ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

May 17, 2023

DOD RELEASES NATIONAL DEFENSE SCIENCE AND TECHNOLOGY STRATEGY

U.S. Department of Defense | May 9, 2023

The Department of Defense released the National Defense Science and Technology Strategy, or NDSTS, today. Guided by the National Defense Strategy, the NDSTS articulates the science and technology priorities, goals, and investments of the Department and makes recommendations on the future of the defense research and engineering enterprise. "To achieve the objectives of the NDS we must leverage critical emerging technologies," said Heidi Shyu, DoD Chief Technology Officer. "This Strategy helps us make carefully crafted decisions that bolster our comparative advantages rather than engaging in wasteful technology races. We will emphasize developing asymmetric capabilities that will help ensure our national security over the long term." The Strategy will execute along three lines of effort: Focus on the Joint Mission by investing in information systems and establishing processes for rigorous, threat informed analysis that will better enable the Department to make informed choices in its science and technology investments.

Read the full article here.

WHY CHINA HAS EDGE ON AI, WHAT ANCIENT EMPERORS TELL US ABOUT XI JINPING

Christy DeSmith | The Harvard Gazette | March 16, 2023

Dictatorships and authoritarian regimes tend to trail more democratic and inclusive nations in fostering cutting-edge, innovative technologies, such as robotics and clean energy. Artificial intelligence may prove an exception, at least in China, owing to dovetailing interests. Harvard Economics Professor David Yang spoke to the outsized success of China's AI sector at a recent dean's symposium on insights gleaned from the social sciences about the ascendant global power. As evidence, he cited a recent U.S. government ranking of companies producing the most accurate facial recognition technology. The top five were all Chinese companies. "Autocratic governments would like to be able to predict the whereabouts, thoughts, and behaviors of citizens," Yang said. "And AI is fundamentally a technology for prediction." This creates an alignment of purpose between AI technology and autocratic rulers, he argued. Because AI heavily depends on data, and autocratic regimes are known to collect vast troves of it, this advantages companies with Chinese government contracts, which can turn around and use state data to bolster commercial projects, he added.

Read the full article here.

PENTAGON CIO AND CDAO: DON'T PAUSE GENERATIVE AI DEVELOPMENT — ACCELERATE TOOLS TO DETECT THREATS

Brandi Vincent | DefenseScoop | May 3, 2023

Though they recognize and share legitimate concerns about emerging generative artificial intelligence capabilities recently unleashed in the wild being applied irresponsibly to cause harm, two senior Pentagon officials confirmed they are not part of the growing movement of experts calling to temporarily halt the technology's development so that humans can first learn more about it and its potential consequences. Large language models that can generate audio, software code, images, text, videos and other media — when people prompt them to do so — make up the wildly popular new tech subfield known as generative AI. ChatGPT, Bing AI and Bard mark some of the major brands. These AI-powered tools hold a lot of promise to assist workers and potentially disrupt the American job market. However, as the technology very rapidly evolves, some of its makers and other leading technologists are advocating for a moratorium that can allow for AI vendors and regulators to have some time to puzzle out ways to safeguard its use.

Read the full article here.

CREATING A STRATEGIC RESEARCH PARTNERSHIP WITH INDIA

Barbara R. Synder | Association of American Universities | May 8, 2023

AAU is proud to lead a task force to look at ways to expand critical research partnerships with India's leading universities. AAU has long advocated for – and the United States has benefited from – broad international collaboration in advancing scientific research and discovery. Top students and researchers from around the globe have come to the United States for decades to study and work; many choose to stay and contribute to our economy, our national security, and our culture after they complete their studies. At the same time, American scientists have gone to other countries to conduct groundbreaking research. As new nations begin to emerge as potential scientific powerhouses, it behooves us to find mutually beneficial ways to partner – and that is why AAU is proud to lead an effort to deepen research ties with India. We recently announced the members and co-chairs for the new AAU-led Task Force on Expanding United States-India University Partnerships.

Read the full article here.

HOW TO AVOID IMMIGRATION-RELATED DISCRIMINATION WHEN COMPLYING WITH U.S. EXPORT CONTROL LAWS

U.S. Department of Justice | Civil Rights Division | April 2023

The purpose of this fact sheet is to help employers avoid discrimination under the Immigration and Nationality Act (INA) when complying with export control laws. Civil Rights Division investigations have found that employers violated the INA based on a misunderstanding of export control laws. Under the INA, it is generally against the law for employers to: make hiring, firing, or recruiting decisions based on workers' citizenship, immigration status, or national origin, or treat workers differently based on these characteristics when verifying their permission to work, including during the Form I-9 and E-Verify processes. What are export control laws and regulations? U.S. export control laws and regulations include: The International Traffic in Arms Regulations (ITAR) and The Export Administration Regulations (EAR). These regulations restrict an employer's ability to export certain goods and software, technology, and technical data (referred to here as export-controlled items). Under these regulations, U.S. persons working for U.S. companies can access export-controlled items without authorization from the U.S. government.

Read the full article here.

HAINES: US MUST 'MOVE WITH URGENCY' TO PREPARE FOR EMERGING TECH THREATS LIKE GENERATIVE AI

Brandi Vincent | DefenseScoop | April 25, 2023

China, Russia, Iran and other nations are increasingly exploiting existing and emerging technologies — like surveillance biometrics and generative artificial intelligence — to advance authoritarianism, enable digital repression and undermine democratic governance globally, U.S. Director of National Intelligence Avril Haines warned on Monday. During an event hosted by the Carnegie Endowment for International Peace, she spotlighted those three nations' recent models and methods for deploying and exporting capabilities to facilitate dictatorial practices. New frameworks and "built-in" technology standards will be needed to promote stronger resilience against those growing threats, she suggested. "In my view, the intelligence community is a critical ally in the fight against authoritarianism and should contribute to the promotion of norms that help to protect against the primary tools of digital authoritarianism and repression, which are censorship, misinformation and disinformation, mass surveillance and invasive spyware used to suppress public debate," she said. Each year, the Office of the Director of National Intelligence (ODNI) conducts and releases a report on worldwide threats to U.S. national security. Haines confirmed the latest review, launched in March 2023, was the first annual threat assessment to devote an entire section to digital authoritarianism.

Read the full article here.

CHATGPT AND THE NEW AI ARE WREAKING HAVOC ON CYBERSECURITY IN EXCITING AND FRIGHTENING WAYS

Dan Patterson | ZDNET | May 7, 2023

Generative artificial intelligence is transforming cybersecurity, aiding both attackers and defenders. Cybercriminals are harnessing AI to launch sophisticated and novel attacks at large scale. And defenders are using the same technology to protect critical infrastructure, government organizations, and corporate networks, said Christopher Ahlberg, CEO of threat intelligence platform Recorded Future. Generative AI has helped bad actors innovate and develop new attack strategies, enabling them to stay one step ahead of cybersecurity defenses. AI helps cybercriminals automate attacks, scan attack surfaces, and generate content that resonates with various geographic regions and demographics, allowing them to target a broader range of potential victims across different countries. Cybercriminals adopted the technology to create convincing phishing emails. AI-generated text helps attackers produce highly personalized emails and text messages more likely to deceive targets. "I think you don't have to think very creatively to realize that, man, this can actually help [cybercriminals] be authors, which is a problem," Ahlberg said.

Read the full article here.

CANADA SET TO NAME FOREIGN LABS, UNIVERSITIES THAT POSE RISK TO NATIONAL SECURITY

Joanna Chiu | Toronto Star | May 8, 2023

Ottawa is in "advanced stages" of drafting a list of entities that pose a risk to national security, and top universities are prepared to avoid working with these entities despite what could be a loss of $100 million or more in annual research funding from foreign partners. The list will include foreign-state-connected universities, research institutes and laboratories that are believed to be at "higher risk" of engaging in theft, unwanted knowledge transfers and interference in research, according to government documents reviewed by the Star.

Read the full article here.

PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS

Ron Ross and Victoria Pillitteri | NIST | May 10, 2023

The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the Federal Government to successfully conduct its essential missions and functions. This publication provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations, when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency, and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry. The requirements apply to components of nonfederal systems that process, store, or transmit CUI *or* that provide protection for such components. The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

Read the full article here.

CANADIAN UNIVERSITIES AND RESEARCH SECURITY

Wesley Wark | Wesley Wark's National Security and Intelligence Newsletter | May 3, 2023

Canadian university administrations and their faculty engaged in research partnerships with overseas entities, especially those linked to China, are under increasing, and probably long overdue, pressure to scrutinize such partnerships for outcomes that could be harmful to Canadian national security. The harms can include intellectual property theft or loss, illicit exploitation of data sets, knowledge transfer of sensitive information, and the exportation of advanced and innovative technologies. The most worrisome beneficiaries include adversarial state militaries (weapons research and development) and their security agencies (surveillance technologies, advanced insider threats). Methods for penetrating university research rarely depend on traditional espionage; instead cover techniques, including the use of proxies—what CSIS calls "non-traditional intelligence collectors"—and clandestine or deceptive practices around research partnerships, are more common. The federal government is trying to set new rules of the road, alongside similar efforts by allies.

Read the full article here.

CHINA'S EXPANDED ESPIONAGE LAW ONLY HASTENS FOREIGN CAPITAL DRAIN

Nikkei Asia | May 3, 2023

China's expanded counterespionage law will take effect in July, enabling the authorities to crack down on a wide range of activities deemed related to "national security and interests." Not only will a broader definition of espionage impact the safety of foreign nationals working in China, but expanding the law will also stifle cross-border economic activity and cause more foreign capital to leave the country. The revised law, passed by the National People's Congress in late April, expanded the definition of espionage to include theft and transfer of documents, data, materials, or items related to national security and interests. Crucially, however, it is still unclear what exactly constitutes national security and interests -- the core part of the legislation. The revision maintains the vague wording "other espionage activities," which has been criticized as leaving room for a broad interpretation and arbitrary enforcement of the law.

Read the full article here.

THE FUTURE OF TECHNOLOGY: LESSONS FROM CHINA—AND THE US

Maya Wang, Frederike Kaltheuner, and Amanda Klasing | Bulletin of the Atomic Scientists | May 9, 2023

Not a day passes by without some alarming headlines about the Chinese government's use of technology, whether it is about Huawei building 5G infrastructure around the world, or about the European Union and the US banning TikTok from government phones. In the United States, public discourse on technology and China is often framed in simplistic, black-and-white terms as a battle between democracy and authoritarianism. According to this logic, a US victory in this technological race is not just self-interested—it is vital to protecting rights and freedoms everywhere. But unfortunately, reality is more complicated. In fact, we would argue that this framing is not just flawed and oversimplified, it is also dangerous for human rights everywhere.

Read the full article here.

UNIVERSITY OF WATERLOO ENDS RESEARCH PARTNERSHIPS WITH HUAWEI, AMID SECURITY CONCERNS OVER CHINA

Joanna Chiu | Toronto Star | May 3, 2023

One of Canada's top research universities will end all its research partnerships with Chinese telecommunications giant Huawei, the Star has learned. "We are disentangling ourselves from this company." Charmaine Dean, vice-president if research of research at the university of Waterloo, told the Star.

Read the full article here.