

Open Source Media Summary

March 14, 2024

NOBEL PRIZE SCIENTIST ON AI, DEMOCRACY AND CRITICAL THINKING

Karen MacGregor | University World News | March 8, 2024

Nobel prize-winning scientists and a world-leading AI researcher highlighted the dazzling potential of AI to support research, the contributions of science to democracy and the importance of critical thinking in the age of AI, at a Nobel Prize Dialogue held in Brussels this week. The three scientists are: Ben Feringa, a Dutch professor who received the 2016 Nobel Prize in Chemistry for his research on molecular machines; Sir Paul Nurse, British winner of the 2001 Nobel Prize in Physiology or Medicine for his work in genetics; and Demis Hassabis CBE, a British AI researcher and co-founder and CEO of Google DeepMind. "We're now at an incredible inflexion point," said Hassabis. "We're about to enter, maybe in the next 10 years, a new golden era of scientific discovery, helped by AI in many fields." His lab is working on a large language model that could work like a research assistant. The scientists joined two Nobel Peace Prize winners and three top democracy researchers at the first Nobel Prize Dialogue held in Brussels to discuss "Fact & Fiction: The future of democracy".

Read the full article here.

A PLAN TO DEVELOP OPEN SCIENCE'S GREEN SHOOTS INTO A THRIVING GARDEN

Greg Tananbaum, Chelle Gentemann, Kamran Naim, and Christopher Steven Marcum | *Issues in Science and Technology* | *Winter 2024*

Over the past several decades, the movement for open science, which promises a more inclusive, efficient, and trustworthy way of conducting and disseminating scientific research, has grown. Driven by the belief that openly sharing knowledge in all its forms—papers, data, software, methods, and more—can help address a raft of societal quandaries (including, though not limited to, systemic inequity and public mistrust in science), the adoption of open science principles has become increasingly mainstream. In the last five years, the White House Office of Science and Technology Policy; the governments of Ireland, Colombia, Spain, France, and the province of Quebec; higher education coalitions in the United States, Africa, South America, the United Kingdom, and Europe; professional societies and associations; and philanthropic funders have all taken steps toward strengthening policies for and reducing barriers to open and the Group of 20 have doubled down on their governments' commitments to invest in open, equitable, and secure strategies for research and development throughout the world.

OPTION FOR STRENGTHENING ALL-SOURCE INTELLIGENCE: SUBSTANTIVE CHANGE IS WITHIN REACH

Cortney Weinbaum, Bradley M. Knopp, Soo Kim, and Yuliya Shokh | Rand | February 28, 2022

Foreign attacks against the United States occur frequently, but the American people, U.S. policymakers, and even some intelligence analysts have become inured to the rising temperature of these national security threats. Although changes have occurred in the structure and organization of intelligence agencies, the intelligence community (IC) continues to face long-standing challenges related to collaboration, the use of open sources, analytic tradecraft, and the risk of politicization. The current environment demands prompt consideration of changes to intelligence structures and authorities that would enable intelligence analysts to become aware of foreign interference and disinformation campaigns sooner; ensure the dissemination of unclassified intelligence assessments to everyone who needs access to them, including private sector organizations; and protect against politicization. This exploratory study sought to address these needs by proposing Big Ideas—game-changing ideas that, while bold and audacious, are also implementable without requiring major intelligence reform.

Read the full article here.

AUSTRALIA FACING ITS HIGHEST-EVER THREAT FROM ESPIONAGE AND FOREIGN INTERFERENCE

Alexander Martin | The Record | February 28, 2024

More Australians are "being targeted for espionage and foreign interference than ever before," the head of the country's domestic security agency has warned. "Australians need to know that the threat is real. The threat is now. And the threat is deeper and broader than you might think," said Mike Burgess, delivering the agency's annual threat assessment on Wednesday evening. The director general of the Australian Security Intelligence Organisation (ASIO) said there was a "a particular team in a particular foreign intelligence service with a particular focus on Australia – we are its priority target." Although he did not name the nation state or provide any details about their tactics, he called the threat group "the A-team." The name wasn't intended to be a compliment, said Burgess, warning that several years ago the A-team "successfully cultivated and recruited a former Australian politician. This politician sold out their country, party and former colleagues to advance the interests of the foreign regime."

Read the full article here.

ACADEMIC FREEDOM A TOP CONCERN AS NEW SECURITY LAW LOOMS

Yojana Sharma | University World News | March 8, 2024

A new security law for Hong Kong, which is expected to have a chilling effect on academic and other freedoms, is being rushed through the city's legislature under an accelerated process after less than a month of public consultations. The so-called Article 23 security law under Hong Kong's own mini-constitution, the Basic Law, will sit alongside the National Security Law (NSL) imposed by Beijing in 2020. The law will introduce or revamp five new types of offences: treason, insurrection, sabotage, external interference, as well as theft of state secrets and espionage. The draft, tabled in the legislature on Friday 8 March, extends sentences for some existing offences, and brings in life sentences for others such as insurrection. Some offences, including "seditious intention", will apply to Hong Kong people abroad, while espionage using remote devices and sabotage related to electronic devices, which "endanger national security", can apply to anyone outside Hong Kong.

