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

Open Source Media Summary

May 16, 2024

UNITED STATES GOVERNMENT POLICY FOR OVERSIGHT OF DUAL USE RESEARCH OF CONCERN AND PATHOGENS WITH ENHANCED PANDEMIC POTENTIAL

The White House | Executive Office of the President of the United States | May 6, 2024

The United States Government Policy for Oversight of Dual Use Research of Concern and Pathogens with Enhanced Pandemic Potential ("Policy") is a unified federal oversight framework for conducting and managing certain types of federally funded life sciences research on biological agents and toxins. This Policy addresses oversight of research on biological agents and toxins that, when enhanced, have the potential to pose risks to public health, agriculture, food security, economic security, or national security.[1] It supersedes the 2012 United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern (Federal DURC Policy),[2] the 2014 United States Government Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern (Institutional DURC Policy),[3] and the Recommended Policy Guidance for Departmental Development of Review Mechanisms for Potential Pandemic Pathogen Care and Oversight (P3CO Framework). [4] This Policy is issued by the Office of Science and Technology Policy (OSTP) in accordance with the directives established by the 2022 National Biodefense Strategy and Implementation Plan,[5] as directed by National Security Memorandum 15,[6] to complete an interagency review of efforts to strengthen responsible conduct for biological research.

Read the full article here.

ODNI RELEASES IC POLICY FRAMEWORK FOR COMMERCIALLY AVAILABLE INFORMATION

Office of the Director of National Intelligence | Press Release | May 8, 2024

The Office of the Director of National Intelligence (ODNI) today released the Intelligence Community (IC) Policy Framework for Commercially Available Information (CAI). Increasingly important to our work, CAI also poses novel issues related to privacy and civil liberties, and ODNI created this Policy Framework to govern the IC's access to, collection, and processing of CAI. "In keeping with my commitment to share as much as possible about the IC's activities, we are sharing this framework which provides effective governance for the IC's handling of CAI while also protecting Americans' privacy and civil liberties," said Director of National Intelligence Avril Haines.

Read the full article here.

WHY THE SECRECY AROUND SECURING AUSTRALIA'S QUANTUM RESEARCH IS SCARY

Brendan Walker-Munro | The Interpreter | May 7, 2024

For most people, quantum computers are the stuff of science fiction. Based on shooting microwave photons at "qubits", quantum computers are estimated to be far more powerful than any other computing system ever invented. So much so that cybersecurity experts are warning of an impending "Q Day", where a functioning quantum computer renders the encrypted systems we use for banking, telecommunications and the military all but obsolete. Foreign spies are already after bleeding-edge quantum secrets in the United States, so it doesn't seem a stretch to imagine the same thing occurring in Australia. But quantum computers aren't science fiction. Not only are they a key deliverable under Pillar 2 of AUKUS – the trilateral security partnership between Australia, the United Kingdom and the United States – they are being built right now. The Australian government has just announced an investment of nearly $1 billion to develop the first Australian quantum computer in Brisbane.

Read the full article here.

SURVEY OF CHINESE ESPIONAGE IN THE UNITED STATES SINCE 2000

Center for Strategic & International Studies

This updated survey is based on publicly available information and lists 224 reported instances of Chinese espionage directed at the United States since 2000. It does not include espionage against other countries, against U.S. firms or persons located in China, nor the many cases involving attempts to smuggle controlled items from the U.S. to China (usually munitions or controlled technologies) or the more than 1200 cases of intellectual property theft lawsuits brought by U.S. companies against Chinese entities in either the U.S. or China. The focus is on the illicit acquisition of information by Chinese intelligence officers or their agents and on the increasing number of Chinese covert influence operations. Chinese espionage is undertaken in pursuit of China's strategic objectives.

Read the full article here.

