of scientific authors. The OECD data are not measuring the movement of non-Chinese into China or non-Americans into the United States. The OECD tracks inflows and outflows of published scientific researchers based on changes in institutional affiliation. If an author who was previously affiliated with a different country publishes another article in a new country, the new country will be credited as receiving a new research scientist.

Read the full article here.

FBI ARRESTS TWO ALLEGED CHINESE AGENTS AND CHARGES DOZENS WITH WORKING INSIDE US TO SILENCE DISSIDENTS

Hannah Rabinowitz, Evan Perez, and Lauren del Valle | CNN | April 18, 2023

The FBI has arrested two alleged Chinese agents and federal prosecutors have charged dozens of others with working to silence and harass dissidents within the United States -- with some even operating an "undeclared police station" in New York City. Lu Jianwang and Chen Jinping allegedly operated the police station in New York City's Chinatown. Both men are US citizens and have been charged with conspiring to act as agents of the Chinese government and obstructing justice. The police station has been shut down since a search warrant was executed at the location last fall, according to John Marzulli, a spokesman for the US Attorney in the Eastern District of New York. The two men appeared in court Monday, with Lu being released on a $250,000 bond and Chen on a $400,000 bond. They are not permitted to travel within half a mile of the Chinese consulate nor mission or communicate with co-conspirators. Neither has entered a plea.

Read the full article here.

DON'T USE PUBLIC PHONE CHARGING STATIONS: FBI

Stephen Neukam | The Hill | April 10, 2023

The FBI is warning people to not use public phone charging stations, which have become increasingly popular in places like airports and shopping malls. The problem is that hackers have found a way to introduce malware and other software onto devices through the public stations, the FBI said. "Avoid using free charging stations in airports, hotels or shopping centers," the FBI's Denver Twitter account said. "Bad actors have figured out ways to use public USB ports to introduce malware and monitoring software onto devices. Carry your own charger and USB cord and use an electrical outlet instead." The warning on social media mirrors guidance the bureau offers on its website. The FBI's Denver office told The Hill nothing prompted the warning on its social media and that it was simply a public service announcement. The FBI is not alone in its warning to avoid the USB charging stations.

Read the full article here.

CISA INTRODUCES SECURE-BY-DESIGN AND SECURE-BY-DEFAULT DEVELOPMENT PRINCIPLES

Kevin Townsend | Security Week | April 14, 2023

CISA has described and published a set of principles for the development of security-by-design and security-by-default cybersecurity products. Pillar Three of the National Cybersecurity Strategy published on March 1, 2023 is titled 'Shape market forces to drive security and resilience'. Within this section the Administration makes two points very clear. Firstly, security liability must be shifted away from the use of security products to the development of security products; and secondly, federal procurement power will be used to encourage this shift. Both points were previewed in a speech given by CISA director Jen Easterly at Carnegie Mellon days earlier (February 27, 2023). She noted that insecurity has become normalized, and that the onus is currently on the user to make use of products less risky. She said this must change, so that the user is forced into making usage more rather than less risky.

Read the full article here.

AMERICA, CHINA AND A CRISIS OF TRUST

Thomas L. Friedman | The New York Times | April 14, 2023

I just returned from visiting China for the first time since Covid struck. Being back in Beijing was a reminder of my first rule of journalism: If you don't go, you don't know. Relations between our two countries have soured so badly, so quickly, and have so reduced our points of contact — very few American reporters are left in China, and our leaders are barely talking — that we're now like two giant gorillas looking at each other through a pinhole. Nothing good will come from this. The recent visit by Taiwan's president, Tsai Ing-wen, to the United States — which prompted Beijing to hold live-fire drills off Taiwan's coast and to warn anew that peace and stability in the Taiwan Strait are incompatible with any move by Taiwan toward formal independence — was just the latest reminder of how overheated this atmosphere is. The smallest misstep by either side could ignite a U.S.-China war that would make Ukraine look like a neighborhood dust-up.

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

ASCE
ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM