RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE

THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary

June 27, 2024

US LAWMAKERS AIM TO LIMIT CITIZENS OF CHINA AND RUSSIA FROM ACCESSING DOE LABS

Mitch Ambrose | American Institute of Physics (AIP) | June 17, 2024

The Senate Intelligence Committee is proposing to prohibit citizens of China and Russia without permanent residence status in the U.S. from accessing Department of Energy national labs without a waiver. The proposal is contained in the Intelligence Authorization Act that the committee released this month after voting unanimously to advance the legislation to the full Senate for consideration. The prohibition would also apply to citizens of Iran, North Korea, and Cuba. The legislation states that while "international cooperation in the field of science is critical to the United States maintaining its leading technological edge," the DOE lab system "is increasingly targeted by adversarial nations to exploit military and dual-use technologies for military or economic gain." It also states that more than 8,000 citizens from China and Russia were granted access to DOE national labs in fiscal year 2023, out of a total of around 40,000 foreign users of the labs. Many of these visits presumably were to the labs' scientific user facilities, which DOE historically has made broadly available to external researchers. DOE is pushing back against the proposed restriction. "This proposal would have a significant impact on our national laboratories.

Read the full article here.

US RESTRICTS EXPORTS TO TOP QUANTUM LABS IN CHINA

Jacob Taylor | American Institute of Physics (AIP) | June 10, 2024

Last month, the Commerce Department placed stringent export controls on many of the top quantum research centers in China. The department singled out 22 institutions for "their participation in the People's Republic of China's (PRC) quantum technology advancements and for acquiring or attempting to acquire U.S.-origin items to enhance the PRC's quantum capabilities." It added that these technologies "have substantial military applications and pose a significant threat to U.S. national security." Among the affected institutions are four branches of the Chinese Academy of Sciences, the Hefei National Laboratory for Quantum Information Science, and the University of Science and Technology of China. USTC was also targeted for "advancing China's nuclear program." The department placed these institutions on the "Entity List," requiring them to secure a license to acquire U.S.-origin technologies. The department also indicated it would likely deny such license requests. Fundamental research partnerships are generally exempt from these controls, but having affiliations with institutions on the Entity List can be considered a risk factor in federal funding decisions.

Read the full article here.

CHINA'S DRONES ARE ITS GREATEST WEAPON IN TODAY'S INFORMATION WARFARE

Rob Joyce | The Hill | June 20, 2024

I've spent a career studying and mitigating threats from our most significant adversaries, and it is clear the growing threat from Chinese-made drones is dire and underappreciated. I couldn't be happier to see members of Congress working across the aisle to rid the U.S. of these dangerous products. Across my decades of public service, including as the acting homeland security adviser for the U.S. National Security Council and director of cybersecurity for the National Security Agency, I recognize urgent threats to our nation when I see them. Chinese drones are one of the most significant intelligence and national security threats we currently face as a country. When it comes to national security, drones have changed the game. The Russian invasion of Ukraine demonstrates the expansive and exceptional capabilities of both large and small drones.

Read the full article here.

THE ROLE OF RESEARCH FUNDERS IN PROVIDING DIRECTIONS FOR MANAGING RESPONSIBLE INTERNATIONALIZATION AND RESEARCH SECURITY

Tommy Shih | ScienceDirect | April 2024

Since the end of the 1990s and in the wake of the Cold War, research publication volume has significantly increased globally and scientific progress has been rapid. Advancements and publication growth have not only come from Western countries, but also from other parts of the world such as Asia, and China in particular (Miao et al., 2022). These developments, which stem from increased international collaboration and brain circulation in the world, are positive from a globalization perspective, but are also affected by changing global power balances (Marginson, 2022a). Geopolitical competition is increasing, and noticeable barriers are being erected by various governments in advanced science nations, especially between the United States (US) and China. This has been thwarting international collaboration in especially technology due to national concerns over losing economic and technological advantages vis-à-vis other countries, through what are perceived as non-reciprocal knowledge exchanges (The White House, 2022a).

Read the full article here.

