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

Open Source Media Summary
August 8, 2024

NCSC UNVEILS THE NEW NATIONAL COUNTERINTELLIGENCE STRATEGY

The National Counterintelligence and Security Center | Press Release | August 1, 2024

The National Counterintelligence and Security Center (NCSC) today unveiled the new National Counterintelligence Strategy, which can be accessed at www.ncsc.gov. "Today's strategy is designed to drive integration, action, and resources across the counterintelligence (CI) community to outmaneuver and constrain foreign intelligence entities (FIEs), protect America's strategic advantages, and invest in the future to meet tomorrow's threats," said NCSC Director Michael Casey. "Developed with our partners across the U.S. government, the strategy provides a comprehensive vision and direction for the CI community to address increasingly complex foreign intelligence threats. "Signed by President Biden today, the strategy updates CI priorities based on current and anticipated threats and communicates these priorities to the CI community, federal, state, and local partners, as well as Congress, industry, academia, foreign partners, and the public. The strategy provides a framework for strategic planning, resourcing, and evaluation. It also aligns CI community efforts with the U.S. National Security Strategy and other national strategies to drive progress in key CI mission areas. Three key pillars govern the strategy:
1) outmaneuver and constrain FIEs; 2) protect U.S. strategic advantages; and 3) invest in the future.

Read the full article here.

CHINESE COMMUNIST, MILITARY WRITINGS REVEAL PLANS FOR STRATEGIC INFLUENCE OPERATIONS THROUGH TIKTOK

Bill Gertz | The Washington Times | August 1, 2024

The Chinese Communist Party and China's military view TikTok as one of several strategic tools for both political-influence operations and military-support actions, according to an open-source intelligence report on the short-video sharing app. The report by two former military and intelligence experts warns that continued use of the wildly popular video-sharing app in the United States will be used by Beijing to target young people and "shift American narratives subtly to favor a more China-centric worldview." The report made public recently examines a law signed by President Biden in April to force TikTok's China-based owner, ByteDance, to sell the American operation to a non-Chinese government-linked owner or be banned nationally. A month later, ByteDance sued to oppose the law, saying it violates the First Amendment. The Justice Department contended in a legal filing last last month that TikTok collects sensitive data on American users' views of religion, abortion and gun control, and censors online material at the direction of ByteDance. The company's American management has denied the charge.

Read the full article here.

CHINA'S APT41 TARGETS TAIWAN RESEARCH INSTITUTE FOR CYBER ESPIONAGE

Jai Vijayan | DARKREADING | August 2, 2024

China-linked advanced persistent threat group APT41 appears to have compromised a government-affiliated institute in Taiwan that conducts research on advanced computing and associated technologies. The intrusion began in July 2023, with the threat actor gaining initial access to the victim environment via undetermined means. Since then, it has deployed multiple malware tools, including the well-known ShadowPad remote access Trojan (RAT), the Cobalt Strike post compromise tool, and a custom loader for injecting malware using a 2018 Windows remote code execution vulnerability (CVE-2018-0824). APT41 is an attribution that several vendors use to track a loose collective of China-nexus threat groups that have been engaged in a broad range of cyber espionage and financially motivated cyberattacks around the world, going back to 2012.

Read the full article here.

EFFECTIVE US GOVERNMENT STRATEGIES TO ADDRESS CHINA'S INFORMATION INFLUENCE

Kenton Thibaut | Atlantic Council | July 30, 2024

China's global influence operations have received increasing attention in the national security community. Numerous congressional hearings, media reports, and academic and industry findings have underscored China's increased use and resourcing of foreign information manipulation and interference (FIMI) tactics in its covert operations both in the United States and abroad. In response, US government offices the Foreign Malign Influence Center (FMIC), the Global Engagement Center (GEC), and the Cybersecurity and Infrastructure Security Agency (CISA), among others, have made strides in raising awareness of the issue and charting pathways to increase the resilience of the US information ecosystem to foreign influence. To date, however, the efforts to counter the influence of the People's Republic of China (PRC) have been fragmented. That fragmentation is indicative of a lack of cohesion around the concept of influence operations itself.

Read the full article here.

COMMITTEE LEADERS LUCAS AND LOFGREN CONTINUE INVESTIGATION INTO OPTICA'S USE OF UNDISCLOSED FUNDS FROM HUAWEI TO BACK U.S. RESEARCH

House Committee on Science, Space and Technology | Press Release | July 30, 2024

Yesterday, Chairman Frank Lucas (R-OK) and Ranking Member Zoe Lofgren (D-CA) sent a follow-up letter to Elizabeth Rogan, CEO of Optica, requesting responses to unanswered questions and addressing new reporting that calls into question how Optica characterized its relationship with Huawei. In their letter, Chairman Lucas and Ranking Member Lofgren said, "We do not believe Optica properly acknowledged the full extent of Huawei's influence in its response to the Committee. Our ability to fully assess the implications of Optica's relationship with Huawei in terms of research security policymaking is undermined by our incomplete understanding of its scope." The Committee leaders continued, "As the research ecosystem at large has adapted, it seems that Optica has remained locked in an outdated posture, deepening its relationship with Huawei as the company is slapped with sanctions by multiple government agencies.

Read the full article here.

GEOPOLITICS THREATENS SCIENCE AND SOCIETAL PROGRESS

Brad Glosserman | The Japan Times | July 30, 2024

International cooperation and collaboration is the backbone of modern science. It's key to solving new and enduring problems in Japan and throughout the world. It ensures that Japan — like most countries — stays on the leading edge of innovation, honing the tools and capabilities it needs to maintain a vibrant and dynamic society and economy. And, of course, that collaboration is now threatened by the deepening tensions that define international relations. It is precisely the applications of that research and their potential impacts that have prompted governments to more closely scrutinize, and subsequently restrict, scientific cooperation. The biggest challenge then today for researchers, the institutions they labor at and the governments that oversee that work, is finding the right balance between promoting and protecting science. It's a work in progress and the effort doesn't seem to be making anyone happy. Collaboration is the new norm in science. In a 2023 paper, Norwegian researchers Dag Aksnes and Gunnar Sivertsen found that the share of publications worldwide representing international collaboration expanded from 4.7% in 1980 to 25.7% in 2021.

Read the full article here.

US BIOTECH RIVALRY WITH CHINA INTENSIFIES AMID SECURITY CONCERNS

Evrim Ağaci | The Pinnacle Gazette | July 31, 2024

The ongoing rivalry between the United States and China has grown increasingly pronounced in the field of biotechnology, prompting lawmakers to express significant concerns regarding the U.S. capacity to effectively compete. As tensions escalate over trade, technology, and national security, legislators are advocating for more proactive measures to bolster American innovation. This situation has led to debates surrounding the potential consequences of curtailing Chinese participation in U.S. biotech industries, a move some warn could backfire. In recent months, voices from both parties in Congress have echoed warnings that America risks falling behind as China emerges as a formidable leader in biotechnology. This shift in the economic landscape has been underscored by notable advancements from Chinese firms, which have made significant strides in areas ranging from agricultural biotechnology to pharmaceuticals and healthcare solutions.

Read the full article here.

CRACKDOWN ON CHINESE STUDENTS RAISES FEARS FOR UK TECH AMBITIONS

Yazhou Sun | BNN Bloomberg | August 1, 2024

Chinese national Luo, 23, was thrilled when he was accepted into Cambridge University's electrical engineering PhD program in 2021. All he needed before starting was clearance from a UK government agency that vets postgraduate students who study topics that could have military applications. Luo considered that a formality, he told Bloomberg in an interview, considering he'd already been green-lit for his masters degree at the same school. But he was rejected. So he applied again, and was rejected again. The agency that reviewed his application — the UK Foreign, Commonwealth & Development Office — gave no reason. But since Luo couldn't fathom being considered a security risk, he applied 14 more times over the next two years while enduring Covid-19 lockdown from his hometown in Sichuan, tweaking the applications to what he hoped would be seen as less sensitive subjects each time to no avail, before switching his research to a field not covered by the FCDO's vetting process.

Read the full article here.

INTELLECTUAL PROPERTY RISK: SAFEGUARDING YOUR TECH COMPANY'S MOST VALUABLE ASSETS

TechFunnel | August 1, 2024

In today's business landscape, intangible assets like intellectual property (IP) are becoming increasingly important, particularly for tech companies. IP holds significant value as it can drive a company's growth and success in the industry, or conversely, its compromise can lead to the company's downfall and potential bankruptcy. Therefore, tech companies must be well-guided in mitigating the risks and threats associated with IP breaches or theft. The main goal of taking proactive measures to safeguard IP is to maintain the integrity of its creator and inventor and to prevent any unwarranted use and unauthorized duplication. Intellectual property pertains to the unique intellectual creations or inventions developed by individuals or brands that hold commercial value and offer trade advantages.

Read the full article here.

INTELLECTUAL PROPERTY PROTECTION: BEST PRACTICES TO REDUCE LIABILITY

Mark Raymond | GoodFirms | August 8, 2024

Innovation can be encouraged only when it gets the proper protection and exclusive control. Consuming intellectual goods requires a form of intellectual property law - the rights, patents, or copyright that indicates the limitation of the use of the information and intellectual goods. With smart fraudsters, identifying and detecting the damage created by infringement and piracy is a challenge. Conventional approaches are insufficient as there is no visibility at the granular level. Intellectual property (IP) rights offer legal protection to inventors and creators as outlined in the law and enable exclusive access. Currently, blockchain and NFTs are poising to have the potential to track and guard intellectual property (IP) better.

Read the full article here.

WITH SMUGGLERS AND FRONT COMPANIES, CHINA IS SKIRTING AMERICAN A.I. BANS

Ana Swanson & Claire Fu | The New York Times | August 4, 2024

The U.S. is trying to stop China from getting Nvidia microchips to advance its military. The private sector is fighting back. In the southern Chinese city of Shenzhen, a mazelike market stretches for a half-mile, packed with stalls selling every type of electronic imaginable. It's an open secret that vendors here are offering one of the world's most sought-after technologies: the microchips that create artificial intelligence, which the United States is battling to keep out of Chinese hands. One vendor said he could order the chips for delivery in two weeks. Another said companies came to the market ordering 200 or 300 chips from him at a time. A third business owner said he recently shipped a big batch of servers with more than 2,000 of the most advanced chips made by Nvidia, the US tech company, from Hong Kong to mainland China.

Read the full article here.

USEFUL RESOURCES

G7 RESEARCH SECURITY AND INTEGRITY PAPERS AND G7 VIRTUAL ACADEMY

Research Collaboration Advice Team | GOV.UK | August 2, 2024

The Department for Science, Innovation and Technology has published two papers on research security and integrity and launched a Virtual Academy with the G7.

View the full resource here.

SAFEGUARDING THE PUBLIC: RUSSIAN INTELLIGENCE POSES A PERSISTENT THREAT TO THE UNITED STATES

The National Counterintelligence and Security Center | August 2024

Despite Russia's substantial military losses since its February 2022 invasion of Ukraine, Russia's intelligence services (RIS) remain a formidable threat to the United States. In recent months, the U.S. government has sanctioned several Russian intelligence operatives and their associates for activities targeting the United States, and authorities across Europe have arrested and charged a number of suspected Russian spies in their nations.

View the full resource here.

INSTITUTIONS' EXPERIENCES WITH THE DEPARTMENT OF DEFENSE POLICY FOR RISK-BASED SECURITY REVIEWS OF FUNDAMENTAL RESEARCH:A SUMMARY OF RESULTS FROM COGR'S SURVEY OF MEMBER INSTITUTIONS

Kristin H. West | Council on Governmental Relations (COGR) | April 26, 2013

In response to concerns about malign foreign influence on fundamental research, federal research funding agencies have implemented requirements designed to ensure that researchers provide complete and accurate disclosures of all appointments, affiliations, and research funding sources.

View the full resource here.

TECHNOLOGY TRANSFER PROGRAM

U.S. Cyber Command

The mission of the Technology Transfer Program for U.S. Cyber Command is to foster collaboration with industry, academia, and other government organizations to develop innovative capabilities and solutions to our challenge problem set. Through strategic partnerships and knowledge sharing, we aim to accelerate the transfer of cutting-edge technologies and expertise to enhance U.S. cyber capabilities for our mission force.

View the full resource here.

TRUSTED RESEARCH GUIDANCE FOR ACADEMIA

The UK Government's National Protective Security Authority | July 2, 2024

The UK has a thriving research and innovation sector that attracts investment from across the world. More than half of UK research is a product of international partnerships. Trusted Research aims to support the integrity of the system of international research collaboration, which is vital to the continued success of the UK's research and innovation sector. It is particularly relevant to researchers in STEM subjects, dual-use technologies, emerging technologies and commercially sensitive research areas. The advice has been produced in consultation with the research and university community and is designed to help the UK's world-leading research and innovation sector get the most out of international scientific collaboration whilst protecting intellectual property, sensitive research and personal information.

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute