RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE

THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary

November 16, 2023

US WON'T LOSE ITS AI LEAD TO CHINA ANYTIME SOON, INFLECTION AI CEO SAYS

Jackie Davalos and Nate Lanxon | Bloomberg | November 9, 2023

China's tech sector is racing to gain ground on developing artificial intelligence technology, but Google DeepMind co-founder Mustafa Suleyman predicts the US will still be in the lead 10 years from now. "I'm pretty sure of that. The fundamentals in the US innovation ecosystem are unquestionably the best in the world," said Suleyman, whose latest venture is Inflection AI, a startup valued at $4 billion. "Without doubt, Silicon Valley is leading the pack, and I think we'll continue to. I think we worry too much that we're going to sort of be dislodged from our podium position." Suleyman made the remarks during an interview for the latest episode of the Bloomberg Originals series AI IRL, available to stream now.
US officials are particularly concerned about China's ability to leverage AI for military purposes. In August, the Biden administration imposed restrictions on US investments in Chinese semiconductor, quantum computing and AI firms, citing national security concerns. Last month, it announced additional measures to curb China's access to advanced semiconductors capable of training AI algorithms.

Read the full article here.

DOD ANNUAL REPORT DETAILS CHINA'S GROWING CYBER CAPABILITIES

Anastasia Obis | GovCIO Media & Research | November 9, 2023

A recently released report on the People's Republic of China lays out an array of military and security developments, drawing attention to the increasing pressure campaign against Taiwan and the continued advancement of the country's cyber capabilities. The annual unclassified report to Congress details the current and probable future course of the People's Liberation Army, Chinese military and security strategy and organizations supporting military goals and developments for the next 20 years. As Beijing is growing its military arsenal, it is also expanding and investing in its cyber capabilities as it moves toward a "highly informatized force capable of dominating all networks and expanding the country's security and development interests." "The PRC has publicly identified cyberspace as a critical domain for national security and declared its intent to expedite the development of its cyber forces," the report states.

Read the full article here.

SIX PRINCIPLES FOR A MORE DYNAMIC AND EFFECTIVE UK–CHINA STRATEGY

Andrew Cainey | Royal United Services Institute (RUSI) | November 8, 2023

China poses an 'epoch-defining and systemic challenge with implications for almost every area of government policy and the everyday lives of British people', according to the UK's March 2023 Integrated Review Refresh. While stopping short of labelling China a 'threat', this is a marked shift from the 'golden era' of UK–China relations heralded during Xi Jinping's 2015 visit to the UK. Such a shift in assessment requires a commensurate response. This Policy Brief reviews the government's response to China to date and examines criticisms of its approach, including calls to publish an 'unclassified version of its China Strategy'. Rather than detail specific policy recommendations or argue in broad-brush terms for a more hawkish or dovish stance, the brief proposes six principles for a more dynamic and broadly based – and so more effective – China strategy.

Read the full article here.

HOUSE COMMITTEE ADVANCES BILL TO TIGHTEN COLLEGES' FOREIGN GIFT REPORTING MANDATES

Jeremy Bauer-Wolf | Higher ED Dive | November 8, 2023

- The House's Republican-led education committee advanced a bill Wednesday that would dramatically widen the scope of foreign gifts and contracts that colleges would need to report to the federal government.
- During a meeting of the Committee on Education and the Workforce, GOP lawmakers accused colleges of failing to disclose the breadth of their foreign donations. Under Section 117 of the Higher Education Act, they must report to the U.S. Department of Education any totaling $250,000 or more in a year.
- Republicans' legislative proposal would drop that threshold to $50,000 or more. Committee Democrats condemned the plan as xenophobic and onerous to the colleges and Education Department, the latter of which wouldn't receive any new funding to help track this data.

Read the full article here.

US UNIVERSITIES INCLUDING CORNELL, HARVARD AND MIT RAKED IN $13B IN 'UNDOCUMENTED CONTRIBUTIONS' FROM FOREIGN DONORS: REPORT

David Propper | New York Post | November 8, 2023

Over 200 US universities including elite institutions Carnegie Mellon, Cornell, Harvard and Massachusetts Institute of Technology have been accused of raking in $13 billion in "undocumented contributions from foreign governments," according to a new report. A sizable portion of the funds were said to be donated from authoritarian regimes around the globe including Qatar, Saudi Arabia, China and the UAE, the report from the Network Contagion Research Institute (NCRI) claimed. The huge windfall of cited money was not recorded with the US Department of Education between 2014 and 2019, the NCRI said. Carnegie Mellon University received the most from foreign entities in that time span at $1.47 billion while Cornell University scooped up $1.29 billion, Harvard University notched $894 million and MIT collected $859 million, according to the report.