'TUNNELVISION' ATTACK LEAVES NEARLY ALL VPNS VULNERABLE TO SPYING

Dan Goodin | WIRED | May 10, 2024

Researchers have devised an attack against nearly all virtual private network applications that forces them to send and receive some or all traffic outside of the encrypted tunnel designed to protect it from snooping or tampering. TunnelVision, as the researchers have named their attack, largely negates the entire purpose and selling point of VPNs, which is to encapsulate incoming and outgoing Internet traffic in an encrypted tunnel and to cloak the user's IP address. The researchers believe it affects all VPN applications when they're connected to a hostile network and that there are no ways to prevent such attacks except when the user's VPN runs on Linux or Android. They also said their attack technique may have been possible since 2002 and may already have been discovered and used in the wild since then.

Read the full article here.

US COMMITTEE TARGETS GEORGIA TECH'S ALLEGED TIES TO CHINESE MILITARY LINKED RESEARCH

Michael Martina | Reuters | May 9, 2024

A U.S. congressional committee on China has asked leading research university Georgia Institute of Technology to detail its collaboration with a Chinese university facing U.S. government restrictions due to its alleged ties to the country's military. Georgia Tech partnered with China's northeastern Tianjin University on cutting edge technologies despite its documented ties to the People's Liberation Army (PLA), John Moolenaar, the new Republican chairman of the House of Representatives' select committee on China, wrote in a letter on Thursday to the U.S. school's president Angel Cabrera. But the Georgia Tech scientist who led the project defended the research, saying all the results were available to the public, that it had passed extensive legal reviews, and that only a small portion of the funding came from the Georgia Tech Research Institute (GTRI), which is heavily sponsored by the Pentagon. The letter noted that Tianjin University and numerous affiliates had been added in 2020 to the Commerce Department's export restrictions list for actions contrary to U.S. national security, including trade secret theft and research collaboration to advance China's military.

Read the full article here.

CHINA'S QUANTUM TECH 'CORE STRENGTH' TARGETED BY LATEST US TRADE BLACKLIST, CHINESE PHYSICISTS WARN

Dannie Peng | South China Morning Post | May 11, 2024

The latest US trade restrictions on China are "unprecedented" and will have a "far-reaching impact" on Chinese quantum research, physicists in the country have warned. This comes after the US Commerce Department's updated export control list released on Thursday named 22 of China's leading players in quantum research and industrialisation among the 37 Chinese "entities" targeted. The additions to the blacklist, officially known as the "Entity List", are designed to prevent US companies from selling materials and equipment to the targeted entities. This is the second time quantum-related research institutes and companies have been added to the trade blacklist, but the scope is much broader, according to Chinese scientists. "Almost all of China's core strength in quantum information research has been listed," said Yin Zhangqi, a physicist at the Beijing Institute of Technology, who described the impact as "huge".

Read the full article here.

UK GOVERNMENT 'PROFOUNDLY WORRIED' ABOUT RESEARCH SECURITY

Robin Bisson | Research Professional News | May 10, 2024

Angela McLean tells of approach by researcher in China after becoming science adviser to MOD. The UK's most senior scientific adviser has said the government is "profoundly worried" about research security, and that most academics are not aware of the scale of the problem. Angela McLean also said she had been approached by a mysterious researcher in China offering to work in her lab, soon after she was appointed chief scientific adviser to the UK Ministry of Defence.

Read the full article here.

U.S. ADDS 37 CHINA ENTITIES TO TRADE BLACKLIST OVER SECURITY CONCERNS

Kyodo News | May 10, 2024

The U.S. government on Thursday added 37 Chinese entities to its trade blacklist, citing national security concerns, with 11 of them accused of being connected with a suspected spy balloon that flew over sensitive areas of the United States last year. Companies, and research institutions and other entities on the list are restricted from doing business with U.S. firms and must gain Commerce Department approval before obtaining goods and technologies from them. Of the 37 entities, the department said 22 were put on the list for their links to China's efforts to improve quantum technology and for acquiring or seeking to acquire U.S.-origin items to boost the country's quantum capabilities. It said some of them are also associated with advancements in China's nuclear programs or have been involved in the export of controlled items to Russia amid its war against Ukraine.

Read the full article here.

NEW BANS ON HUAWEI: ANOTHER SHOT IN BIDEN'S ECONOMIC WAR ON CHINA

Peter Symonda | World Socialist Web Site | May 8, 2024

The US has fired another shot in the escalating economic war with China by imposing new bans limiting the sale of semiconductors to Huawei. The Financial Times (FT) revealed this week that the Biden administration had revoked export licences that allow Intel and Qualcomm to sell their chips to the hi-tech Chinese corporation. The US commerce department confirmed the new bans to the FT but provided no details nor the specific reasons. A spokesperson declared in the vaguest terms that the US makes such decisions to "protect our national security and foreign policy interests, taking into consideration a constantly changing threat environment and technological landscape." Washington's concerns about "national security" and claims of unfair economic practices obscure the more fundamental reason for efforts to cripple Huawei.

Read the full article here.

OMB OVERHAULS REGULATIONS FOR FEDERAL GRANTS AND COOPERATIVE AGREEMENTS

William Ferreira, Will Crawford, and Lauren Colantonio | Hogan Lovells (ENGAGE) | May 9, 2024

The U.S. Office of Management and Budget (OMB) has released its long-awaited "Guidance for Federal Financial Assistance" to revise the regulations previously known as the OMB Uniform Guidance. With Federal grant funding opportunities soaring into the hundreds of billions of dollars, the final rule is a significant development for recipients of Federal awards, including nonprofits, institutions of higher education, research institutions, hospitals, companies, and others that receive Federal financial assistance. The final rule takes effect October 1, 2024. Between 2012 and 2013, OMB worked with Federal agencies to revise and streamline grants guidance to develop the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance) located at 2 CFR part 200.

Read the full article here.

WHAT WENT WRONG WITH INTERNATIONAL EDUCATION IN THE UK?

Louise Nicol | University World News | May 10, 2024

Commentating on the state of international education in the United Kingdom since 2019 resembles something akin to a slow-motion car crash as post-study work visas, hailed as essential for the sustained growth of international student recruitment, have become the sector's de facto crutch in the absence of a strategy to support international graduates' transition to successful careers back in their home countries. The UK sector now waits anxiously for 14 May when the Migration Advisory Committee (MAC) reports to government, following an expedited review of the UK Graduate Route with the CEO of Universities UK, Vivienne Stern quoted as saying that there is "a very high risk of a manifesto from the Conservative Party that includes a commitment to removing the Graduate Route". The Labour Party is likely to follow suit, in a fight to win the 'Red Wall' (traditionally Labour-voting areas that swung to the Conservatives after Brexit).

Read the full article here.

FOREIGN INTERFERENCE COMMISSION RELEASES INITIAL REPORT

Michael Tansey | Foreign Interference Commission | May 3, 2024

After conducting months of investigation and hearing from more than 60 witnesses during 21 days of hearings, the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions has released its Initial Report, which focuses on foreign interference in the 2019 and 2021 federal elections. Commissioner Marie-Josée Hogue found that the Canadian electoral system itself is robust, but she did find evidence of foreign interference. "Acts of foreign interference did occur during the last two federal general elections, but they did not undermine the integrity of our electoral system," she said. "Our system remains sound. Voters were able to cast their ballots, their votes were duly registered and counted and there is nothing to suggest that there was any interference whatsoever in this regard. Nor did foreign interference have any impact on which party formed the government in the two most recent elections. Nonetheless, the acts of interference that occurred are a stain on our electoral process and impacted the process leading up to the actual vote."

Read the full article here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute

USEFUL RESOURCES

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

GitHub.com

The CISA Vulnrichment project is the public repository of CISA's enrichment of public CVE records through CISA's ADP (Authorized Data Publisher) container. In this phase of the project, CISA is assessing new and recent CVEs and adding key SSVC decision points. Once scored, some higher-risk CVEs will also receive enrichment of CWE, CVSS, and CPE data points, where possible. Producers and consumers of this CVE data should already be familiar with the current CVE Record Format and can access this data in the normal ways, including the GitHub API.

View the full resource here.

#STOPRANSOMWARE: BLACK BASTA

Joint Cybersecurity Advisory | Media News | May 10, 2024

This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources. The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Department of Health and Human Services (HHS), and Multi-State Information Sharing and Analysis Center (MS-ISAC) (hereafter referred to as the authoring organizations) are releasing this joint CSA to provide information on Black Basta, a ransomware variant whose actors have encrypted and stolen data from at least 12 out of 16 critical infrastructure sectors, including the Healthcare and Public Health (HPH) Sector.

View the full resource here.

CYBERLAW FINAL CHEAT SHEET

Mo Khairy | Connect 4 Techs | January 14, 2024

Welcome to our latest resource that's bound to make your Cyberlaw final preparations a breeze! As the semester concludes, we understand the pressure of preparing for exams, especially when it comes to a complex subject like Cyberlaw. To alleviate your stress, we've crafted a comprehensive "Cyberlaw Final Cheat Sheet" that will serve as your go-to guide for acing your exams. In this Cheat Sheet, we'll provide an overview of the cheat sheet, discuss its contents, highlight key topics, and conclude with details on how you can access this valuable resource.

View the full resource here.

COMPUTER SECURITY RESOURCE CENTER

National Institute of Standards and Technology

The Computer Security Resource Center (CSRC) has information on many of NIST's cybersecurity- and information security-related projects, publications, news and events. CSRC supports people and organizations in government, industry, and academia—both in the U.S. and internationally.

- Learn more about current projects and upcoming events
- Search and browse our publications library of current and historical standards, guidelines, and other reports

View the full resource here.

NIST RELEASES FOUR DRAFT PUBLICATIONS FOCUSED ON AI SECURITY

Steve Haley | Compliance Point | May 7, 2024

The National Institute of Standards and Technology (NIST) released four draft publications designed to help organizations improve the safety, security, and trustworthiness of artificial intelligence (AI) systems. The new guidance from NIST follows President Biden's 2023 Executive Order on AI security and the release of the NIST AI Risk Management Framework (AI RMF) earlier in 2024. The new publications focus on multiple aspects of AI technology, including managing the risks of generative AI, transparency in digital content created or altered by AI, and developing global AI standards. All the new NIST publications are initial public drafts, and NIST is soliciting public comments on each through June 2, 2024. Instructions for submitting comments can be found in the respective publications, which are linked in the descriptions below.

View the full resource here.

BEYOND THE SCIF: A CONVERSATION WITH REP. BRAD WENSTRUP (R-OH) ON AI AND BIOSECURITY

On May 6, following introductory remarks by Chairman of the House Permanent Select Committee on Intelligence Mike Turner (R-OH), Rep. Brad Wenstrup (R-OH) moderated a panel with AEI's Dan Blumenthal, Anna Puglisi of Puglisi Ventures, Anthony Ruggiero of the Foundation for Defense of Democracies, Palantir's Ken Staley, and Dov S. Zakheim of the National Security Commission on Emerging Biotechnology. Panelists discussed the state of US biosecurity, China's efforts to gain leverage in biosecurity research processes, and what the US can learn from its experience combating COVID-19. Panelists also reviewed the United States' lack of preparedness for combating bioweapons and naturally occurring pathogens, underscoring the need to research new technologies, protect existing supply chains, and determine how best to work with existing international organizations.

View the full resource here.

LIVESTREAM—RESPONSIBLE COLLABORATION THROUGH APPROPRIATE RESEARCH SECURITY, MAY 23

Rebecca Keiser, NSF chief of research security strategy and policy, will deliver a keynote address on the origins of the RoRs program on May 23 at 8:30 am CDT. Her remarks will be livestreamed on our website. Supported by the NSF's Office of the Chief of Research Security, Strategy, and Policy, the workshop will bring together leading experts from academia, government, and industry to explore the threats and challenges facing the international research and innovation ecosystem. The workshop is led by Rice University's Office of Research Security and the Baker Institute Science and Technology Program in close collaboration with the University of Houston, IPTalons, Inc., the Society of Research Administrators International, and the National Science Foundation (Grant No. 2348714).

View the event details here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute