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

Open Source Media Summary

October 3, 2024

EXCLUSIVE: INSIDE BEIJING'S APP COLLECTING INFORMATION FROM BELT AND ROAD COMPANIES

Daria Impiombato, Bethany Allen, and Nathan Attrill | Australian Strategic Policy Institute | September 27, 2024

China's Ministry of Foreign Affairs operates a secure digital platform that connects it directly with Chinese companies operating abroad, requiring participating companies to submit regular reports about their activities and local security conditions to the government, internal documents reveal. The documents obtained and verified by ASPI's China Investigations and Analysis team show how the platform, called Safe Silk Road (平安丝路), collects information from companies participating in the Belt and Road Initiative (BRI), Chinese leader Xi Jinping's signature foreign policy initiative. The BRI has facilitated Chinese infrastructure projects and other investment in more than 100 countries, particularly developing regions. The Safe Silk Road platform was initially launched in 2017 and is now used by at least dozens of Chinese companies across several continents. By tapping into the extensive network of Chinese companies engaged in projects around the world, the platform demonstrates how Beijing is finding new ways of improving its global information and intelligence collection to better assess risks, and ultimately protect its interests and its citizens, even in the most remote corners of the world.

Read the full article here.

ENTERPRISE RISK MITIGATION BLUEPRINT FOR NON-INTELLIGENCE AGENCIES

National Counterintelligence and Security Center | 2023

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. Personal data, trade secrets, intellectual property, technology, and research and development are being aggressively targeted by adversaries who have the capability, patience, and resources to obtain them. To achieve their objectives, FIEs are employing a wide range of illegal techniques including insider threats, cyber penetrations, supply chain attacks, and blended operations that combine some or all of these methods.

Read the full article here.

THE CHINA CHALLENGE: HOW THE U.S. CAN COUNTER BEIJING'S AUTHORITARIAN AMBITIONS

Igor Khrestin | George W. Bush Presidential Institute | September 16, 2024

China "presents America's most consequential national security challenge," according to the most recent National Security Strategy of the United States. What is known as the China challenge is among the few domestic or foreign policy issues that have united Democratic and Republican administrations in recent history. As Mike Gallagher, the former Chairman of the bipartisan House Select Committee on the Chinese Communist Party, said: "This is an existential struggle over what life will look like in the 21st century – and the most fundamental freedoms are at stake." The rise of an authoritarian China is a multigenerational call to action for the United States to address. Members of Congress and top administration officials alike have believed that dealing with Beijing in the long term will be an all-societal undertaking in which America and Americans must prevail if our country is to keep its privileged position as the leading superpower that shapes the global order – or let a communist authoritarian regime fundamentally reshape that order.

Read the full article here.

REPUBLICANS SOUND ALARM ON RESEARCH PARTNERSHIPS WITH CHINA

Kathryn Palmer | Inside Higher Education | September 24, 2024

Republican lawmakers want to enact stronger guardrails for research partnerships between American universities and China, purportedly to prevent the Communist power from exploiting federally funded research for its own strategic use, according to a report released Monday by the chairs of the House Committee on the Chinese Communist Party (CCP) and the House education and workforce committee. "To win the future and beat the Chinese Communist Party in developing next-generation technology, we must stop government research that bolsters our adversaries' military and intelligence-gathering capabilities," said House Energy and Commerce Committee chairwoman Cathy McMorris Rodgers.

Read the full article here.

THE 'CHINA INITIATIVE' FAILED U.S. RESEARCH AND NATIONAL SECURITY. DON'T BRING IT BACK.

Michael German | Brennan Center for Justice | September 23, 2024

Allies of former President Donald Trump want to bring back one of his administration's most disastrous policies, the China Initiative. Project 2025, a set of policy proposals put forward by the conservative Heritage Foundation, recommends reviving the program through executive action. And House Republicans, joined by 23 Democrats, just passed a bill that would require reinstating a rebranded version of it.
For the sake of U.S. national security, these efforts must be defeated. Launched by the Department of Justice in 2018 and led by the FBI and federal prosecutors, the China Initiative was an unmitigated failure that caused lasting harm to U.S. national interests. Ostensibly designed to combat economic espionage and intellectual property theft by Chinese government agents, the program quickly devolved into a campaign of racial profiling and fearmongering that targeted U.S.-based scientists and technologists who were not even suspected of spying or intellectual property theft.