Read the full article here.

EUROPE AND THE US WON'T WIN THE AI RACE BY DEPRIVING THEMSELVES OF TALENT

Anu Bradford | Financial Times | November 6, 2023

The contest over technological supremacy in the age of artificial intelligence is intensifying as tech companies and governments race to seize opportunities presented by the AI revolution. The outcome of this contest depends on many variables, but often overlooked is the fact that no country will win the AI race without cultivating the human talent that is central to innovations in the field. The US today retains an edge over China across several metrics in the fight for talent in the technology. It leads in foundational research, being home to 13 out of 15 leading AI research institutions. The US also produces the most AI unicorns — start-up businesses valued at more than $1bn. At the same time, China is investing heavily in developing AI, and already leads in related patent applications and journal citations globally.

Read the full article here.

UNITED STATES AND INDIA ARE BECOMING SCIENCE PARTNERS OF CHOICE

Natasha Gilbert | Nature | November 8, 2023

Achyuta Adhvaryu, an economics and public-policy researcher, moved across the United States from Michigan to San Diego this year, to launch the 21st Century India Center at the University of California (UC), San Diego. The centre aims to foster new connections between researchers at the university and academics at top institutions in India, an often-difficult task, says Adhvaryu, given India's sprawling higher-education system comprising roughly 50,000 academic institutions. By funding trips and organizing meetings, staff at the centre act as intermediaries, helping to facilitate relationships that might not have formed organically. An ocean scientist at UC San Diego's Scripps Institution of Oceanography, for example, has engaged the centre to connect them with researchers in India to work on a project about sea-level rise in the Indian Ocean.

Read the full article here.

THE SECURITY CHALLENGES OF EMERGING TECHNOLOGIES: COMMONS-BASED OPTIONS FOR CANADA

Robin Collins | Centre for International Policy Studies | November 8, 2023

In a recent issue of Foreign Affairs, Bremmer and Suleyman offer a very sober and disturbing evaluation ("The AI Power Paradox") of the likely speed that new technologies will take over and come to dominate. This is because artificial intelligence will outpace our regulatory systems, both national and international, simply because of the accelerative nature of AI, the clumsiness of international diplomacy and the limits of international verification and enforcement regimes. They suggest we urgently focus on institution-building considerations:

- Establish a global scientific body (as was done for climate with the IPCC) to objectively advise governments and international bodies.
- Manage tensions between the two main state players, the USA and China, using verification and monitoring approaches. Because the AI problem, which is mostly open-sourced, is highly decentralized they suggest establishing a Geotechnical Stability Board, supported by national regulatory and international standard setting (ISO) bodies.

Read the full article here.

A NEW ERA OF RESEARCH SECURITY

Brian Owens | University Affairs | June 14, 2023

Canada is home to a great deal of world-class research, but the federal government and its security services are raising the alarm that the country's combination of advanced technology, human talent and democratic society has made it an attractive target for foreign spies and their agents. "Espionage and foreign interference activities pose threats to the integrity of Canada's research enterprise, as well as our country's national security," a spokesperson for Innovation, Science and Economic Development Canada (ISED) said in a statement to University Affairs. New guidelines on how to protect research, and rules governing foreign collaborations, have proliferated over the past few years to deal with these threats. Many researchers, however, worry that the heightened focus on security and a lack of clarity around what is considered acceptable could have a chilling effect on international collaborations. Security threats come from many different countries that could be considered enemies of, or at least strategic competitors with Canada, including Iran, Russia and North Korea.

Read the full article here.

THE CYBER-RESILIENT CEO

Paolo Dal Cin, Valerie Abend, Rachel Barton and Yusof Seedat | Accenture

CEOs are fully aware of the threats to their business from cyberattacks. Yet, our research shows most lack confidence in their organization's ability to avert or minimize such attacks. They learn how to be cyber resilient only after their organization experiences a breach. This reactionary way of treating cybersecurity results in greater risk of attacks and higher costs to remediate them. Our research finds that there is a better way for some. In this practical guide, we explore how CEOs are best placed to set in motion five actions that minimize risk and put cyber resilience at the heart of their reinvention efforts. Is cybersecurity a business priority? It should be. It keeps business operations running smoothly, helps organization's optimize performance and secures customer and supplier relationships. CEOs that sideline cybersecurity expose their organizations to more risk. Powerful forces are multiplying digital vulnerabilities.

Read the full article here.

RESEARCH POINTS TO 5 WAYS TO IMPROVE CYBERSECURITY CULTURE

Jon Oltsik | TechTarget | November 8, 2023

Cybersecurity culture helps merge cybersecurity and the business. New research from TechTarget's Enterprise Strategy Group and the Information Systems Security Association (ISSA) provided multiple suggestions from cybersecurity professionals to help drive this change in five key areas. The European Union Agency for Network and Information Security defines cybersecurity culture as "the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest themselves in people's behavior with information technologies. Cybersecurity culture encompasses familiar topics, including cybersecurity awareness and information security frameworks, but is broader in both scope and application, being concerned with making information security considerations an integral part of an employee's job, habits and conduct, embedding them in their day-to-day actions. When organizations embrace this culture change, cybersecurity becomes everyone's job -- developers, line-of-business managers, knowledge workers, executives -- everyone.

Read the full article here.

ORGANIZATIONS UNDERESTIMATING THE SERIOUSNESS OF INSIDER THREATS

Help Net Security | April 8, 2022

Imperva releases data that shows organizations are failing to address the issue of insider threats during a time when the risk is at its greatest. New research, conducted by Forrester, found that 59% of incidents in EMEA organizations that negatively impacted sensitive data in the last 12 months was caused by insider threats, and yet 59% do not prioritize insider threats the way they prioritize external threats. Despite the fact that insider events occur more often than external ones, they receive lower levels of investment. This approach is at odds with today's threat landscape where the risk of malicious insiders has never been higher. The rapid shift to remote working means many employees are now outside the typical security controls that organizations employ, making it harder to detect and prevent insider threats. Further, the Great Resignation is creating an environment where there is a higher risk of employees stealing data.

Read the full article here.

10 BEST PRACTICES FOR PHYSICAL SECURITY IN THE WORKPLACE

Jackie Crowley | California Business Journal

When it comes to your business and organization, protecting your assets, people, and spaces should be your priority. That's where physical security steps in. It's like a shield that guards against different threats, from sneaky intruders to unexpected disasters. Why do companies often arrange physical security awareness training? Why does physical security in the workplace matter this much? You can think of it as a smart combination of technology and security strategies that help you to keep your company safe. The benefits of physical security awareness training aren't just about stopping burglars. It's your defense against vandalism, internal threats, cyber-attacks, accidents, and natural disasters.

Read the full article here.

PROTECTING CRITICAL AND EMERGING U.S. TECHNOLOGIES FROM FOREIGN THREATS

National Counterintelligence and Security Center | October 2021

Given the unique opportunities and challenges posed by emerging technologies, the National Counterintelligence and Security Center (NCSC) today announced it is prioritizing its industry outreach efforts in a select few U.S. technology sectors where the stakes are potentially greatest for U.S. economic and national security. These sectors produce technologies that may determine whether America remains the world's leading superpower or is eclipsed by strategic competitors in the next few years.

Read the full article here.

RESEARCH SECURITY TRAINING COURSES

Government of Canada

The Government of Canada has developed three publicly available courses to better equip Canadian researchers with the knowledge and resources to protect their research. To enroll in these courses, sign-up to ISED Learning platform using one of our secure access option. The GCKey option is available to any user, Canadian or international. Each course has a duration of approximately 30 to 40 minutes. Click the links below to enroll and access the courses.

View the full resource here.

TARGETING U.S. TECHNOLOGIES: A REPORT OF THREATS TO CLEARED INDUSTRY

Defense Counterintelligence and Security Agency | October 2021

With the mission of securing the trustworthiness of the Federal Government's workforce, the integrity of its Cleared Contractor support, and the uncompromised nature of its technologies, services, and supply chains, the Defense Counterintelligence and Security Agency continues to transform to meet the substantially increased threat associated with great power competition. For the first two decades of the 21st century, counterterrorism dominated the strategic landscape. Today, the Nation's most pressing threat comes from near peer adversaries that target our personnel and industrial base with the goal of competing with or surpassing the United States as the premier economic and military power.

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute