RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE
THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary
July 11, 2024

MULTIPLE NATIONS ENACT MYSTERIOUS EXPORT CONTROLS ON QUANTUM COMPUTERS

Matthew Sparkes | NewScientist | July 3, 2024

Secret international discussions have resulted in governments across the world imposing identical export controls on quantum computers, while refusing to disclose the scientific rationale behind the regulations. Although quantum computers theoretically have the potential to threaten national security by breaking encryption techniques, even the most advanced quantum computers currently in public existence are too small and too error-prone to achieve this, rendering the bans seemingly pointless. The UK is one of the countries that has prohibited the export of quantum computers with 34 or more quantum bits, or qubits, and error rates below a certain threshold. The intention seems to be to restrict machines of a certain capability, but the UK government hasn't explicitly said this. A *New Scientist* freedom of information request for a rationale behind these numbers was turned down on the grounds of national security. France has also introduced export controls with the same specifications on qubit numbers and error rates, as has Spain and the Netherlands. Identical limits across European states might point to a European Union regulation, but that isn't the case.

Read the full article here.

MANUFACTURING DECEIT: HOW GENERATIVE AI SUPERCHARGES INFORMATION MANIPULATION

Amaris Rancy | National Endowment For Democracy | June 18, 2024

Authoritarian actors have long worked to undermine democracy at a global scale by manipulating the information space, but the recent emergence of faster, more expansive, and potentially more potent "generative AI" technologies is creating new risks. With more than fifty national elections around the globe taking place in 2024, the stakes this year are particularly high. While it may still be too early to assess whether this new technology is creating *decisive* advantages for authoritarian powers, it is clear that they are experimenting and incorporating these tools into their strategies to undermine democracy. That said, beyond specific manipulative information campaigns, the deeper impact of this new technology may be felt beyond the election context, in citizens' loss of trust in online content, or in democracy itself. Earlier models of artificial intelligence excel in the recognition and analysis of patterns in large-scale collections of text, audio, or visual data. Generative models of artificial intelligence surpass the capabilities of these earlier models in significant ways. They extrapolate from patterns to create new content. Further, generative models operate in response to simple, natural-language text prompts, lowering the bar for their use and setting the stage for an even more complex and vexing information landscape.

Read the full article here.

DIFFERENT MAKES US STRONGER: AMERICAN DIVERSITY IS A NATIONAL SECURITY ASSET

Jaret Riddick | FEDSCOOP | July 3, 2024

There are many challenges facing the United States today that threaten the country's global leadership and economic power. One of the most significant strategic challenges can be summed up as the Great Power Competition, where Russia represents an acute threat, and China, the premier pacing threat. Amidst these real-world challenges, the United States continues to have a special tool critical to its national security, and indeed, global leadership - the diversity of its people. The urgency that current threats pose requires U.S. policymakers to resist being drawn into self-defeating divisive politics. Instead, American diversity should be valued not only as an inherent good, but as a strategic asset. The Great Power Competition is shaping up to be a race for technological dominance, and talent will be key to winning this race. America's diverse untapped talent from populations typically underrepresented in technical fields presents a valuable asset that should not go unnoticed.

Read the full article here.

COMMENTARY: HOW THE INTELLIGENCE COMMUNITY HAS HELD BACK OPEN-SOURCE INTELLIGENCE, AND HOW IT NEEDS TO CHANGE

Chris Rasmussen | Center for the Study of Intelligence | June 2024

Plans and strategies for improving open-source intelligence (OSINT) operations in the Intelligence Community often suffered from framing challenges. Many proposals for the way forward framed OSINT primarily as a collection challenge, which reduced OSINT to a collection supplement to classified analysis. This collection framing did not adequately help OSINT professionalize as a full-fledged analytic discipline. Moreover, it perpetuated the thinking that OSINT requires more "integration" into classified operations to be successful. Integration is not the main problem to solve when it comes to improving OSINT operations. Overuse of mission-integration jargon has hampered the professionalization of OSINT. In fact, in my view more OSINT silos-clusters of tightly connected business functions—are critically necessary to improve OSINT operations in the IC. All businesses and endeavors, public or private, for profit, or non-profit, or mission driven, form specialized and shared vocabularies around their execution of tasks and labor. Jargon helps specialized teams communicate and coordinate.

Read the full article here.

SPY AGENCY ISSUES WARNING TO BILLIONS OF SMARTPHONE USERS TO AVOID BEING SPIED ON

Anthony Cuthbertson | The Independent | June 4, 2024

The US National Security Agency has issued advice to smartphone owners to prevent their devices from being hacked and their personal details and money stolen. The government agency's Mobile Device Best Practices report is aimed at the billions of people around the world who use either an Android or an iOS smartphone, who are all exposed to a variety of cyber risks like spear-phishing attacks and zero-click exploits. Smartphone users can protect themselves against many of these hacks by simply turning their phones off and on again, according to the NSA's guidance. "Threats to mobile devices are more prevalent and increasing in scope and complexity," the US surveillance agency wrote in its guide. "Users of mobile devices desire to take full advantage of the features available on those devices, but many of the features provide convenience and capability but sacrifice security." Among the standard advice of using strong passwords and using any biometric security features like face and fingerprint recognition, the NSA also offers other instructions that may be less familiar to average phone users.

Read the full article here.

A HACKER STOLE OPENAI SECRETS, RAISING FEARS THAT CHINA COULD, TOO

Cade Metz | New York Times | July 4, 2024

Early last year, a hacker gained access to the internal messaging systems of OpenAI, the maker of ChatGPT, and stole details about the design of the company's A.I. technologies. The hacker lifted details from discussions in an online forum where employees talked about OpenAI's latest technologies, according to two people familiar with the incident, but did not get into the systems where the company houses and builds its artificial intelligence. OpenAI executives revealed the incident to employees during an all-hands meeting at the company's San Francisco offices in April 2023 and informed its board of directors, according to the two people, who discussed sensitive information about the company on the condition of anonymity. But the executives decided not to share the news publicly because no information about customers or partners had been stolen, the two people said. The executives did not consider the incident a threat to national security because they believed the hacker was a private individual with no known ties to a foreign government. The company did not inform the F.B.I. or anyone else in law enforcement.

Read the full article here.

WASHINGTON'S SCRUTINY OF CHINESE AND CHINESE AMERICAN SCIENTISTS IS HURTING THEIR PRODUCTIVITY-AND GLOBAL SCIENTIFIC COOPERATION

Lionel Lim | Fortune | July 4, 2024

Trade and technology aren't the only areas hit by worsening U.S.-China tensions. Washington's worries about espionage and giving its rival a lead in strategic research is making science the newest victim of geopolitics. Even the 45-year-old U.S.-PRC Science and Technology Agreement, the first agreement between the two countries after relations were normalized, is on the ropes. The sinking relationship between the U.S. and China is hindering scientific cooperation, according to a new working paper from the National Bureau of Economic Research. The paper studies three measures: the mobility of STEM trainees between the U.S. and China, how often scientists in one country used works from another, and scientist productivity. According to the working paper, Chinese graduates were 16% less likely to attend a U.S.-based PHD program between 2016 and 2019. The paper also reports a steep decline in Chinese citations of U.S. science, though finds no decline in U.S. citations of Chinese research.

Read the full article here.

CHINA TO BOOST BASIC RESEARCH IN NATURAL RESOURCES ON ITS PATH TO TECH SELF-RELIANCE

William Zheng | South China Morning Post | July 3, 2024

The Chinese government has pledged to support a wide range of basic research related to natural resources to support its goal of turning the country into a science superpower. The objectives are among the Ministry of Natural Resources' new policy guidelines to strengthen fundamental research released by the ministry on its official social media accounts on Wednesday. Beijing's top leaders last month committed to building China into a major world science power by 2035, acknowledging that science and technology will be key drivers for the world's second-largest economy as it faces external and internal challenges. The pledge came as China and the US compete in several arenas, including geopolitics, trade and technology.

Read the full article here.

THE US MUST SECURE ITS SUPREMANCY AGAINST CHINA IN AI AND CLOUD COMPUTING

Klon Kitchen | The Hill | July 6, 2024

The race for dominance in cloud computing and artificial intelligence (AI) is heating up, and China is pulling ahead with aggressive tactics. If the U.S. doesn't step up now, we risk losing our technological edge and compromising national security. Cloud computing is arguably the backbone of today's AI renaissance, providing essential infrastructure for the training, processing and deploying of today's most advanced models leveraging the most sophisticated semiconductors available. With over 70 percent of companies adopting AI platforms and 85 percent developing AI applications in the cloud, the U.S. government faces an urgent task: ensuring that high-performing chips are manufactured and deployed by trusted entities and that AI is developed in secure, reliable clouds. American cloud providers are crucial for AI innovation, yet they face unfair competition from Chinese firms backed by state subsidies and predatory pricing.

Read the full article here.

SILICON VALLEY STEPS UP SCREENING ON CHINESE EMPLOYEES TO COUNTER ESPIONATE

Stella Hsu | Voice of American (VOA) | July 4, 2024

Leading U.S. technology companies reportedly have increased security screening of employees and job applicants, which experts say is necessary to counter the cyber espionage threat from China. While the enhanced screening is being applied to employees and applicants of all races, those with family or other ties to China are thought to be particularly vulnerable to pressure from the Beijing government. But at least one Chinese computer science graduate student at a U.S. university is hoping to make his ties to China an asset. Zheng, who does not want to reveal his first name for fear of retaliation from the Chinese government, says he recently changed his focus to cybersecurity in hopes of improving his job prospects in the United States. "The goal is a bit high, but I think I know more about China as a person born and raised in China. I hope to become a force with my own characteristics in cybersecurity and a role in fighting against Chinese cyber-attacks," said Zheng, who is seeking political asylum in the United States.

Read the full article here.

CHINESE FIRM SOUGTH TO USE UK UNIVERSITY LINKS TO ACCESS AI FOR POSSIBLE MILITARY USE

Hannah Devlin | The Guardian | June 16, 2024

A Chinese state-owned company sought to use a partnership with a leading British university in order to access AI technology for potential use in "smart military bases", the Guardian has learned. Emails show that China's Jiangsu Automation Research Institute (Jari) discussed deploying software developed by scientists at Imperial College London for military use. The company, which is the leading designer of China's drone warships, shared this objective with two Imperial employees before signing a £3m deal with the university in 2019. Ministers have spent the past year stepping up warnings about the potential security risk posed by academic collaborations with China, with MI5 telling vice-chancellors in April that hostile states are targeting sensitive research that can "deliver their authoritarian, military and commercial priorities". The former Conservative leader Iain Duncan Smith said: "Our universities are like lambs to the slaughter.

Read the full article here.

CHINA START SMARTPHONE INSPECTIONS TO BOOST ANTI-ESPIONAGE EFFORTS

Kyodo News | July 1, 2024

China implemented new regulations on Monday under its toughened counterespionage law, which enables authorities to inspect smartphones, personal computers and other electronic devices, raising fears among expatriates and foreign businesspeople about possible arbitrary enforcement. The new rules, which came into effect one year after the revised anti-espionage law expanded the definition of espionage activities, empower Chinese national security authorities to inspect data, including emails, pictures, and videos stored on electronic devices. Such inspections can be conducted without warrants in emergencies. If officers are unable to examine electronic devices on-site, they are authorized to have those items brought to designated places, according to the regulations. It remains unclear what qualifies as emergencies under the new rules. Foreign individuals and businesses are now expected to face increased surveillance by Chinese authorities as a result of these regulations.

Read the full article here.

FOREIGN PROFESSOR FIRED FROM CHINESE UNIVERSITY AFTER INTERVIEW WITH VOA

Voice of America (VOA) | July 2, 2024

Björn Alexander Düben, a German assistant professor at Jilin University's School of Public Diplomacy, was mysteriously dismissed and instructed to leave China after a nine-year tenure, following his participation in an interview with Voice of America (VOA). This dismissal highlights the severe restrictions on free speech imposed by the Chinese Communist Party (CCP). Düben's troubles began shortly after he commented on Chinese leader Xi Jinping's visit to Europe in an article published by VOA Mandarin on May 11. The next day, he received a WeChat message from the university's international secretary, which stated, "It is well known that colleges and universities must be responsible for any form of interviews with domestic and foreign media." This message hinted at the sensitive nature of his comments regarding the Chinese leadership. On May 15, Düben was informed that his classes for the day were suspended due to all classrooms being occupied.

Read the full article here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute

USEFUL RESOURCES

CHINA PRIMER: CHINA'S POLITICAL SYSTEM

Congressional Research Service | July 1, 2024

The People's Republic of China (PRC or China) is the only Communist Party-led state either among the five permanent members of the United Nations Security Council or among the members of the G-20 grouping of major economies. As Congress has intensified its focus on China in the context of U.S.-China strategic competition, Members have increasingly sought to legislate and conduct oversight on matters that require an understanding of the PRC political system. Select features of that system are introduced below. The PRC is both a nation state and a Leninist "party-state." The Communist Party of China (CPC), also known as the Chinese Communist Party (CCP), is China's dominant political institution.

View the full resource here.

SECURE AMERICA'S FUTURE IN QUANTUM: PROTECT YOUR RESEARCH

Office of the Director of National Intelligence

THREAT: Foreign adversaries are targeting quantum industry and academic personnel, facilities, networks, research, and technology to gain an economic and military advantage.

View the full resource here.

EXPLORING MEMORY SAFETY IN CRITICAL OPEN SOURCE PROJECTS

America's Cyber Defense Agency | June 26, 2024

In December 2023, the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and international cybersecurity authorities from Australia, Canada, New Zealand, and the United Kingdom, published The Case for Memory Safe Roadmaps. This joint publication notes that memory safety vulnerabilities are among the most prevalent classes of software vulnerability and generate substantial costs for both software manufacturers and consumers related to patching, incident response, and other efforts. It further recommends software manufacturers create memory safe roadmaps, including plans to address memory safety in external dependencies, which commonly include open source software (OSS).

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute