ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

August 31, 2023

CHINESE SPY TARGETED THOUSANDS OVER LINKEDIN

Gordon Corera | BBC News | August 23, 2023

The Times said that the spy worked for Beijing's Ministry of State Security and used a series of false names. The MI5 has previously warned that spies are using LinkedIn to target those with access to confidential information. The Chinese Embassy has been contacted for comment. A parliamentary report also warned that the aim was sometimes to lure people to China and then compromise them. The alleged spy is said to have used several names over a period of five years. The most prominent used was Robin Zhang. During that time it is claimed he offered British and other officials business opportunities, with an endgame of gaining sensitive information from them. He is also said to have offered a recruitment consultant up to £8,000 each time they handed over details of someone who worked for the intelligence services. Some of the targets were said to have been offered trips to China and paid speaking engagements. Others were asked to provide reports, which the alleged spy would then use to request more confidential documents with the aim of entrapment.

Read the full article here.

WHY LINKEDIN IS A SNOOPER'S PARADISE

Gareth Corfield | The Telegraph | August 24, 2023

Sitting in a Hong Kong hotel room as a handwritten non-disclosure agreement was thrust under his chin, Gawain Towler realised that answering a LinkedIn invitation from a Chinese "businessman" may have been a mistake. "I chatted to them and I thought it's totally legit," the former director of communications for Nigel Farage's UK Independence Party says, recalling the first message he received on the networking site in March 2018. Towler thought he was being courted for lucrative consulting work for a Chinese company hoping to expand into the UK. Yet the job was not legitimate. The approach was part of a years-long espionage effort aimed at recruiting influential and senior Britons to spy for Beijing. Towler was given a phone and instructions for how to covertly share documents through Instagram using a custom app. He made his excuses and left, alerting the security services when he returned to Britain. The use of LinkedIn as a major tool of China's espionage efforts has been laid bare this week, with an account under the name of Robin Zhang unmasked as part of a far-reaching state intelligence-gathering effort suspected of targeting thousands of Westerners.

Read the full article here.

GLOBAL TENSION IS SEVERING DEEP RESEARCH TIES BETWEEN THE US AND CHINA

Karen Hao and Sha Hua | The Australian | August 22, 2023

One of the most productive scientific collaborations of the 21st century is pulling apart, as deteriorating relations between the US and China lead researchers to sever ties. The decoupling, which began in recent years with investigations into Chinese researchers in the US, has accelerated as tensions have risen between the superpowers.

Read the full article here.

US EXTENDS SCIENCE PACT WITH CHINA: WHAT IT MEANS FOR RESEARCH

Natasha Gilbert and Gemma Conroy | Nature | August 25, 2023

The US government has extended for six months a key symbolic agreement to cooperate with China in science and technology. The agreement was due to expire on 27 August, and its short-term extension has revived researchers' hopes that the 44-year-old pact will continue. The pact does not provide research funding. Rather, it is an umbrella agreement to encourage collaboration and goodwill between US and Chinese government agencies, universities and institutions doing research in agriculture, energy, health, the environment and other fields. The extension means that, for now, research will continue as normal. The non-binding agreement was first signed in 1979 and has since been renewed every five years. The new extension stops short of a full renewal, which some scientists worry is now in jeopardy. Without the agreement, research cooperation and programmes between the two governments could flounder, some specialists warn. The extension "is not as good as a renewal", says Denis Simon, a researcher in global business and technology at the University of North Carolina at Chapel Hill. "But it's a good start. It says the US wants to stay connected."

Read the full article here.

FINDING SAFE HARBORS FOR DEVELOPMENT IMPACT: NAVIGATING U.S.-CHINA STORMY WATERS FOR THE GLOBAL PUBLIC GOOD

Steve Davis | Center for Strategic and International Studies | August 23, 2023

As intense geostrategic rivalry becomes an enduring feature of the U.S.-China relationship, CSIS and the Brookings Institution have launched a joint project, Advancing Collaboration in an Era of Strategic Competition, to explore and expand the space for U.S.-China collaboration on matters of shared concern. This essay, by the chair of the project's advisory council, argues that game-changing opportunities for social impact across health, climate change, and food security are within reach—but will depend on new mechanisms and narratives that enable collaborations between partners in the United States and China to proceed in smart, informed, and geopolitically sensitive ways. In West Africa, a new breed of rice that can withstand flooding and drought has allowed farmers to triple their productivity, improving local economies and feeding thousands of people. In regions from South America to Scotland, new green technologies are generating an abundance of clean energy.

Read the full article here.

NEW PRC RESTRICTIONS ON DATA SHARING

Intersections | August 2023

A major regulatory trend in China in recent years has been Beijing's effort to exercise increasingly stringent control over what information leaves China, and over the information handled by corporate experts and consultants inside China. As of this year, the PRC government's updated counter-espionage law defines much of this corporate data as sensitive, and those who share it overseas are increasingly at risk of penalties. This section covers two actions by Beijing that are part of its effort to restrict outbound information flows: raids on corporate due diligence firms inside the PRC, notably the consulting firm Capvision, and limiting access from outside China to widely used corporate and academic databases. PRC firm Capvision raided by PRC authorities for allegedly providing "state secrets" to foreign clients. In May 2023, PRC authorities conducted a raid against international consulting firm Capvision, which specializes in connecting international investors with in-country experts on Chinese companies and markets. During the raid, authorities questioned staff and announced that they would open investigations into both the company and specific personnel.

Read the full article here.

FEDS PUT CYBERSECURITY FOR AI, QUANTUM COMPUTING IN THE SPOTLIGHT

Tim Starks and David DiMolfetta / Washington Post | August 22, 2023

A trio of government agencies on Monday urged organizations to prepare now for quantum computers' ability to break through encryption, telling them to develop a "road map" for a future that grows near. The government message follows closely behind another from last week, with an agency saying artificial-intelligence software should be made "secure by design" — that is, developed with security as a core feature. Together, the guidance represents two ways that feds are grappling with the cybersecurity ramifications of emerging technology. Their efforts include the recent launch of an AI cybersecurity challenge and internal goals for agencies to prepare for post-quantum cryptography. The Cybersecurity and Infrastructure Security Agency, the National Security Agency, and the National Institute of Standards and Technology published a quantum "factsheet" on Monday.

Read the full article here.

NSF SEEKS TO TACKLE FOREIGN PARTNERSHIP FEARS

Paul Basken | Times Higher Education | August 23, 2023

The US National Science Foundation is making a concerted effort to resolve high-stakes debates over US research security by creating a formal network of scientists to study the best ways of handling the problem. As both Republicans and Democrats in the US grow increasingly antagonistic towards China and other countries they regard with suspicion, the NSF initiative aims to precisely identify and study the threat to the US from foreign misuse of the nation's research enterprise. "At NSF, we're very data-driven," Rebecca Keiser, the NSF's chief of research security strategy and policy, said in announcing the plan. "And so what we wanted to do was explore what was occurring here." The idea follows years of rising complaints from politicians and national security officials aimed at the US research community over perceptions that Chinese partners are stealing ideas of economic and military value. University leaders generally have acknowledged the concern but argued that the collaborations provide the US with a net benefit.

Read the full article here.

NIST EXPANDS CYBERSECURITY FRAMEWORK WITH NEW PILLAR

Phil Muncaster | Infosecurity Magazine | August 10, 2023

The US National Institute of Standards and Technology (NIST) has released a new draft version of its popular best practice security framework, designed to expand its scope and provide more guidance on implementation. The NIST Cybersecurity Framework (CSF) 2.0 is the first refresh since it was launched in 2014. It is designed to help organizations "understand, reduce and communicate about cybersecurity risk," the standards body said. "With this update, we are trying to reflect current usage of the Cybersecurity Framework, and to anticipate future usage as well," said the framework's lead developer, Cherilyn Pascoe. "The CSF was developed for critical infrastructure like the banking and energy industries, but it has proved useful everywhere from schools and small businesses to local and foreign governments. We want to make sure that it is a tool that's useful to all sectors, not just those designated as critical."

Read the full article here.

CHINA WANTS TO RUN YOUR INTERNET

Edoardo Campanella and John Haigh | Foreign Policy | August 25, 2023

For the last two centuries, great powers—both nations and their associated firms—have fiercely competed to set the technical standards for leading technologies. By imposing their preferred standards, nations not only solve technical problems to their advantage but they also project power globally. Standards determine what kind of technology will prevail in the future, ensuring market dominance to national champions, while forcing foreign competitors to adapt at hefty costs. As the industrialist Werner von Siemens reportedly put it: "He who owns the standards, owns the market." Given the broad ramifications of the internet, its governance represents the regulatory battleground of the future. The internet is heavily dependent on shared standards across multiple platforms that have evolved over decades to assure compatibility across hardware and software. These shared standards enable highly decentralized components developed by disparate parties to integrate into an effective overall system. Talking about the original vision of the internet, one of the inventors of its protocols, Vinton G. Cerf, argued that "universal connectivity among the willing was the default assumption."

Read the full article here.

CHINA'S SCIENTIFIC PAPERS: HEAVY ON QUANTITY, WEAK ON QUALITY

GreekCityTimes | August 2023

In the world, China ranks second after the US in its total investment in research and development, but the country's audit report has found a gaping hole in universities and research institutions' scientific papers and their real use. Most of them have been found to be involved in research work that has no use in industrial applications, an audit report recently carried out by the Audit Office of Guangxi said. The 15,000-word audit report which was, as per South China Morning Post, removed shortly after uploading on the website of the Audit Office of Guangxi, an autonomous region in southern China, has made a scathing attack on universities and their performance. Nine universities of the region could convert just less than 1% of their research work in science and technology —from 2020 to 2022---to industrial applications, the Hong Kong-based daily newspaper said, quoting a just released audit report.

Read the full article here.

INTERNATIONALISATION GUIDELINES: BONUS OR BURDEN FOR HE?

Jan Petter Myklebust | University World News | August 24, 2023

A Norwegian government report providing guidelines and advice to higher education and research institutions and aimed at safeguarding academic values and national interests against foreign intelligence and interference, digital security and illegal knowledge transfers has been launched in response to what is seen as a growing global challenge. The Directorate of Higher Education and Skills and the Norwegian Research Council delivered its report on regulations and tools for responsible international cooperation to the Ministry of Higher Education and Research on 14 August. "International higher education and research cooperation have over recent years become more demanding and the sector is facing the dilemma every day between openness and security, and they have been asking for more information and guidelines from us," said Minister of Research and Higher Education Sandra Borch at the launch of the guidelines held at the Arctic University of the North at the start of the university year.

Read the full article here.

GERMANY MUST ADAPT RESEARCH PRACTICES IN LIGHT OF CHINESE THREAT -MINISTER

Friederike Heine and Miranda Murray | Reuters | August 21, 2023

Germany must bring its academic practices in line with its security interests in light of tensions with systemic rivals such as China, the country's research minister wrote in an editorial published in the FAZ newspaper's Monday edition. Last month, the German government released its long-awaited China strategy with the goal of reducing critical dependencies on the country as it becomes increasingly assertive in attempts to change the rules-based international order. "We must not be naive in dealing with a regime that has the stated goal of converting civilian research into military applications and achieving dominance when it comes to critical technologies," Bettina Stark-Watzinger said. Research conducted in Germany must be better protected considering the risk of critical know-how reaching China and the country's possible use of civilian research for military purposes, the minister wrote.

Read the full article here.

HUGE CYBERATTACK DISABLES TELESCOPES IN HAWAII AND CHILE

Christopher McFadden | Interesting Engineering | August 26, 2023

A major cyberattack has shut down remote connections to prominent National Science Foundation (NSF) space telescopes worldwide, Science reports. Ten telescopes have been impacted for over two weeks now, with on-site operatives able to keep some operational, albeit less efficiently. The shutdowns are causing chaos in the astronomy sphere, with many essential windows of opportunity being missed for space observations. While incredibly frustrating for researchers relying on the telescopes, experts are still none the wiser about why the telescopes were targeted. "NOIRLab is continuing its efforts to diligently investigate and resolve the 1 August cybersecurity incident that occurred in its computer systems. This incident resulted in the temporary shutdown of Gemini North and South telescopes and some of the smaller telescopes on Cerro Tololo in Chile," explained NOIRLab (the NSF-run coordinating center for ground-based astronomy) in a press release update.

Read the full article here.

PROTECT YOURSELF: COMMERCIAL SURVEILLANCE TOOLS

The National Counterintelligence and Security Center

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.

Read the full article here.

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