ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

December 14, 2022

PCAST RELEASES REPORT ON STRENGTHENING BIOMANUFACTURING TO ADVANCE THE BIOECONOMY

The White House | December 8, 2022

The President's Council of Advisors on Science and Technology (PCAST) is recommending actions for maintaining United States competitiveness in the global bioeconomy. Released today, a new report recommends actions to promote the growth of the U.S. bioeconomy in three key areas: boosting manufacturing capacity, addressing regulatory uncertainty, and updating our national strategy to meet the demands of the 21st century. "Biomanufacturing is integral to solutions for many of our national and global challenges, including resource utilization, climate change, economic stability, environmental justice, and improved health," said Frances Arnold, PCAST co-chair. "This PCAST report will help set in motion actions that accelerate progress in developing the bioeconomy." The Biden-Harris Administration's Executive Order 14081, Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy, and the CHIPS and Science Act, help position the United States to maintain its leadership in biomanufacturing by bolstering infrastructure for the bioeconomy, supporting a diverse domestic workforce, and catalyzing the country's scientific and technological pursuits.

Read the full article here.

HOW THE DECADES-LONG CHINESE ESPIONAGE CAMPAIGN "STOLE" US MILITARY TECHNOLOGY

Kris Osborn | Warrior Maven - Center for Military Modernization | December 7, 2022

Paradigm-changing deep-penetrating warheads, new hardened, heat resistant nano-composite materials enabling hypersonic weapons flight, vertical take-off-and-landing drones and a new generation of submarine "quieting" technologies are all massively impactful breakthrough technology of vital significance to cutting-edge and future US weapons systems. All of these areas of innovation and scientific exploration, some of which involved the discovery and development of "disruptive" or breakthrough technologies, were heavily focused upon in recent decades at the well known, prestigious US Los Alamos National Laboratory. However, to put things simply and clearly, many of the US-driven technological advances in these critical areas appear to have been stolen by Chinese spies. Technologically driven Chinese espionage at Los Alamos hit the news in a very public way earlier this year, following a private counterintelligence investigation. The discoveries shined additional light on the concerning and well-documented problems arising from Chinese cyber attacks, espionage and deliberate efforts to "steal" sensitive US military technology.

Read the full article here.

GOOGLE CLOUD GETS DOD'S BLESSING. BUT WILL IT WIN CONTRACTS?

Lauren C. Williams | Defense One | December 6, 2022

Google is one step closer to being a cloud provider contender for the Defense Department. The Pentagon's IT agency granted the tech giant provisional authority to host sensitive, unclassified information from national security systems—a key requirement for the Defense Department's data-sharing plans with Joint All Domain Command and Control, or JADC2. Google cloud services span infrastructure, platform, and software "capabilities across public and hybrid cloud environments, supporting up to [Impact Level 5] data for DOD and federal communities," according to the Defense Information Systems Agency's blog post announcing the decision. The Defense Department has six security levels designated for cloud providers, with Impact Level 6 reserved for classified data. "This authorization will provide the warfighter another safe, secure cloud-hosting capability to store and process mission-critical information," Air Force Lt. Gen. Robert Skinner, DISA's director and commander of the Joint Force Headquarters-Department of Defense Information Network, said in the blog post.

Read the full article here.

US MILITARY'S NATIONAL MEDIA EXPLOITATION CENTER TO REFOCUS ON CHINA

Colin Demarest | C4ISRNET | December 7, 2022

U.S. officials plan to shrink the National Media Exploitation Center, a hub coordinating FBI, CIA, Defense Intelligence Agency and National Security Agency efforts to parse documents, video, audio and other information sources for defense and intelligence distribution, to better position it for a future competition with China. "We are in the process right now of trying to define what it looks like for NMEC to succeed, when its primary focus is no longer on a terrorist hiding in a cave in Afghanistan," John Kirchhofer, the DIA's chief of staff, said Nov. 29 at a livestreamed Intelligence and National Security Alliance event. "We are reducing the size of NMEC, and we want what's left of it to be really hyper-focused on strategic competition." The clearinghouse was established in 2001 to harmonize the receipt, analysis and sharing of documents and other information seized by the U.S. military and intelligence community.

Read the full article here.

HOW U.S.-CHINA TENSIONS HAVE HURT AMERICAN SCIENCE

Ilaria Mazzocco and Maya Mei | Big Data China | December 9, 2022

There is a growing concern in Washington that the United States government, its companies, and universities have helped drive the rapid growth of China's high-tech sector to the detriment of America's overall national interest. Accusations of intellectual property (IP) theft and state-sponsored industrial espionage by China have loomed large in the bilateral relationship. These concerns were at the heart of the Section 301 investigation launched by the U.S. Trade Representative (USTR) in 2018, which resulted in the subsequent imposition of tariffs and a trade war between the two countries. Moreover, as competition between Washington and Beijing deepens, the Biden administration has made it clear that it believes the United States must maintain as big of a lead as possible in key technologies, even if this means constraining previously permitted commercial sales and investments. Such sweeping policies on research and technology have had a chilling effect on academic collaboration between the United States and China. Reducing Chinese access to U.S. technology and cutting-edge research may be desirable for national security motivations regardless of the broader impact, but policymakers should be aware of the potential ramifications for the United States.

Read the full article here.

AN EXPLORATORY ANALYSIS OF THE CHINESE HYPERSONICS RESEARCH LANDSCAPE

Geoffrey Chambers, PhD | BluePath Labs | China Aerospace Studies Institute | December 5, 2022

A 2012 book by two leading HV researchers Cai Guobiao and Xu Dajun provides a framework that informs our understanding and evaluation of Chinese HV research and development (R&D) priorities and activities. The authors, being well-versed in the layout and capabilities of the Chinese aerospace R&D ecosystem, identified 31 technologies organized into the six categories to serve as the basic framework guiding R&D activities. To assist R&D program planners in their formulation of China's HV research development strategy, they derived an HV Technology Criticality Ranking of the 31 technologies based on their assessment of the significance of these technologies for HV development and their required level of effort needed to make significant progress. The motivations for and techniques used by Cai and Xu in developing their HV development framework and the associated technology criticality rankings are analogous to the US Air Force's Lead-Leverage-Watch model or the US Army's Lead-Collaborate-Watch model for R&D research prioritization.

Read the full article here.

NETHERLANDS PLANS NEW CURBS ON CHIP-MAKING EQUIPMENT SALES TO CHINA

Kanjyik Ghosh | Reuters | December 8, 2022

The Netherlands plans new controls on exports of chip-making equipment to China and a deal could be announced next month, Bloomberg News reported on Thursday, citing people familiar with the matter. Dutch firm ASML Holdings NV (ASML.AS) is a world leader in semiconductor production equipment and had sales to customers in China of more than 2 billion euros ($2.1 billion) last year. However since 2018 the Dutch government has not granted ASML licences to export its most advanced machines to China as they are considered "dual use" with potential military applications. Dutch Trade Minister Liesje Schreinemacher last month said the Netherlands was in talks with the U.S. government about new export restrictions on semiconductor equipment sales to China. According to Bloomberg, an agreement could come as soon as next month, adding that it was unclear what the new restrictions would mean for ASML's sales to China.

Read the full article here.

IMPROVED EXPORT CONTROLS ENFORCEMENT TECHNOLOGY NEEDED FOR U.S. NATIONAL SECURITY

Gregory C. Allen, Emily Benson, William Alan Reinsch | Center for Strategic and International Studies | December 5, 2022

As technology has become increasingly central to strategic competition with Russia and China, export controls have moved to the forefront of U.S. foreign policy on technology issues. Most notably, restricting Russia's access to advanced technology through export controls is a key part of the U.S. response to Russia's invasion of Ukraine, as U.S. government officials have repeatedly stated.
Unfortunately, nearly all the debate is focused on whether and when to apply export controls, not how to ensure that export controls are effectively administered and enforced once applied.
The Bureau of Industry and Security (BIS) at the Department of Commerce oversees most export controls. Unfortunately, BIS is increasingly challenged by worldwide smuggling and export control evasion networks, especially those that are supported by Russia and China.

Read the full article here.

CHINA'S BRUTE FORCE ECONOMICS: WAKING UP FROM THE DREAM OF A LEVEL PLAYING FIELD

Liza Tobin | Texas National Security Review | Winter 2022/2023

In 2017, China's chief justice, Zhou Qiang, told legal officials in Beijing to resist "erroneous" ideas from the West like "constitutional democracy," "separation of powers," and "independence of the judiciary." His statements shocked some Western observers who had watched in cautious optimism as Zhou, a well-educated jurist with a reputation as a reformer, spearheaded efforts to make China's courts more professional. Behind Zhou's words was a hard truth: Reforms could only go so far before they collided with the reality that, in the People's Republic of China, the judiciary is subordinate to the Chinese Communist Party. This dynamic matters beyond China's borders. Cooperative trading relations require a common set of rules or expectations that ensure that economic competition occurs on a level playing field. Beijing's rejection of the rule of law as a fundamental operating principle means that the normative commercial structures upon which modern trade depends are at the mercy of a powerful and ideologically motivated political party.

Read the full article here.

SAFEGUARDING OUR FUTURE: PROTECTING PERSONAL HEALTH DATA FROM FOREIGN EXPLOITATION

The National Counterintelligence and Security Center | January 31, 2022

Foreign companies and some U.S. businesses with facilities abroad have been partnering or contracting with U.S. organizations to provide diagnostic tests and services that in some cases collect specimens, DNA, fitness / lifestyle information, or other personal health data from patients or consumers in the United States. Some of these companies may be subject to foreign laws that can compel them to share such data with foreign governments, including governments that exploit personal health data for their own ends and without regard to individual privacy. For example, several Chinese companies have partnered or contracted with U.S. organizations and are accredited, certified, or licensed to perform genetic testing or whole-genome sequencing on patients in the U.S. healthcare system, potentially giving them direct access to the genetic data of patients in the United States.[1] Chinese companies are compelled to share data with the government of the People's Republic of China,[2] which has used genetic data for state surveillance and repression of its ethnic and religious minorities,[3,4] as well as for military research and applications.[5]

Read the full article here.