ENHANCING RESEARCH SECURITY

E. Thierry | Policy Commons | March 26, 2024

On 24 January 2024, the European Commission tabled a proposal for a Council recommendation on enhancing research security. The procedure does not require the European Parliament's involvement. Research security refers to the safeguarding of scientific activities against misuse and undue influence by third countries or non-state actors. Risks to research include the illicit transfer of knowledge or technology resulting in a threat to the EU's security or undermining its values. Competence for identifying and managing these risks lies with several public bodies, including national authorities and academic institutions. Research security is therefore distinct from research integrity, which seeks to safeguard the reliability and honesty of knowledge creation by individual scientists and academic institutions in line with scientific standards.

Read the full article here.

A DUTY TO PROTECT FROM SCIENCE? INTERACTIONS IN INTERNATIONAL LAW BETWEEN RESEARCH SECURITY AND THE RIGHT TO SCIENCE

Brendan Walker-Munro | South Cross University | May 23, 2024

China boasts some of the world's most talented cybersecurity researchers and white hat hackers, as well as a strict cybersecurity law compelling individuals to assist the state. This combination appears to contribute to China's nation-state hacking groups' prowess and ability to wield more zero-day vulnerabilities than any other country, as they support Beijing's robust cyberespionage agenda, as well as intellectual property theft on behalf of public and private entities, according to a new report from cybersecurity researcher Eugenio Benincasa. Beijing is using domestic capture-the-flag and other hacking competitions to spot, develop and recruit new hacking talent domestically, as well as to gather and route information about zero-day flaws to the country's military and intelligence apparatus, according to Benincasa, who's a senior researcher in the Cyberdefense Project with the Risk and Resilience Team at the Center for Security Studies at Switzerland's public research university ETH Zurich.

Read the full article here.

UNIVERSITIES MUST HELP COUNTER THE GROWING THREAT OF AI EXTREMISM

Jan Petter Myklebust and Karen MacGregor | University World News | June 20, 2024

AI researchers are misjudging the threat of AI extremism, a recent report has warned. There is an urgent need for governments, academia and the private sector to develop collective guidelines around open source AI models to prevent them from falling into the hands of extremists. Further, "as a matter of critical security, governments, the private sector and academia need to agree on rules restricting not only the availability of results from biomedical models that have potential dual-use capabilities, but also the information available on the researchers who created these models and who could be blackmailed (with or without AI)", advises the report. The report is written by Stephane Baele, professor of international relations at UCLouvain in Belgium and honorary associate professor of security and political violence at the University of Exeter in the United Kingdom; and Lewys Brace, a senior lecturer and co-director of the Centre for Computational Social Science at Exeter.

Read the full article here.

TO WHAT EXTENT IS CHINA A 'SECURITY THREAT'?

Debasish Sarmah | Institute for Security and Development Policy | June 17, 2024

With the conclusion of the Cold War and the disintegration of the Union of Soviet Socialist Republics (USSR), the United States (U.S.) emerged as the dominant force in the global economic, political, and military spheres. This marked the beginning of a new era, with U.S. President George H. W. Bush advocating for the principles of the Western order that had triumphed over the USSR, rebranding it as a 'liberal international order'.[1] The Cold War-era international institutions such as the United Nations (UN) and North Atlantic Treaty Organization (NATO), along with arms control treaties, were assimilated into what Bush referred to as the 'new world order'.[2] Since then, the liberal international order has propelled the rise of numerous modern-day economic powers. Among them was China, where the Western democracies anticipated that the liberal ideals would be embraced as the country modernized and prospered. However, in a twist of events, China veered off this anticipated path.

Read the full article here.

RECORD SETTLEMENT OVER CHINA FUNDING PUTS U.S. RESEARCH INSTITUTIONS ON NOTICE

Jeffrey Mervis | Science | June 12, 2024

Over the past 5 years, the U.S. Department of Justice (DOJ) has won only a handful of criminal cases in which it prosecuted scientists alleged to have defrauded the government by not disclosing research support they received from China. But last month DOJ sent a clear message that, despite that poor track record, research institutions will be held accountable for mistakes in monitoring outside support to their faculty. A 17 May settlement with the Cleveland Clinic Foundation (CCF) requires the medical colossus to pay the government $7.6 million to resolve allegations it mismanaged three grants from the National Institutes of Health (NIH). It's a record amount for a case involving foreign research support, a mechanism U.S. policymakers believe China has used to steal U.S. technology. "Today's settlement illustrates the importance of being truthful at every stage of the grants process," U.S. Attorney Rebecca Lutzko said in a statement announcing the settlement. In addition to the fine, the settlement requires a top CCF administrator "to personally attest" to the accuracy of all information it submits to NIH.

Read the full article here.

MICROSOFT IN DAMAGE-CONTROL MODE, SAYS IT WILL PRIORITIZE SECURITY OVER AI

Ashley Belander | Ars Technica | June 13, 2024

Microsoft is pivoting its company culture to make security a top priority, President Brad Smith testified to Congress on Thursday, promising that security will be "more important even than the company's work on artificial intelligence." Satya Nadella, Microsoft's CEO, "has taken on the responsibility personally to serve as the senior executive with overall accountability for Microsoft's security," Smith told Congress. His testimony comes after Microsoft admitted that it could have taken steps to prevent two aggressive nation-state cyberattacks from China and Russia. According to Microsoft whistleblower Andrew Harris, Microsoft spent years ignoring a vulnerability while he proposed fixes to the "security nightmare." Instead, Microsoft feared it might lose its government contract by warning about the bug and allegedly downplayed the problem, choosing profits over security, ProPublica reported.

Read the full article here.

ARE AI-BASED ATTACKS TOO GOOD FOR SECURITY AWARENESS TRAINING?

Tom Tovar | DARKREADING/Appdome | June 17, 2024

In an era where artificial intelligence (AI) continues to advance at a staggering pace, traditional security awareness training is being challenged like never before. The rise of sophisticated AI-powered threats such as smishing, vishing, deepfakes, and AI chatbot-based attacks could render this traditional human-centric approach to defense increasingly ineffective.

Today, Humans Have a Slight Advantage

Currently, security awareness training teaches individuals to spot the signs and tactics used in social engineering attacks. Consumers and employees are taught to recognize suspicious emails (phishing), dubious text messages (smishing), and manipulative phone calls (vishing). Training programs help individuals identify red flags and detect subtle inconsistencies — such as slight variations in language, unexpected requests, or minor errors in communication — to provide a critical line of defense.

Read the full article here.

A QUANTITATIVE ASSESSMENT OF DEPARTMENT OF DEFENSE S&T PUBLICATION COLLABORATIONS

Emelia Probasco and Autumn Toney | Center for Security and Emerging Technology | June 2024

While the effects of the Department of Defense's broad investments in research and development go far beyond what is publicly disclosed, authors affiliated with the DOD do publish papers about their research. These papers reflect a small portion of the DOD's engagement efforts across an enormous research ecosystem, but they nonetheless offer some insight into the patterns of research collaboration by the DOD. By analyzing more than 100,000 papers authored by researchers affiliated with the DOD*in the OpenAlex database, we find:

- Of 100,158 DOD-affiliated papers that we manually reviewed for specific entity affiliation, approximately 86% list an author from a DOD organization (such as the U.S. Army, Naval, or Air Force Research Laboratory), 12% include a DODaffiliated federally funded research and development center or university affiliated research center (FFRDC/UARC), and 2% have both a DOD and a DOD FFRDC/UARC affiliated author.

Read the full article here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute

DON'T TRUST BUT VERIFY: STRENGTHENING U.S. LEADERSHIP TO SAFEGUARD OUR CYBER DEFENSES

MITRE | June 6, 2024

While some cyber risks are well-known and understood, others are emerging with little consensus on how to protect against them and what future challenges they might pose. What's clear is that critical infrastructure is at risk, the cost of cyber crime is rising, cyber threats are global in scope, emerging technologies present concerns, and zero trust and assurance are crucial. With the responsibilities and authorities for cybersecurity divided among U.S. government departments, agencies, and offices—and shared with many sectors, critical infrastructure owners and operators, and SLTT governments—our success depends on effective U.S. leadership. Beyond describing risks and challenges, this paper also provides four sets of specific priority recommendations, namely:

1. **Implement measures to protect critical infrastructure** — update the National Preparedness System to account for large-scale critical infrastructure attacks, require zero trust principles for operational technology, operationalize software bill of materials (SBOM) for critical infrastructure systems, and explore new partnership models.

View the full resource here.

SCIENCE AND SECURITY RESOURCE DOCUMENT

Association of American Universities | June 2024

Research institutions play a crucial role in safeguarding national security by protecting confidential data, intellectual property, and classified materials from foreign threats. Institutions must also keep their faculty and students apprised of new disclosure and training requirements mandated by the federal government. This resource document identifies key terms; effective practices proposed by institutions and government and non-government entities; links to various government and non-government entity lists, and topical analysis and proposed policy recommendations in several key areas.

View the full resource here.

CLARIVATE REVEALS WORLD'S LEADING AND TRUSTED JOURNALS WITH THE 2024 JOURNAL CITATION REPORTS

Clarivate | June 20, 2024

Clarivate Plc (NYSE:CLVT), a leading global provider of transformative intelligence, today released the 2024 update to the Journal Citation Reports™ (JCR™). The reports provide an essential and comprehensive resource of high-quality journals, ranked by field to enable academic institutions, researchers and publishers to gauge the significance of journals in the global research landscape. Changes to journal rankings include the addition of the Emerging Sources Citation Index. Only journals that have met the rigorous quality standards for inclusion in the Web of Science Core Collection™ are featured within the Journal Citation Reports, to ensure that users can confidently rely on the information and descriptive data provided.

View the full resource here.

PROTECT YOURSELF: COMMERCIAL SURVEILLANCE TOOLS

The National Counterintelligence and Security Center | June 2024

Companies and individuals have been selling commercial surveillance tools to governments and other entities that have used them for malicious purposes. Journalists, dissidents, and other persons around the world have been targeted and tracked using these tools, which allow malign actors to infect mobile and internet-connected devices with malware over both WiFi and cellular data connections. In some cases, malign actors can infect a targeted device with no action from the device owner. In others, they can use an infected link to gain access to a device.

View the full resource here.

PHISHING GUIDANCE: STOPPING THE ATTACK CYCLE AT PHASE ONE

The National Counterintelligence and Security Center | June 2024

Social engineering is the attempt to trick someone into revealing information (e.g., a password) or taking an action that can be used to compromise systems or networks. Phishing is a form of social engineering where malicious actors lure victims (typically via email) to visit a malicious site or deceive them into providing login credentials. Malicious actors primarily leverage phishing for:

- Obtaining login credentials. Malicious actors conduct phishing campaigns to steal login credentials for initial network access.
- Malware deployment. Malicious actors commonly conduct phishing campaigns to deploy malware for follow-on activity, such as interrupting or damaging systems, escalating user privileges, and maintaining persistence on compromised systems.

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute

UPCOMING RESEARCH SECURITY EVENTS

TRADE SECRETS PROTECTION AND ENFORCEMENT PRACTICE IN CHINA

Trade secrets play an important role in firm competitiveness and strategic positioning, especially for startups and in research and development–intensive industries. Firms should actively prevent unauthorized disclosures of trade secrets. In case of a theft, they may need to pursue enforcement. Protecting trade secrets is an ongoing challenge for companies doing business in the United States and the People's Republic of China. Join us at United States Patent and Trademark Office (USPTO) headquarters in Alexandria, Virginia, for an examination of enforcement avenues against trade secret misappropriation in China.

- June 28, 2024
- United States Patent and Trademark Office, 600 Dulany Street, Alexandria, VA 22314

View the full resource here.

PUBLIC SAFETY CANADA RESEARCH SECURITY WEBINAR: MODULE 1 - SAFEGUARDING SCIENCE (JULY)

Safeguarding Science: Raising awareness of security risks and mitigation tools in the research ecosystem

The purpose of the Safeguarding Science workshop is to raise awareness within Canada's scientific and academic communities about research security-related issues. The primary objective of this workshop is to explain the potential for misuse of dual-use research, technology and materials, along with possible risk indicators and mitigation tools to protect Canadian research assets.

- July 9, 2024
- Online Event

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute