RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE

THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary

December 21, 2023

DISCOURSE POWER: THE CCP'S STRATEGY TO SHAPE THE GLOBAL INFORMATION SPACE

Christopher Walker | National Endowment for Democracy | December 5, 2023

I would like to thank Chairman Gallagher, Ranking Member Krishnamoorthi, and the other esteemed members of the Select Committee for the opportunity to offer testimony on the critical subject of the Chinese Communist Party's (CCP) influence in the global information space. For the purposes of this testimony, I will focus principally on two aspects of the CCP's growing effort to shape the information domain. The first relates to ideas, the second to the global information infrastructure that disseminates the ideas. The authorities in Beijing take information seriously. It is why they devote such extraordinary resources and effort to controlling and manipulating it. They also take ideas seriously, which explains the extent to which the regime works to prevent the emergence of alternative ones, especially in (but not limited to) the Chinese language media ecosystem, within and beyond the PRC's borders. At home, the CCP draws on its extensive instruments of state power to smother dissent. Abroad, the Chinese authorities cannot apply unchecked repression.

Read the full article here.

NEW FLORIDA LAW BLOCKS CHINESE STUDENTS FROM ACADEMIC LABS

Jeffrey Mervis | Science | December 12, 2023

A new state law is thwarting faculty at Florida's public universities who want to hire Chinese graduate students and postdocs to work in their labs. In effect since July, the law prohibits institutions from taking money from or partnering with entities in China and six other "countries of concern." The list of banned interactions includes offering anyone living in one of those countries a contract to do research. Students could be hired only if they are granted a waiver from the state's top higher education body. But how that process would work is not clear, and the 12 public colleges and universities covered by the law are still writing rules to implement the statute. More than 280 faculty members at the University of Florida, which has the state's largest research portfolio, have signed a petition urging UF to clear up the confusion-and to voice support for an open-door policy on hiring. "We urgently request a timely decision that allows us to recruit top international graduate students with an assistantship, irrespective of their nationality," declares the petition, sent on 6 December to UF President Ben Sasse and senior UF leadership.

Read the full article here.

CHINA'S GLOBAL POLICE STATE: BACKGROUND AND U.S. POLICY IMPLICATIONS

Andrew Hartnett, Nicole Morgret and Rachael Burton | U.S.-China Economic and Security Review Commission | December 13, 2023

The Chinese Communist Party (CCP) is carrying out a global campaign to silence its critics. This campaign targets groups including China's ethnic and religious minorities, dissidents and activists, journalists, students, and others. The victims of the CCP's repression are not just Chinese citizens living abroad but also citizens and residents of the United States and other countries.1 The CCP employs a broad toolkit to stalk, surveil, harass, intimidate, and assault these groups with the ultimate goal of controlling all forms of opposition. In doing so, the CCP eliminates what it perceives as threats to its own stability and survival. In addition to the direct pain and suffering Beijing inflicts on those it targets, its actions have three main implications for U.S. national security: Beijing's transnational law enforcement efforts frequently violate countries' sovereignty.

Read the full article here.

AUTOMAKERS' PROTECTION OF SOFTWARE UNDERSCORES ISSUE OF RISING IP THEFT

Dale Buss | Forbes | November 30, 2023

The theft of American intellectual property is endemic. According to a widely cited report issued by the Commission on the Theft of American Intellectual Property, IP theft costs the U.S. economy hundreds of billions of dollars each year: Estimates range from $225 billion to $600 billion. Nowhere is this more potentially important than in the auto industry. Automakers have been wrestling with Big Tech companies for years over who ultimately is driving the car, since Google, Apple and the like figured out that software would configure the future of the automobile, not traditional hardware like the engine — or tailfins. Major tech players insinuated themselves into a position behind the car's dashboard through navigation systems, user interfaces and the like, then the electrification of vehicles as well as the push toward autonomous driving gave them unprecedented openings.

Read the full article here.

DOD AWARDS $161 MILLION TO UNIVERSITIES TO PURCHASE EQUIPMENT SUPPORTING DEFENSE-RELEVANT RESEARCH

U.S. Department of Defense | December 12, 2023

The Department of Defense today announced awards totaling $161 million to 281 university researchers under the Defense University Research Instrumentation Program. The grants will support the purchase of major equipment to augment current and develop new research capabilities relevant to the Department at 120 institutions across 39 states in fiscal year 2024. DURIP is a strategic investment through which the DOD champions the country's scientific ecosystem. The program equips universities to perform state-of-the-art research that boosts the United States' technological edge, while ensuring that the future science, technology, engineering, and mathematics workforce remains second to none. This year's awards will accelerate basic research in areas the National Defense Science and Technology Strategy prioritizes, including quantum computing and quantum networks, bioelectronics, hypersonics, autonomy, and the design, development, and characterization of novel materials.

Read the full article here.

DOE LAUNCHES NEW OFFICE TO COORDINATE CRITICAL AND EMERGING TECHNOLOGY

Department of Energy | December 12, 2023

The U.S. Department of Energy (DOE) today announced the launch of the Office of Critical and Emerging Technology to ensure U.S. investments in areas such as artificial intelligence (AI), biotechnology, quantum computing, and semiconductors leverage the Department's wide range of assets and expertise to accelerate progress in these critical sectors. Critical and emerging technologies (CET) have broad applications throughout DOE, such as clean energy, national defense, and pandemic preparedness. Major advances in CET hold extraordinary potential for the economy and national security but also pose significant risks, and DOE's new office will focus the Department's efforts to ensuring that its capabilities are helping to solve critical science, energy, and security challenges. "Since their inception, DOE's National Laboratories have been central to the nation's scientific and technological advancement, and we are preparing to ensure that, as new technologies emerge, the United States leads the way in exploring those frontiers," said U.S. Secretary of Energy Jennifer M. Granholm.

Read the full article here.

MCCAUL RELEASES 90-DAY REVIEW REPORT OF COMMERCE DEPARTMENT'S BIS

Foreign Affairs Committee | December 7, 2023

Today, House Foreign Affairs Committee Chairman Michael McCaul released a 90-Day Review Report of the Commerce Department's Bureau of Industry & Security (BIS), the regulatory body responsible for regulating dual-use export controls. Chairman McCaul determined that BIS has enabled a virtually unrestricted flow of American technology to CCP-controlled companies, facilitating China's rapid rise as a technological, economic, and military superpower. "We can no longer afford to avoid the truth: the unimpeded transfer of U.S. technology to China is one of the single-largest contributors to China's emergence as one of the world's premier scientific and technological powers," stated Chairman McCaul**.** "Now is the time to fix this – and the stakes couldn't be higher. The United States must have a win-at-all-costs mentality in these emerging technologies and invest in innovation while denying and delaying China's access to critical U.S. technologies."

Read the full article here.

CONTROLLING LARGE LANGUAGE MODEL OUTPUTS: A PRIMER

Jessica Ji, Josh A. Goldstein and Andrew Lohn | Center for Security and Emerging Technology
December 2023

Concerns over risks from generative artificial intelligence (AI) systems have increased significantly over the past year, driven in large part by the advent of increasingly capable large language models (LLMs). Many of these potential risks stem from these models producing undesirable outputs, from hate speech to information that could be put to malicious use. However, the inherent complexity of LLMs makes controlling or steering their outputs a considerable technical challenge. This issue brief presents three broad categories of potentially harmful outputs—inaccurate information, biased or toxic outputs, and outputs resulting from malicious use—that may motivate developers to control LLMs. It also explains four popular techniques that developers currently use to control LLM outputs, categorized along various stages of the LLM development life cycle: 1) editing pre-training data, 2) supervised fine-tuning, 3) reinforcement learning with human feedback and Constitutional AI, and 4) prompt and output controls.

Read the full article here.

PRIVILEGE ELEVATION EXPLOITS USED IN OVER 50% OF INSIDER ATTACKS

Bill Toulas | Bleeping Computer | December 8, 2023

Elevation of privilege flaws are the most common vulnerability leveraged by corporate insiders when conducting unauthorized activities on networks, whether for malicious purposes or by downloading risky tools in a dangerous manner. A report by Crowdstrike based on data gathered between January 2021 and April 2023 shows that insider threats are on the rise and that using privilege escalation flaws is a significant component of unauthorized activity. According to the report, 55% of insider threats logged by the company rely on privilege escalation exploits, while the remaining 45% unwittingly introduce risks by downloading or misusing offensive tools. Rogue insiders typically turn against their employer because they have been given financial incentives, out of spite, or due to differences with their supervisors. CrowdStrike also categorizes incidents as insider threats when they are not malicious attacks against a company, such as using exploits to install software or perform security testing.

Read the full article here.

NATIONAL SCIENCE FUNDERS EYE SETTING UP INTERNATIONAL NETWORK TO SHARE RESEARCH-SECURITY INFORMATION

Richard Hudson | Science Business | December 12, 2023

As part of a broader push to tighten security, science funders in the US, UK and Canada are considering setting up a network to share information about security risks affecting international research projects, according to a senior US science official. The network would enable regular sharing of unclassified information among key science agencies and their ministries. "Because our researchers collaborate together so much, it makes sense for us to share information – to create an international network," said Rebecca Keiser, head of research security at the US National Science Foundation (NSF). The discussions are already underway with the UK science ministry and its main funding body, UK Research and Innovation, as well as with Canada's innovation ministry and Natural Science and Engineering Research Council. Discussions are also planned with Dutch officials, and possibly others.

Read the full article here.

RUSSIAN RSB CYBER ACTOR STAR BLIZZARD CONTINUES WORLDWIDE SPEAR-PHISHING CAMPAIGNS

Australian Cyber Security Center | December 8, 2023

The Russia-based actor Star Blizzard (formerly known as SEABORGIUM, also known as Callisto Group/TA446/COLDRIVER/TAG-53/BlueCharlie) continues to successfully use spear-phishing attacks against targeted organisations and individuals in the UK, and other geographical areas of interest, for information-gathering activity. The UK National Cyber Security Centre (NCSC), the US Cybersecurity and Infrastructure Security Agency (CISA), the US Federal Bureau of Investigation (FBI), the US National Security Agency (NSA), the US Cyber National Mission Force (CNMF), the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), the Canadian Centre for Cyber Security (CCCS), and the New Zealand National Cyber Security Centre (NCSC-NZ) assess that Star Blizzard is almost certainly subordinate to the Russian Federal Security Service (FSB) Centre 18. Industry has previously published details of Star Blizzard. This advisory draws on that body of information.

Read the full article here.

FIVE EYES NATIONS WARN MOSCOW'S MATES AT THE STAR BLIZZARD GAME HAVE NEW PHISHING TARGETS

Jessica Lyons Hardcastle | The Register | December 8, 2023

Russia-backed attackers have named new targets for their ongoing phishing campaigns, with defense-industrial firms and energy facilities now in their sights, according to agencies of the Five Eyes alliance. In a joint security alert issued on Thursday, seven agencies* from Australia, Canada, New Zealand, the US and the UK, warned about a criminal gang named Star Blizzard and its evolving phishing techniques. The agencies note that the Russian gang, also known as Callisto Group/TA446/COLDRIVER/TAG-53/BlueCharlie "is almost certainly subordinate to the Russian Federal Security Service (FSB) Center 18." This isn't to be confused with Russia's military intelligence agency, the GRU, which also has its own cyber-spy arm and also likes to go phishing in US and European networks. "Russia continues to be a threat," Rob Joyce, director of NSA's cybersecurity directorate, warned in a statement. "Those at risk should note that the FSB likes to target personal email accounts, where they can still get to sensitive information but often with a lower security bar."

Read the full article here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute

ENTERPRISE RISK MITIGATION BLUEPRINT FOR NON-INTELLIGENCE AGENCIES

National Counterintelligence and Security Center | December 2023

Nothing in this document shall be construed as authorization for any organization to conduct activities not otherwise authorized under statutes, executive order, or other applicable law, policy, or regulation nor does this document obviate an organization's responsibility to conduct activities that are otherwise mandated, directed, or recommended for execution under the same. Threats are not limited to only cyber, insider, foreign intelligence and/or criminal activities. Today's global threat environment is more diverse and dynamic than ever. The 2023 Annual Threat Assessment of the U.S. Intelligence Community (IC) 1 identified a growing number of foreign intelligence entities (FIE), state actors, and non-state actors targeting the United States Government (USG) and the private sector. They are no longer interested just in obtaining classified U.S. secrets but are also collecting sensitive unclassified information from most government agencies and virtually every sector of our economy.

Read the full article here.

RESET, PREVENT, BUILD: A STRATEGY TO WIN AMERICA'S ECONOMIC COMPETITION WITH THE CHINESE COMMUNIST PARTY

The Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party | December 5, 2023

For a generation, the United States bet that robust economic engagement would lead the Chinese Communist Party to open its economy and financial markets and in turn to liberalize its political system and abide by the rule of law. Those reforms did not occur. Since its accession to the World Trade Organization in 2001, the CCP has pursued a multidecade campaign of economic aggression against the United States and its allies in the name of strategically decoupling the People's Republic of China from the global economy, making the PRC less dependent on the United States in critical sectors, while making the United States more dependent on the PRC. In response, the United States must now chart a new path that puts its national security, economic security, and values at the core of the U.S.-PRC relationship. The House Select Committee on the Strategic Competition between the United States and the Chinese Communist Party (Select Committee) has studied the PRC's pattern of aggression and economic manipulation and recommends the following strategy for economic and technological competition with the PRC.

Read the full article here.