Read the full article here.

EXCESSIVE SECRECY 'UNDERMINING SECURITY' OF AUSTRALIAN RESEARCH

John Ross | Times Higher Education | September 25, 2024

Excessive secrecy in Australian security circles is fostering an all-or-nothing mentality that undermines natural justice and exacerbates security risks, according to an expert. Brendan Walker-Munro said a code of silence kept universities in the dark over their legitimate security issues. Staff from the government's security agency, Asio, often wanted to offer guidance but were "hamstrung" by the organisation's "incredibly strong" secrecy provisions. "Universities…have been asking and even begging the government [for] more clarity," he said. "The intelligence services…want to get this right and to help as much as they can. But it's nowhere near as tailored as the universities are asking for and probably actually need." A string of unexplained prohibitions involving Asio – including the vetoing of five Australian Research Council grants, the cancellation of two Chinese scholars' visas and delays in the processing of hundreds of foreign doctoral students' visa applications – has left universities and their staff jumping at shadows.

Read the full article here.

FRANCE AND CANADA STRENGTHEN RESEARCH TIES

Polly Nash | The Pie | September 26, 2024

Convening in Toulouse ahead of the international EAIE 2024 conference, Universities Canada and France Universités signed a memorandum of understanding (MoU) to strengthen the two countries' higher education sectors and communities. "The partnerships and insights gained through this agreement will help Canadian universities collaborate across Europe to tackle some of the biggest global challenges we face – whether it's housing, productivity or social inequality," said Gabriel Miller, president and CEO of Universities Canada. "The agreement focusses on facilitating increased dialogue between French and Canadian universities to nourish the discussions around internationalisation of education and research, with a special focus on student mobility, collaboration in research and security of science," a spokesperson for France Universités told *The PIE* News.

Read the full article here.

AUSTRALIA'S OBSESSION WITH FOREIGN INTERFERENCE IS A THREAT TO ITS ACADEMY

Brendan Walker-Munro | Times Higher Education | September 23, 2024

The news in Australia has recently been full of the government's efforts to double down on dealing with foreign interference, including at universities. In May, for instance, a Chinese PhD candidate was refused a student visa for alleged involvement in development of weapons of mass destruction because of his research on drones. In July, the government announced an expansion of the Countering Foreign Interference Taskforce, as well as new powers to expel suspected foreign agents. Then in August, UNSW-Canberra – the university collocated with the Australian Defence Force Academy – was accused of blacklisting Chinese academics. Chris Taylor, an analyst at the Australian Strategic Policy Institute, says all this is just evidence of a "bipartisan, prioritised approach" by the Australian government. That is certainly true. The previous government made foreign interference a serious crime, ranking up there with espionage, treason and terrorism. And our security agencies have been trumpeting the threat posed by foreign interference – from enemies and friends alike.

Read the full article here.

TAIWAN AND US TO DEEPEN COOPERATION IN SCIENTIFIC INNOVATION

Taiwan Today | April 10, 2024

National Science and Technology Council Minister Wu Tsung-tsong received a delegation from the U.S. National Science Foundation April 8 in Taipei City, underscoring the commitment to deepening collaboration in technological innovation that the two sides share. Led by Carol Bessel, section head of the Directorate for Technology, Innovation and Partnerships (TIP) under the NSF, other prominent members of the group included Samir Iqbal, director of the foundation's partnerships for innovation program. According to the NSTC, a science and technology agreement was inked between Taiwan and the U.S. in December 2020. The delegation's visit this month followed a recent high-level policy dialogue held in Taiwan on science and technology. During his welcome speech, Wu said that the common mission of both NSTC and NSF encompassed supporting academic research, technology transfer and innovation. Wu also pointed out that in recent years, generative artificial intelligence has revolutionized industries and led to successful startups in both countries.

Read the full article here.

UK, US AND CANADA TO COLLABORATE ON AI AND CYBER SECURITY

Lis Evenstad | Computer Weekly.com | September 23, 2024

The UK government has signed a collaboration agreement with the US and Canada, which will see the countries work together to leverage new artificial intelligence (AI) and cyber security technologies. The Ministry of Defence's (MoD) Defence and Science Technology Laboratory (DSTL) will lead the work in the UK, while the US Defence Advanced Research Projects Agency (DARPA) and Defence and Research Development Canada (DRDC) will manage the work in their respective countries. The countries will jointly research, develop, test and evaluate new technologies for AI, cyber and information domain-related technologies. MoD Science and technology director Nick Joad said that international research collaborations with US and Canada are "some of our most vital and enduring partnerships", adding: "This agreement cements our collective commitments to advancing emerging cyber security technologies such as cyber security and AI to enhance the defence and security of our nations."

Read the full article here.

FINAL U.S. MISCONDUCT RULE DROPS CONTROVERSIAL CHANGES

Jeffrey Mervins | Science | September 13, 2024

The U.S. agency that investigates research misconduct by federally funded biomedical scientists has dropped a controversial proposal that would have allowed it to publicize previously undisclosed misconduct findings by universities. In announcing the first revision of its research misconduct policy in 20 years, the federal Office of Research Integrity (ORI) said it removed the draft provision in response to complaints from many institutions about "regulatory overreach" and possible "breaches of confidentiality." ORI also:

- dropped a proposed 30-day deadline for starting an inquiry after an institution first receives an allegation of possible misconduct;
- restored a university's ability to forgo a full investigation if it decides the conduct was the result of "honest error"; and
- withdrew a requirement that institutions record and transcribe all statements obtained during an initial review of the allegations.

Read the full article here.

CHINA IS CHURNING OUT AI RESEARCH BUT 'DECOUPLED' FROM GLOBAL NETWORKS, REPORT FINDS

Ling Xin | South China Morning Post | September 26, 2024

China's artificial intelligence research output is rising rapidly but remains relatively "decoupled" from US-led global collaboration networks, a report by the Nature Index has found. Six of the top 10 "rising institutions" in the field from 2019 to 2023 were in China, according to the latest AI index, compiled by part of the group which owns the British journal Nature. However, China's global contectivity is lagging behind the US – the leading AI Nation which also plays central role to international collaboration - as well as Britain and Germany.

Read the full article here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute

IRANIAN CYBER ACTORS TARGETING PERSONAL ACCOUNTS TO SUPPORT OPERATIONS

National Cyber Security Centre | September 27, 2024

The Federal Bureau of Investigation (FBI), U.S. Cyber Command - Cyber National Mission Force (CNMF), the Department of the Treasury (Treasury), and the United Kingdom's National Cyber Security Centre (NCSC) are disseminating this joint Cybersecurity Advisory (CSA) to highlight continued malicious cyber activity by cyber actors working on behalf of the Iranian Government's Islamic Revolutionary Guard Corps (IRGC1). This IRGC cyber activity is targeted against individuals with a nexus to Iranian and Middle Eastern affairs; such as current or former senior government officials, senior think tank personnel, journalists, activists, and lobbyists. Additionally, FBI has observed these actors targeting persons associated with US political campaign activity, likely in support of information operations.

View the full resource here.

INSIDER THREAT GUIDE

National Counterintelligence and Security Center | September 26, 2024

The National Insider Threat Task Force (NITTF) published its "Guide to Accompany the National Insider Threat Policy and Minimum Standards" to orient U.S. Government departments and agencies to the various concepts and requirements embedded within the national program. Of course, the threat landscape continually evolves as technology rapidly shifts and organizations change in response to various pressures. Thus, the insider threat mission is a dynamic effort requiring constant evaluation, fresh perspectives, and updated approaches. As a result, the NITTF has released the 2024 "Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards."

View the full resource here.

VIDEO CLIP: CHINESE INFLUENCE AT U.S. UNIVERSITIES AND NATIONAL SECURITY THREATS

C-Span | September 26, 2024

"Washington Times" National Security Editor Guy Taylor talked about the national security threats posed by China and a congressional report that asserts Beijing has exploited its ties with American universities and used U.S. government-funded research to advance its own military technology.

View the full resource here.