EXPERTS CHALLENGE ASSUMPTION OF TOO MANY OVERSEAS STUDENTS

Nic Mitchell | University World News | March 6, 2024

A new paper from a group of experts, including three former universities ministers, challenges suggestions that the United Kingdom has too many international students and warns that the government is using outof-date data to predict the number of overseas students expected to come to the UK for their higher education. The report, *Evidence versus Emotion: The facts about international student recruitment and what they mean*, was published on 5 March 2024 by the International Higher Education Commission (IHEC), which describes itself as "an evidence-led, apolitical forum helping to rebuild a consensus on the role of international higher education in civic society". It claims the UK government was rattled by the recent rapid growth in overseas students, particularly masters students during and just after the COVID pandemic when rival study abroad destinations were closed to foreigners – and that the UK's knee-jerk reactions, including stopping overseas taught postgraduate students bringing family members from this January and hikes to visa charges and the health service surcharge, are unwarranted.

Read the full article here.

KNOWLEDGE SECURITY AT STAKE

Leo Eigner | Center for Security Studies | March 6, 2024

A free, open, and international research and education environment is essential to scientific progress. At the same time, geopolitical tensions pose new challenges to the science, technology, and innovation sector. In many Western countries, approaches to knowledge security are being developed to protect core scientific values and preserve national interests. Research-performing organizations, such as universities and private companies, are at the forefront of scientific and technological breakthroughs and are therefore the fulcrum of geopolitical competition. The global science, technology, and innovation (STI) sector relies on international mobility and cooperation, which has benefited scientific and economic actors around the world. In the last decade, however, evidence has come to light that authoritarian governments, in China, Russia, Iran, and elsewhere, are exploiting the openness of the STI sector to modernize their militaries, strengthen their governance and surveillance systems, and spread propaganda abroad.

Read the full article here.

TRUMP VERSUS BIDEN: WHAT THE REMATCH COULD MEAN FOR THREE KEY SCIENCE ISSUES

Jeff Tollefson, Natasha Gilbert, Max Kozlov and Mariana Lenharo | Nature | March 6, 2024

Voters in 15 US states and one territory weighed in at the polls on 5 March, or 'Super Tuesday', and the results lock in a rematch between Republican Donald Trump and the incumbent, Democrat Joe Biden, in November's election for the next US president. The outcome could have massive implications for the environment, public health and international collaborations between scientists — as well as, some fear, US democracy itself. rump soundly beat his lone remaining challenger for the Republican nomination, Nikki Haley, a former US ambassador to the United Nations, who dropped out of the race on 6 March. The former president prevailed despite facing 91 criminal charges alleging interference with the 2020 presidential election, economic fraud and mishandling of classified materials. The result of this year's election could hinge on the outcome of those cases, as well as on potential long-shot presidential challenges from candidates labelling themselves as independents.

TECH, NATIONAL SECURITY, AND CHINA: Q&A WITH JASON MATHENY

Rand | March 8, 2024

Jason Matheny is one of the nation's leading experts on the interplay between technology and national security. In the Biden White House, he held three positions simultaneously: deputy assistant to the president for national security, National Security Council coordinator for technology, and deputy director of the Office of Science and Technology. He was the go-to guy in making sure that the administration understood how advances in technology affected national security, particularly when it comes to China. Matheny played a significant role in devising ways to try to keep the United States ahead of China in developing advanced semiconductors and artificial intelligence. After leaving the administration in 2022, he became CEO of RAND, the national security think tank. This interview is part of Rules of Engagement, a series by Bob Davis, who covered the U.S.-China relationship at The Wall Street Journal starting in the 1990s. In these interviews, Davis asks current and former U.S. officials and policymakers what went right, what went wrong, and what comes next.

Read the full article <u>here</u>.

WHY THE US BORDER REMAINS 'A PLACE OF TERROR' FOR CHINESE RESEARCHERS

Virginia Gewin | Nature | February 26, 2024

When an engineer of Chinese descent, who wishes to remain anonymous, took a flight back to his US university from a conference in Canada in September last year, he got a surprise at a stopover in Chicago, Illinois. The captain asked everyone to show their passports to border agents at the gate. The engineer, who has a Chinese passport and a green card to live and work permanently in the United States, estimates that he was detained for 90 minutes, and was asked to share his phone and laptop passwords or surrender his devices. He recalls being asked about his research, collaborations and recent publications with Chinese colleagues, and whether any of technologies they worked on were being transferred anywhere else. The unsettling experience prompted him to pull his name from joint publications with his collaborators in China. "I was considering changing my passport to become a US citizen before this incident, but now I'm just not sure," he adds. "They are treating us like spies."

Read the full article here.

CHINA'S NEW AI 'SUPERMIND' DEEPENS CHALLENGE TO U.S.

Didi Kirsten Tatlow | Newsweek | February 29, 2024

China is building a vast, AI-based intelligence platform dubbed "Supermind" to track millions of scientists and researchers around the world so it can hoover up breakthrough technologies for industry and the military, according to a person with close knowledge of the project and public sources reviewed by *Newsweek*. The state-funded platform, which says it uses sophisticated artificial intelligence systems to help find talent for China, is under construction in a new "information and intelligence" center that began work last year in the southern technology hub of Shenzhen. The city is home to global tech brands such as Huawei, ZTE and Tencent— some of which have been sanctioned by the U.S. government on national security and human rights grounds. The effort, revealed by *Newsweek*, has been called "Supermind" by the state-controlled Shenzhen Special Zone Daily and the AMiner university fund linked to Tsinghua University that offers grants for it. With \$280 million invested mostly by the Shenzhen government, according to the person with close knowledge of the project, it represents a step in China's efforts to win a global technology competition with the United States.

WHY TIKTOK IS A THREAT TO DEMOCRACY

Aynne Kokas | Journal of Democracy | October 2022

Since launching in 2016, the video-sharing app TikTok has become one of the world's most popular socialmedia platforms. Owned by the Chinese tech firm ByteDance, TikTok surpassed one-billion active global users in 2021. But as those users post and watch short videos, behind the scenes TikTok is meticulously collecting data on them, tracking their preferences and online activities. The rapid global expansion of Chinese tech firms such as ByteDance has created a regulatory conundrum for countries worldwide. From Australia and Japan to India and Pakistan to the United States, governments have been grappling with the expanding scope of China's digital regulations, which have set the stage for Beijing's global collection of data. As data traverses borders without explicit consent, the privacy of individuals, organizations, and even government bodies is at risk, posing a potential threat to national security.

Read the full article here.

US, CHINA IN A TECH-TRACKING SUPERMIND COMPETITION

Gabriel Honrada | Asian Times | March 5, 2024

China is developing an AI-based intelligence platform called "Supermind" to track millions of scientists and researchers worldwide, aiming to hoover up breakthrough technologies for industry and the military. The state-funded platform uses sophisticated AI systems to help find talent for China and is under construction in a new "information and intelligence" center in Shenzhen, home to big tech firms like Huawei, ZTE and Tencent, Newsweek reported. The project, fueled by a US\$280 million investment mainly by the Shenzhen government, represents a significant AI-empowered step in China's bid to win a global technology competition with the US. The Supermind will offer users 300 million global science and technology research papers and 120 million patents and have the ability to locate 130 million international scholars or "human talents" to scrutinize their work.

Read the full article here.

HOW AMERICA'S CHIPS ACT HURTS TAIWAN

Chang-Tai Hsieh and Chintay Shih | Project Syndicate | February 26, 2024

The concentration of advanced semiconductor manufacturing in Taiwan has raised fears in the United States about the vulnerability of this supply chain should China blockade or invade the island. The US CHIPS and Science Act seeks to address that vulnerability with \$52 billion in subsidies to encourage semiconductor manufacturers to relocate to America. But the legislation, as designed, will fall short of its objective; it may even weaken Taiwan's most important industry, further threatening the island's security. Today's semiconductor industry is dominated by specialized companies located around the world.

Read the full article here.



The Research and Innovation Security and Competitiveness Institute



CYBERSECURITY GUIDANCE: CHINESE-MANUFACTURED UAS

Cybersecurity and Infrastructure Security Agency | January 17, 2024

Chinese-manufactured unmanned aircraft systems (UAS), more commonly referred to as drones, continue to pose a significant risk to critical infrastructure and U.S. national security. While any UAS could have vulnerabilities that enable data theft or facilitate network compromises, the People's Republic of China (PRC) has enacted laws that provide the government with expanded legal grounds for accessing and controlling data held by firms in China. The use of Chinese-manufactured UAS requires careful consideration and potential mitigation to reduce risk to networks and sensitive information. The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) encourage U.S. critical infrastructure owners and operators to procure UAS that follow secure-by design principles, including those manufactured by U.S. companies. CISA and FBI further recommend following principles and implementing cybersecurity recommendations listed in this guidance to any organization procuring and operating UAS.

View the full resource here.

ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY

Office of the Director of National Intelligence | February 5, 2024

This annual report of worldwide threats to the national security of the United States responds to Section 617 of the FY21 Intelligence Authorization Act (Pub. L. No. 116-260). This report reflects the collective insights of the Intelligence Community (IC), which is committed every day to providing the nuanced, independent, and unvarnished intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world. This assessment focuses on the most direct, serious threats to the United States primarily during the next year. The order of the topics presented in this assessment does not necessarily indicate their relative importance or the magnitude of the threats in the view of the IC. All require a robust intelligence response, including those where a near-term focus may help head off greater threats in the future. Information available as of 22 January was used in the preparation of this assessment

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute