ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

January 18, 2023

WITH F.B.I. SEARCH, U.S. ESCALATES GLOBAL FIGHT OVER CHINESE POLICE OUTPOSTS

Megha Rajagopalan and William K. Rashbaum | The New York Times | January 12, 2023

Beijing says the outposts aren't doing police work, but Chinese state media reports say they "collect intelligence" and solve crimes far outside their jurisdiction. The nondescript, six-story office building on a busy street in New York's Chinatown lists several mundane businesses on its lobby directory, including an engineering company, an acupuncturist and an accounting firm. A more remarkable enterprise, on the third floor, is unlisted: a Chinese outpost suspected of conducting police operations without jurisdiction or diplomatic approval — one of more than 100 such outfits around the world that are unnerving diplomats and intelligence agents. F.B.I. counterintelligence agents searched the building last fall as part of a criminal investigation being conducted with the U.S. attorney's office in Brooklyn, according to people with knowledge of the inquiry. The search represents an escalation in a global dispute over China's efforts to police its diaspora far beyond its borders. Irish, Canadian and Dutch officials have called for China to shut down police operations in their countries.

Read the full article here.

RUSSIAN HACKERS PEPORTEDLY TARGETED US NUCLEAR RESEARCH LABS: HERE'S HOW THEY TRIED TRICKING SCIENTISTS

Bidhu Pattnaik | Yahoo Finance | January 7, 2023

A group of Russian hackers reportedly targeted three U.S. nuclear research laboratories in the summer of 2022. The Russian group Cold River carried out a phishing campaign against scientists at the Brookhaven, Argonne, and Lawrence Livermore National Laboratories to obtain passwords, Reuters reports. According to the report, hackers created fake login pages for the laboratories and contacted nuclear scientists to try to trick them into revealing their passwords. "This is one of the most important hacking groups you've never heard of," Reuters quoted Adam Meyers, senior vice president of intelligence at U.S. cybersecurity firm CrowdStrike saying. "They are involved in directly supporting Kremlin information operations." Cold River hacked into and leaked emails belonging to the former head of Britain's MI6 spy service in 2022 and targeted Britain's foreign ministry in 2016. The hacking team has been involved in many other high-profile hacking incidents. According to Reuters, western officials say the Russian government is a global leader in hacking and uses cyber espionage to spy on foreign governments and industries to seek a competitive advantage.

Read the full article here.

SHOULD DEMOCRACIES DRAW REDLINES AROUND RESEARCH COLLABORATION WITH CHINA?

Jeffrey Stoff | Center for Research Security & Integrity | 2023

Global research collaboration in scientific and engineering fields has been critical to advancing the frontiers of knowledge, promoting economic prosperity, and solving global challenges. The global research enterprise is, by design, largely open and unrestricted. However, new risks and challenges threaten this open collaboration, particularly regarding authoritarian nations like the People's Republic of China (PRC) and Russia. The Russian invasion of Ukraine – with China's economic and probable military support – and the ever-growing possibility of China attempting to take Taiwan by military force have real implications for allied democracies. As US President Biden stated in the 2022 National Security Strategy, "the PRC is the only country with both the intent to reshape the international order, and increasingly, the economic, diplomatic, military, and technological power to do so."

Read the full article here.

'UNBELIEVABLY RIDICULOUS': FOUR-STAR GENERAL SEEKS TO CLEAN UP PENTAGON'S CLASSIFICATION PROCESS

Aaron Mehta | Defense News | January 29, 2020

Gen. John Hyten, vice chairman of the Joint Chiefs of Staff, said Wednesday that he hopes to see "significant improvement" this year on loosening classification standards in the infamously overclassified Pentagon. Hyten said the process, which has the backing of Defense Secretary Mark Esper and Chairman of the Joint Chiefs of Staff Gen. Mark Milley, will attempt to make it easier to communicate with industry, the public and internally at the Defense Department. "In many cases in the department, we're just so overclassified it's ridiculous, just unbelievably ridiculous," Hyten told the audience at an Air Force Association event. To underline his point, Hyten said when he was head of U.S. Strategic Command, he invited Adm. Harry Harris, then the head of U.S. Pacific Command, to a briefing — one so classified that their deputy commanders, both three-star officers, were not allowed to attend. If "the only people in the room are four-stars, you really can't get any work done," he noted.

Read the full article here.

THE CHINA-US QUANTUM RACE

Sam Howell | The Diplomat | January 13, 2023

Quantum researchers in China claim to have an algorithm capable of breaking public-key encryption, years before anyone expected. Accurate or not, the announcement serves as a reminder that surprising quantum breakthroughs are possible in the near term. If the Biden administration is serious about its designation of quantum information science (QIS) as a critical technology area for national security, it must do more to safeguard U.S. quantum superiority. QIS uses the laws of quantum physics, which describes the properties of nature on a tiny scale, to advance the processing, analysis, and transmission of information. Quantum computing, quantum encryption, and quantum sensing constitute the three primary domains within QIS. Although it is an evolving field, QIS promises to transform almost any industry dependent on speed and processing power, from aerospace and automotive to finance and pharmaceuticals. Like other emerging technologies, quantum has become a crux of China-U.S. competition. The first country to operationalize quantum technologies will possess a toolkit of capabilities that can overwhelm unprepared adversaries. Quantum-enabled countries could crack existing encryption methods, build unbreakable encrypted communications networks, and develop the world's most precise sensors.

Read the full article here.

HOW THE DECADES-LONG CHINESE ESPIONAGE CAMPAIGN "STOLE" US MILITARY TECHNOLOGY

Kris Osborn | Warrior Maven | December 7, 2022

Paradigm-changing deep-penetrating warheads, new hardened, heat resistant nano-composite materials enabling hypersonic weapons flight, vertical take-off-and-landing drones and a new generation of submarine "quieting" technologies are all massively impactful breakthrough technology of vital significance to cutting-edge and future US weapons systems. All of these areas of innovation and scientific exploration, some of which involved the discovery and development of "disruptive" or breakthrough technologies, were heavily focused upon in recent decades at the well known, prestigious US Los Alamos National Laboratory. However, to put things simply and clearly, many of the US-driven technological advances in these critical areas appear to have been stolen by Chinese spies. Technologically driven Chinese espionage at Los Alamos hit the news in a very public way earlier this year, following a private counterintelligence investigation. The discoveries shined additional light on the concerning and well-documented problems arising from Chinese cyber attacks, espionage and deliberate efforts to "steal" sensitive US military technology.

Read the full article here.

HOW CHINA FUNDS FOREIGN INFLUENCE CAMPAIGNS

Digital Forensic Research Lab | January 12, 2023

A review of financial records for Chinese Communist Party (CCP) organizations with foreign influence capabilities reveals that funding for propaganda activities in China is largely project based, with most of the financing comes from public funds. CCP organizations release public financial reports that can be analyzed to understand China's priorities when it comes to information operations. The DFRLab dissected the financials of two Chinese media organizations and two municipal-level CCP departments to reveal insights into the funding of foreign influence campaigns. Our examination included the financial records for Xinhua News Agency, China Media Group (CMG), the Beijing United Front Work Department (UFWD), and the Beijing Propaganda Department. Xinhua's foreign media operations have operated at a loss since the pandemic began, yet the work is still supported by the news agency because of its strategic importance. Xinhua sees itself as being engaged in a global "public opinion war" in which it is fighting offensively.

Read the full article here.

SWISS UNIVERSITIES ON GUARD AGAINST CHINESE ESPIONAGE

SWI Swissinfo | December 26, 2022

The suspicion that Chinese researchers pass on information from the Western scientific world to Beijing has led some Swiss universities to strengthen their cooperation with Switzerland's Federal Intelligence Service, according to the Swiss weekly. Others have scrapped research collaboration efforts. The Chinese law on intelligence clearly states that all citizens must cooperate with the national intelligence service, the newspaper noted. And the researchers most loyal to Beijing typically benefit from grants for stays abroad. "China has two strategies," said Jean-Marc Rickli, director of global and emerging risks at the Geneva Centre for Security Policy in a recent interview with Swiss public broadcaster RTS. "In the field of humanities and social sciences, it is to help develop a narrative that is pro-Chinese. And in the field of engineering, it is much more based on capturing knowledge in order to transfer it to China." His assessment of what drives Beijing's interest in Swiss universities draws on the findings of two reports published in 2021 by French. The technological rivalry between the United States and China puts Swiss institutions in an uncomfortable position.

Read the full article here.

HOW U.S. SCIENTISTS ARE COLLABORATING WITH CHINA'S MILITARY: 'WAKE-UP CALL'

Didi Kirsten Tatlow | Newsweek | January 11, 2023

Work on a robotic fish with potential military use was just one of hundreds of examples of collaboration between scientists in the U.S. and its allies and researchers linked to China's military, according to a new study seen by Newsweek. The study, which focuses primarily on scientists in key U.S. NATO ally Germany, reveals a scale of collaboration between scientific institutions in the West and researchers connected with China's military that is far greater than has previously been reported. The release of the report, shared exclusively with Newsweek ahead of its publication in Washington D.C., comes at a time of growing tension between the U.S. and China, with President Joe Biden's administration singling out China as America's key competitor and taking more steps to limit technology transfer. The scientific establishment has been slow to react to the changing times, said Jeffrey Stoff, author of the report "Should Democracies Draw Redlines around Research Collaboration with China?", which assessed 43,000 papers published between 2016 and May 2022, with about one sixth of those studies having a U.S. co-author.

Read the full article here.

ARMY TO IMPLEMENT NEW CYBERSECURITY APPROACH TO SAFEGUARD NETWORK

Doug Graham | U.S. Army | January 10, 2023

Although it sounds counter-intuitive, implementing zero trust principles is the pathway to ensuring that the Army's data and communications network will be a trustworthy pillar supporting Army modernization, according to network cybersecurity experts across the service. During last month's Technical Exchange Meeting (TEM) 9 in Nashville, which convened industry and government experts to discuss current and future Army data and communications capabilities, the Army and Department of Defense amplified the adoption of zero trust architecture to continuously authenticate, authorize and validate users to access applications and data. This lack of assumed "trust" makes hacking into a zero-trust system more difficult than periphery cyber defense systems, which confine authentication to those seeking entry into the network, experts said. Zero trust systems do not stop at policing entry. They insert security checks throughout the entire system, through tagging the data itself, to verification of interactions and insisting on identification and verification of every part of the network including individuals and devices such as computers, servers, printers, phones and radios.

Read the full article here.

UNDERSTANDING OPSEC - THE OPSEC CYCLE

National Counterintelligence and Security Center | January 2023

Operations Security (OPSEC) isn't rocket science, nor should it be. Most of us apply OPSEC principles in our daily lives without realizing it. Whenever an individual identifies personal information that needs to be protected in order to limit risk, they are practicing OPSEC. Not sharing Social Security numbers or other personally identifiable information (PII) — knowing adversaries can use this data to commit identity theft — is common sense, but it is also the first step of the OPSEC Cycle. The threat of information loss/compromise can also be applied to departments/agencies, businesses, corporations, and any other organization, thereby compelling the need to implement the OPSEC Cycle and a robust OPSEC program. As detailed below, the first step in the OPSEC Cycle involves identifying critical information. Critical information is that which you determine is important to your organization, and if exposed, could be useful by itself or in aggregate to a known or unknown adversary.

Read the full article here.

SCIENTISTS AREN'T TRAINED TO MENTOR. THAT'S A PROBLEM

Adam Ruben | Science | August 31, 2020

Throughout most of grad school, I was impressed by how thoroughly unimportant I was to the people running the labs I worked in. I didn't expect to have best-buds-on-a-road-trip relationships with my advisers, but I didn't realize I'd pretty much be thought of as Training Grant Expenditure Number Eight. Day one in a lab usually felt like this: ME: My mind is open; I am yours to educate! Illuminate the corridors of scientific wonder, and be my true guide as you train me in your ways. MY ADVISER: Here's a stack of journal articles. See you in a week. Yet that's what an adviser is, at least etymologically: someone who provides advice. Not guidance, not teaching, just … advice. In other words, we sometimes draw a false equivalence between research advisers and mentors. And while many advisers are excellent mentors, it's not exactly a prerequisite for running a lab. But it doesn't have to be that way. Back in the days when traveling and audiences both existed, I gave the keynote address at an event for HSI STEM Impact, a program for undergraduate science students at Texas State University.

Read the full article here.

THE PLA'S PEOPLE PROBLEM

Taylor A. Lee and Peter W. Singer | Defense One | January 11, 2023

Too much Western analysis and debate about China's impressive military buildup focuses on its equipment and weapons, and too little on its people. Yet personnel recruiting, training, and retention issues might be exactly what holds China back in the "marathon" it is racing against the United States. For instance, the Defense Department's annual China Military Power Report goes into considerable detail about the PLA's new equipment, but makes almost no mention of personnel. The same is true of congressional testimony by government and non-government officials, as well as statements by politicians everywhere from the hearing room to cable news. And like those who expected a swift Russian victory in Ukraine, the new cottage industry of think tank reports and wargames on a potential Taiwan war count ships, planes, and tanks, while spending less time on the skill and will of the people in them. The PLA has long struggled to field quality personnel. In its early years, most personnel were illiterate, including officers. (This mirrored even the most senior CCP political leaders; for instance, Chen Yonggui rose to Vice Premier despite not being able to read.)

Read the full article here.

THOUSANDS OF SCIENTISTS PUBLISH A PAPER EVERY FIVE DAYS

John P. A. Ioannidis, Richard Klavans, and Kevin W. Boyack | Nature | September 12, 2018

Authorship is the coin of scholarship — and some researchers are minting a lot. We searched Scopus for authors who had published more than 72 papers (the equivalent of one paper every 5 days) in any one calendar year between 2000 and 2016, a figure that many would consider implausibly prolific1. We found more than 9,000 individuals, and made every effort to count only 'full papers' — articles, conference papers, substantive comments and reviews — not editorials, letters to the editor and the like. We hoped that this could be a useful exercise in understanding what scientific authorship means. We must be clear: we have no evidence that these authors are doing anything inappropriate. Some scientists who are members of large consortia could meet the criteria for authorship on a very high volume of papers. Our findings suggest that some fields or research teams have operationalized their own definitions of what authorship means. The vast majority of hyperprolific authors (7,888 author records, 86%) published in physics. In high-energy and particle physics, projects are done by large international teams that can have upwards of 1,000 members. All participants are listed as authors as a mark of membership of the team, not for writing or revising the papers.

Read the full article here.

THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Safeguarding Our Future:

Secure America's Future In Quantum: Protect Your Research

Safeguarding Science:

An Outreach Initiative for Protecting Research and Innovation in Emerging Technologies

THE TEXAS A&M UNIVERSITY SYSTEM

The Academic Security and Counter Exploitation Program is coordinated by The Texas A&M University System Research Security Office as a service to the academic community.
https://rso.tamus.edu