ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

January 12, 2022

OSTP RELEASES HIGHLY ANTICIPATED GUIDANCE ON NATIONAL SECURITY STRATEGY FOR FEDERALLY FUNDED RESEARCH

Kate Gallin Heffernan and Marylana Saadeh Helou | The National Law Review | January 7, 2022

On January 4, 2022, the White House Office of Science and Technology Policy (OSTP) issued the long-anticipated guidance for federal agencies to implement National Security Presidential Memorandum (NSPM)-33. Encouraging an approach that balances research security with continued scientific innovation, the guidance stresses consistency in requirements, transparency regarding those requirements, and collective responsibility among researchers, awardee institutions, and funding agencies in meeting those requirements. NSPM-33, published during the final week of the Trump administration, outlined steps the United States can take to protect intellectual capital, discourage research misappropriation, and ensure responsible management of taxpayer dollars while maintaining an open environment to foster research discoveries, collaborations, and innovation. The Biden administration endorsed the memorandum, and in August, OSTP announced that it was in the process of creating guidance for federal agencies to implement NSPM-33 "effectively, rigorously, and uniformly … in a way that protects the nation's interests in both security and openness." In recent years, federal agencies have devoted significant time and effort to combat the threat of undue foreign influence on federally funded research and the potential theft of U.S. intellectual property.

Read the full article here.

CHINA'S NEW AI GOVERNANCE INITIATIVES SHOULDN'T BE IGNORED

Matt Sheehan | Carnegie Endowment for International Peace | January 4, 2022

Over the past six months, the Chinese government has rolled out a series of policy documents and public pronouncements that are finally putting meat on the bone of the country's governance regime for artificial intelligence (AI). Given China's track record of leveraging AI for mass surveillance, it's tempting to view these initiatives as little more than a fig leaf to cover widespread abuses of human rights. But that response risks ignoring regulatory changes with major implications for global AI development and national security. Anyone who wants to compete against, cooperate with, or simply understand China's AI ecosystem must examine these moves closely. These recent initiatives show the emergence of three different approaches to AI governance, each championed by a different branch of the Chinese bureaucracy, and each at a different level of maturity. Their backers also pack very different bureaucratic punches. It's worth examining the three approaches and their backers, along with how they will both complement and compete with each other, to better understand where China's AI governance is heading.

Read the full article here.

CHINA: THE CIVIL-MILITARY CHALLENGE

Anthony H. Cordesman and Grace Hwang | Center for Strategic and International Studies
January 4, 2022

There is no simple way to address the complex changes that China's growing strategic presence and military capabilities pose in competing with the United States and other states. It is clear, however, that China's capabilities to compete have increased radically in virtually every civil and military area since 1980, and that China has set broad goals for achieving strategic parity and superiority in the future – although its timeframes and definitions of such goals are vague. The end result is that the United States adopted a new National Security Strategy in 2017 and a new National Defense Strategy in 2018 that both focused on China as an emerging peer threat to the U.S. and as a central focus of its strategy. The Biden administration has not issued revised versions of these documents, but its FY2021 budget submission as well as the testimony of senior U.S. officials to Congress on U.S. strategy and force plans make it clear that China is now a central focus of the Biden administration's national security planning efforts. This report is a revised and greatly expanded version of Volume One of a two-part e-book that helps to explain these shifts in China's strategic position and the reasons why major changes are needed in U.S. strategy.

Read the full article here.

BEIJING'S 'RE-INNOVATION' STRATEGY IS KEY ELEMENT OF U.S.-CHINA COMPETITION

Emily Weinstein | Brookings | January 6, 2022

It wasn't long ago that many U.S. government officials and China experts still clung to the idea that Chinese innovation was mostly based on copying U.S. methods and technology. To some extent, they weren't entirely wrong. As the analyst Arthur Kroeber argues in China's Economy, Chinese firms are good at "adaptive innovation"—the concept of "taking existing products, services, or processes and modifying them to make them more receptive to China's economic and military needs." So when China's People's Liberation Army unveiled its J-20 stealth fighter in 2011, it caused an uproar in U.S. defense circles because of its similarity to American equivalents and seemed to confirm the perception of China as reliant on copying the work of others. Indeed, whether by theft or forced transfer, the acquisition of foreign intellectual property has served as a key component of China's technological forward march. However, the legal, illegal, and extralegal appropriation of foreign technologies and products is only one part of the story. In fact, the Chinese government has been pushing its tech industry to move beyond copycat methods. Beijing has also leveraged overseas technology and knowledge—in conjunction with supporting reforms—to bolster its own innovation capabilities and adapt them to fit within the Chinese model.

Read the full article here.

TRUSTED RESEARCH GUIDANCE FOR ACADEMIA

Center for the Protection of National Infrastructure | January 4, 2022

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.

Read the full article here.

US COUNTERINTELLIGENCE SHARES TIPS TO BLOCK SPYWARE ATTACKS

Sergiu Gatlan | BleepingComputer | January 7, 2022

The US National Counterintelligence and Security Center (NCSC) and the Department of State have jointly published guidance on defending against attacks using commercial surveillance tools. Tips shared in the joint advisory are designed to help people at risk of being targeted by surveillance campaigns block attempts to track their location, record their conversations, and harvest their personal information and online activity using mercenary spyware deployed on their mobile devices. "Companies and individuals have been selling commercial surveillance tools to governments and other entities that have used them for malicious purposes," the two US government agencies said [PDF]. "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."

Read the full article here.

CONVICTED CHINESE SCIENTIST WAS RECRUITED BY BEIJING'S 'TALENTS' PROGRAM

Bill Gertz | The Washington Times | January 7, 2022

A Chinese scientist who pleaded guilty to U.S. economic espionage charges on Thursday was recruited by the Chinese government as part of a foreign spying program that recruited people with access to foreign trade secrets and technology sought by Beijing. Xiang Haitao, a former scientist with Monsanto, and permanent U.S. resident, was arrested in November 2019 upon returning to the United States after working in China and helping Beijing utilize a proprietary commercial U.S. technology system designed to increase farm output. After initially pleading not guilty to a federal indictment for economic spying, Xiang, 44, changed his plea to guilty in federal court in the Eastern District of Missouri in St. Louis. The plea agreement revealed Xiang was recruited by the Chinese Academy of Science, the Beijing government's science program, as part of a program called the Hundred Talents Program in 2016. The program, also sometimes known as the Thousand Talents Program, has produced scores of FBI investigations and prosecutions of more than a dozen Chinese nationals and Americans who U.S. investigators charge have been working secretly for China at American universities and research centers.

Read the full article here.

WHY ENDING THE JUSTICE DEPARTMENT'S "CHINA INITIATIVE" IS VITAL TO U.S. SECURITY

Michael German | Brennan Center for Justice | January 4, 2022

Chinese and Chinese-American scientists are increasingly fearful about working in the United States, according to a recent survey. The study, conducted by the Committee of 100 and the University of Arizona, revealed that over 50 percent of scientists of Chinese ancestry working in the United States, regardless of citizenship, fear they are under surveillance by the U.S. government. Many are reconsidering their plans to stay in the United States. This trepidation results from a cramped and distorted vision of national security on the part of the U.S. government, and it could not come at a worse time. The reverberating effects within the scientific community threaten to undermine the primacy of U.S. science and technology at a time when the pandemic and climate change have become predominant threats to Americans' health and prosperity.

Read the full article here.

HOW MANY CONFUCIUS INSTITUTES ARE IN THE UNITED STATES?

National Association of Scholars | January 6, 2022

This list, originally published in March 2018, will be updated periodically. If you know of additional Confucius Institutes that have opened or closed, please let us know at peterson@nas.org. Since 2004, the Chinese government has sponsored Confucius Institutes on college and university campuses around the world, providing teachers, textbooks, and operating funds. Until recently, an agency of the Chinese Ministry of Education, the Hanban, oversaw Confucius Institutes. In the wake of widespread criticism, the Chinese government has reorganized Confucius Institutes under a new organization, the Chinese International Education Foundation. In April 2017, the National Association of Scholars released Outsourced to China: Confucius Institutes and Soft Power in American Higher Education, a comprehensive report on the way the Chinese government infiltrates American colleges and universities to enhance its own image. At that time, we counted 103 Confucius Institutes in the United States. As of January 6, 2022, NAS counts a total of 27 Confucius Institutes in the United States.

Read the full article here.

EUROPE NEEDS TO UNDERSTAND CHINESE RESEARCH – OR RISKS BEING EXPLOITED

David Matthews | Science|Business | January 6, 2022

The EU urgently needs better intelligence about China's science and technology system to avoid being taken advantage of, warns a new report, the latest sign of European anxiety that it lacks a deep understanding of the country. There is an information "asymmetry" between China, which has a long-standing global network on the lookout for foreign technology, and Europe, which only recently woke up to the fact that China might be a technological rival, according to the Berlin-based Mercator Institute for China Studies (MERICS). "It's quite a fragmented picture across Europe," said Rebecca Arcesati, an author of the report. "That stands in contrast with China's investment in information collection which supports the state's efforts to acquire foreign technology and knowledge." Attempts to hammer out a roadmap between Brussels and Beijing that would set the terms of research cooperation remain stalled, although negotiations are continuing, with a new meeting planned for late spring. The report cites a string of scandals in Denmark where academics collaborated on sensitive Chinese research without apparently realising their mistake.

Read the full article here.

A CHINESE SCIENTIST IN MISSOURI ADMITTED STEALING A SECRET ALGORITHM FROM MONSANTO TO PASS TO BEIJING

Bill Bostock | Insider | January 7, 2022

A Chinese scientist has admitted stealing trade secrets from the agrochemical giant Monsanto, the Justice Department said Thursday. Xiang Haitao, 44, worked as an imaging scientist for Monsanto in Missouri between 2008 and 2017, during which time Monsanto and its subsidiary The Climate Corporation worked on a secret algorithm known as the "Nutrient Optimizer," the department said, citing court documents. The algorithm helped farmers their productivity, the DOJ said. Before leaving the company, Xiang downloaded a copy of the algorithm, and then flew to China on a one-way ticket, the department said. Law-enforcement officers searched Xiang's electronics at the airport, but he was ultimately allowed to leave the US, the department said. Investigators later concluded that "one of Xiang's electronic devices contained copies of the Nutrient Optimizer," the DOJ said. US law-enforcement officials were able to arrest Xiang after he returned to the US sometime between 2017 and 2019, the department said.

Read the full article here.

PROTECT YOURSELF: COMMERCIAL SURVEILLANCE TOOLS

National Counterintelligence and Security Center | January 7, 2022

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. These surveillance tools can record audio, including phone calls; track phone's location; access and retrieve virtually all content on a phone, including text messages, files, chats, commercial messaging app content, contacts, and browsing history. Following are common cybersecurity practices that may mitigate some risks.

Read the full article here.

ACADEMIC COOPERATION AND GEOPOLITICS IN A NEW WORLD

Thomas Jorgensen | University World News | January 6, 2022

In recent years, growing geopolitical tensions have led to a reconsideration of international academic cooperation. As a result, the relationships that universities forge around the world have come under the spotlight. In the United States, Chinese espionage has become a prominent topic, while in the European Union the quest for strategic and technological sovereignty has cast doubt on even cooperation with very close partners such as the United Kingdom and Switzerland. The new situation requires new responses from higher education institutions and policy-makers alike. There is, and remains, a broad consensus in Europe that international cooperation strengthens the quality of university missions and society's knowledge base in general. The current discussion, however, revolves around how much cooperation leads to dependence, particularly on technologies that are seen as strategically important. There are also concerns about how partners use technology in systems that do not share Europe's civic values, with issues concerning mass surveillance and social control being particularly controversial in the European debate.

Read the full article here.