ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

May 20, 2021

FOREIGN INTELLIGENCE ENTITIES' RECRUITMENT PLANS TARGET CLEARED ACADEMIA

Defense Counterintelligence and Security Agency | April 2021

Foreign Intelligence entities (FIE), specifically China and Russia, use academic talent recruitment plans and academic excellence initiatives to collect U.S. scientific research and technologies in a strategic effort to enhance their militaries and economies. China and Russia often utilize foreign students accepted to U.S. universities or at postgraduate research programs to collect sensitive U.S. Government information and/or technology. Additionally, Iran uses government-sponsored initiatives to persuade students studying abroad to return and share their knowledge. FIE target U.S. subject matter experts (SMEs), professors, and researchers in order to obtain sensitive U.S. Government information and technology.

Read the full report here.

IF WE DON'T SECURE PEOPLE, INFORMATION SECURITY WILL REMAIN A PIPE DREAM

Bill Priestap and Holden Triplett | Lawfare | May 14, 2021

As we've written previously on Lawfare, businesses are on the frontline of an intense geopolitical competition. Their assets—like innovative technologies, complex research and development, and data—are being targeted by nation-states. Many businesses have tried to address this risk by implementing or beefing up their information security programs. But those programs, unfortunately, provide only a partial solution. In the past few days, U.S. media have been in a frenzy about the Colonial Pipeline ransomware attack. It appears likely that many businesses will respond to the news in a purely technical manner. Chief information and security officers (CISOs) will be asked how secure their information technology systems are, and whether anything needs to be done to enhance cyber defenses. But if businesses seek to strengthen their defenses only through cybersecurity improvements, they will remain vulnerable to similar and different threats. This is because at the heart of every business's information security efforts is a flaw that few have addressed adequately: A business's people present the ultimate vulnerability. By virtue of their employment, employees have access to a business's most valuable assets. No sophisticated hack or stealing of credentials is necessary. Employees are already on the inside. And their access can easily be exploited by a sophisticated nation-state that is adept at surreptitiously manipulating people. Until employees are appropriately safeguarded, true information security is likely to remain just beyond reach.

Read the full article here.

CONGRESS'S FIXATION WITH CHINA'S 'MALIGN INFLUENCE' UNDERMINES AMERICANS' CIVIL LIBERTIES AND SECURITY

Jessica J. Lee and Rachel Esplin Odell | Responsible Statecraft | May 14, 2021

At a conference of Chinese Americans last week, former Washington governor and former U.S. Ambassador to China Gary Locke decried the way that "geopolitical tensions between the U.S. and China, coupled with overreaching U.S. policies" have created a hostile environment for people of Chinese descent in America. To counter these trends, he highlighted the important principle, "We make America great by celebrating our diversity, not by fearing it or demonizing it." Unfortunately, the Strategic Competition Act recently approved by the Senate Foreign Relations Committee and a related bill that may be marked up by the House Foreign Affairs Committee would do the opposite. Specifically, Sections 132, 133, and 136 of the SCA, which echo provisions in H.R. 2329 on "countering the Chinese Communist Party's malign influence," risk missing the bigger picture of influence operations emanating domestically and globally, as well as deepening paranoia and anger against Asian Americans by painting China's threat in broad strokes. There are at least four ways in which these bills would negatively affect U.S. interests.

Read the full article here.

UNIVERSITY RESEARCHER SENTENCED TO PRISON FOR LYING ON GRANT APPLICATIONS TO DEVELOP SCIENTIFIC EXPERTISE FOR CHINA

U.S. Department of Justice | May 14, 2021

An Ohio man and rheumatology professor and researcher with strong ties to China was sentenced to 37 months in prison for making false statements to federal authorities as part of an immunology research fraud scheme. As part of his sentence, Zheng was also ordered to pay more than $3.4 million in restitution to the National Institute of Health (NIH) and approximately $413,000 to The Ohio State University. Song Guo Zheng, 58, of Hilliard, was arrested Friday, May 22, 2020, after he arrived in Anchorage, Alaska, aboard a charter flight and as he prepared to board another charter flight in order to flee to China. He was carrying three large bags, one small suitcase and a briefcase containing two laptops, three cell phones, several USB drives, several silver bars, expired Chinese passports for his family, deeds for property in China and other items. He was transported to the Southern District of Ohio and made his first federal court appearance in Columbus last July.

Read the full article here.

COMMITTEES ADVANCE BILLS ADDRESSING RESEARCH COMPETITIVENESS, FOREIGN INFLUENCE

Christa Wagner | AAMC | May 14, 2021

Committees in both the House and Senate marked up and advanced legislation the week of May 10 to address the United States' global research competitiveness and foreign government influence in research. The Senate Committee on Commerce, Science, and Transportation amended the Endless Frontier Act (S. 1260) [refer to Washington Highlights, April 23] before approving the bill by a vote of 24-4. The bill aims to bolster the United States' global competitiveness, especially with China, through investments in innovation, technology, research and development, supply chains, and the STEM workforce. The committee approved an amendment in the nature of a substitute that was developed following bipartisan negotiations, and the committee adopted 53 of the more than 100 amendments considered during the markup.

Read the full article here.

FOSTERING INTERNATIONAL COLLABORATION WHILE MANAGING UNDUE FOREIGN INFLUENCE IN ACADEMIC RESEARCH

Anne Pifer, Roseann Luongo, and Amanda Gerfuson | Huron

As global collaboration increases and instances of questionable influence by foreign entities over federally funded research continue to surface, institutions are being called to enhance compliance programs to mitigate this evolving risk. While the concept of inappropriate conduct in research is not new, federal agency disclosure requirements have reinforced the definition of foreign influence and increased the severity with which noncompliance is prosecuted as institutions are held to higher standards of accountability and transparency. This intensified spotlight on compliance with shifting regulatory demands has created a complex and high-stakes environment in which failure to adhere to federal mandates may lead to formal inquiries and civil or even criminal charges.

Read the full article here.

SENATE REPUBLICANS: NSF CAN'T BE TRUSTED TO SAFEGUARD RESEARCH FROM CHINA

Ryan Lovelace | The Washington Times | May 12, 2021

Republican lawmakers pushing to keep tax dollars intended for scientists out of the hands of the Chinese government have taken their fight to the public. As the Senate debated what had been a bipartisan proposal by Majority Leader Charles E. Schumer to send billions to the National Science Foundation, Republicans balked, saying the agency cannot be trusted to safeguard government-funded research that in the past has been routinely compromised by China. Mr. Schumer's Endless Frontier Act that would route $100 billion to NSF had seven original Democratic co-sponsors and seven Republican co-sponsors, including Sen. Rob Portman of Ohio. But Mr. Portman said on Wednesday that he had reservations about continuing to support the bill because NSF "does very little to protect its research" from China. "They have no dedicated compliance officers, they depend on the [inspector general] to find grant fraud," he said at a committee meeting. "It doesn't prevent researchers it funds from participating in talent recruitment plans like the Thousand Talents Plan. More concerning, the head of NSF's office of international science and engineering testified before a subcommittee that she had only recently heard about the Thousand Talents Plan despite it being around for two decades."

Read the full article here.

REPUBLICANS TO INTRODUCE LEGISLATION CALLING FOR COLLEGES TO DISCLOSE FOREIGN INFLUENCE

Henry Rodgers and Marlo Safi | Daily Caller | May 12, 2021

Republican Alabama Rep. Mo Brooks will introduce legislation Wednesday calling for colleges and universities to disclose any foreign influence. The legislation, first obtained by the Daily Caller, requires colleges and universities to report any gifts from foreign countries and entities and for the schools to publicly disclose the names of all of their foreign donors. The bill also requires colleges and universities to list gift reasons and any gift conditions, as well as the department, college or project the money is supposed to go to. The bill is titled the Zero Foreign Influence in Education Act and targets large donations from U.S. "geopolitical foes," such as China. The bill points to Section 117 of the Higher Education Act, which requires universities to report gifts or contracts greater than $250,000 in a calendar year.

Read the full article here.

EVERYTHING YOU NEED TO KNOW ABOUT THE NEW EXECUTIVE ORDER ON CYBERSECURITY

Robert Chesney and Trey Herr | Lawfare | May 13, 2021

Yesterday evening, the Biden administration released its much-anticipated "Executive Order on Improving the Nation's Cybersecurity." It is tempting to yawn; every administration in recent memory has done something of this kind, after all, and not always to significant effect. But this executive order deserves your attention. It contains concrete measures tailored to respond to lessons learned from recent crises, especially the SolarWinds and Microsoft Exchange compromises. Is there more work to do? Obviously, yes. But to a significant extent that's a job for Congress. The question at the moment is whether the Biden administration with this executive order has made good use of the limited tools that it controls directly. As we explain below, the answer is largely yes.

Read the full article here.

SENATE PANEL BACKS FUNDING BAN ON U.S. RESEARCHERS IN CHINESE TALENT PROGRAMS

Jeffrey Mervis | Science | May 13, 2021

The U.S. Senate's commerce committee has voted to ban any U.S. scientist who participates in a Chinese-sponsored talent recruitment program from receiving or making use of federal funding. Yesterday's vote—just the first step toward making the provision law—represents a ratcheting up of current U.S. efforts to block the Chinese government from stealing or gaining improper access to federally funded research. The new restrictions are tucked into bipartisan legislation championed by Senate Majority Leader Chuck Schumer (D–NY), called the Endless Frontier Act (EFA), which would authorize massive budget increases for the National Science Foundation and research at the Department of Energy, and also give NSF a new technology directorate. The committee voted 24 to four to advance the latest version of the bill (S.1260), which could be headed to the Senate floor as soon as next week. A similar bill with the same restrictions is pending in the U.S. House of Representatives. The 340-page EFA is aimed at strengthening the country's ability to turn basic research into technologies essential for U.S. economic and national security.

Read the full article here.

STATEMENT FROM CISA ACTING DIRECTOR WALES ON EXECUTIVE ORDER TO IMPROVE THE NATION'S CYBERSECURITY AND PROTECT FEDERAL NETWORKS

Cybersecurity & Infrastructure Security Agency | May 13, 2021

Yesterday, President Biden signed an executive order to improve the nation's cybersecurity and protect federal government networks. Cybersecurity and Infrastructure Security Agency (CISA) Acting Director Brandon Wales released the following statement: "President Biden's executive order is an important step forward in bolstering our nation's cybersecurity. As last week's ransomware attack against the Colonial Pipeline and recent intrusions impacting federal agencies demonstrate, our nation faces constant cyber threats from nation states and criminal groups alike." "As the nation's lead agency for protecting the federal civilian government and critical infrastructure against cybersecurity threats, CISA serves a central role in implementing this executive order. This executive order will bolster our efforts to secure the federal government's networks, including by enabling greater visibility into cybersecurity threats, advancing incident response capabilities, and driving improvements in security practices for key information technology used by federal agencies.

Read the full article here.

HDIAC WEBINAR: DOD'S RESEARCH SECURITY AND S&T PROTECTION EFFORTS TO COUNTER FOREIGN INFLUENCE

Homeland Defense & Security Information Analysis Center | May 13, 2021

The United States faces evolving challenges to its military and technological dominance. Some of the most pressing challenges include rapid technological change, development and procurement issues, and great power competition from Russia and China. Preserving our technological advantage from unwanted diversion, exploitation, or transfer must also be balanced against the need for competitive, global talent activities to mitigate unwanted foreign influence and technology transfer. In this webinar, Mr. Gardner discusses how the Department of Defense (DoD) is developing standardized research security efforts, offering new program protection resources, and how the Under Secretary of Defense for Research and Engineering's (OUSD(R&E)) Strategic Technology Protection and Exploitation (STP&E) office is developing and sharing best practices in research security and program protection with DoD, U.S. government, academic, and international partners.

Watch the webinar here.

UNIVERSITIES SHOULDN'T WAIT FOR MARISE PAYNE'S AXE TO FALL ON CHINA-FUNDED INSTITUTES

Salvatore Babones | The Sydney Morning Herald | May 10, 2021

The universities can't squirm out of it this time. Last year, all 13 Australian universities that host China-funded Confucius Institutes declined to register them under the Foreign Influence Transparency Scheme. Some even tweaked their contracts with the Chinese government to avoid having to register on technicalities. The government was not amused. Last December, the Australia's Foreign Relations Act, or AFRA, removed any ambiguity: it gave universities six months to declare any "written arrangement, agreement, contract, understanding or undertaking" with any foreign government or any foreign university that "does not have institutional autonomy". Australia's states and territories were also forced to declare their foreign entanglements, and the act gives the Foreign Minister the power to cancel any state, territory, or university arrangements that she deems "inconsistent with Australia's foreign policy". Ministerial protestations notwithstanding, the obvious target of the AFRA is China.

Read the full article here.

SENATE PANEL APPROVES BILL THAT WOULD INVEST BILLIONS IN TECH

Maggie Miller | The Hill | May 12, 2021

The Senate Commerce Committee voted Wednesday to approve legislation that would invest billions in science and emerging technologies in an effort to compete with China. The bipartisan Endless Frontiers Act was approved by the committee by a vote of 24-4, with four Republican members voting against the bill. The committee approved the legislation with significantly less funds included for the founding of a Technology and Innovation Directorate at the National Science Foundation, with much of the originally proposed $100 billion being funneled to other research efforts. The bill overall is meant to give a boost to U.S. research and emerging technologies to compete on the global stage, such as in fields including artificial intelligence, quantum computing and semiconductors. The bill was approved after several hours of debate that saw over 100 amendments proposed by senators, including one measure proposed by Sen. Gary Peters (D-Mich.) the committee approved that would provide $2 billion to address the semiconductor shortage, according to the Detroit News.

Read the full article here.

CONTROLLED UNCLASSIFIED INFORMATION (CUI) TOOLKIT

Center for Development of Security Excellence

As part of the phased DOD CUI Program implementation process, the designation, handling, and decontrolling of CUI (including CUI identification, sharing, marking, safeguarding, storage, dissemination, destruction, and records management) will be conducted in accordance with (IAW) DODI 5200.48

Read the full article here.

PENTAGON BACKS OFF XIAOMI BLACKLISTING AFTER LEGAL CHALLENGE

Dan Strumpf | The Wall Street Journal | May 12, 2021

The U.S. Defense Department agreed to remove Xiaomi Corp. from a blacklist banning U.S. investment in the Chinese tech giant, opting against further defending a Trump administration action that alleged ties between the smartphone maker and the Chinese military. The retreat comes two months after Xiaomi won a key victory in a federal lawsuit challenging the listing, in which a Washington, D.C., judge criticized the Pentagon's rationale for the move and ordered a temporary halt against its enforcement. In a one-page legal filing on Tuesday, lawyers for both Xiaomi and the Pentagon said the company's removal from the blacklist was appropriate following the judge's order. Shares of Xiaomi ended 6.1% higher in Hong Kong following the announcement. In agreeing to delist Xiaomi, the Pentagon signaled a willingness to walk away from a sustained fight over one of the Trump administration's final actions against a major Chinese tech company. Xiaomi joins a small but growing list of Chinese tech companies including the owners of Chinese social-media apps TikTok and WeChat that have successfully won courtroom reprieves against Trump-era actions.

Read the full article here.

U.S. INTELLIGENCE AGENCIES WARN ABOUT 5G NETWORK WEAKNESSES

Ravie Lakshmanan | The Hacker News | May 11, 2021

Inadequate implementation of telecom standards, supply chain threats, and weaknesses in systems architecture could pose major cybersecurity risks to 5G networks, potentially making them a lucrative target for cybercriminals and nation-state adversaries to exploit for valuable intelligence. The analysis, which aims to identify and assess risks and vulnerabilities introduced by 5G adoption, was published on Monday by the U.S. National Security Agency (NSA), in partnership with the Office of the Director of National Intelligence (ODNI) and the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). "As new 5G policies and standards are released, there remains the potential for threats that impact the end-user," the report said. "For example, nation states may attempt to exert undue influence on standards that benefit their proprietary technologies and limit customers' choices to use other equipment or software." Specifically, the report cites the contribution of adversarial nations to the development of technical standards, which may pave the way for adopting untrusted proprietary technologies and equipment that could be difficult to update, repair, and replace. Also of concern, per the report, are the optional security controls baked into telecommunication protocols, which, if not implemented by network operators, could leave the door open to malicious attacks.

Read the full article here.

BRITAIN SETS OUT PLANS TO CRACK DOWN ON SPYING BY FOREIGN STATES

Reuters | May 11, 2021

Britain set out plans to crack down on hostile activity by foreign states on Tuesday, introducing a proposed law to give security services and law enforcement new powers to tackle growing threats. The bill will haul legislation into the modern age, updating archaic official secrets acts, some dating back more than hundred years, so that they are relevant to the threats posed in the age of cyber warfare, the government said. British spy chiefs say both China and Russia have sought to steal commercially sensitive data and intellectual property as well as to interfere in politics, while Russian agents are also accused of carrying out an attack on former Russian spy Sergei Skripal on British soil in 2018. The country's treason law could also be revamped, as the country looks to suppress state-backed espionage, according to a briefing document which accompanied the Queen's speech which detailed proposed new laws on Tuesday.

Read the full article here.

DEEMED EXPORTS AND HIRING OF FOREIGN NATIONALS: TIME TO REEVALUATE?

Faegre Drinker Biddle & Reath LLP, and Mollie Sitkowski | JD Supra | May 3, 2021

It may be time to reevaluate your company's approach to "deemed exports" and the hiring of foreign nationals, based on the recent changes to the country designations of Myanmar/Burma, Russia and Hong Kong, as well as the addition of certain items to the Commerce Control List (CCL) as "emerging technology" and the movement of other items from the U.S. Munitions List (USML) to the CCL. Two executive agencies govern exports — the Department of State's Directorate of Defense Trade Controls (DDTC) and the Department of Commerce's Bureau of Industry and Security (BIS). DDTC implements and enforces the International Traffic in Arms Regulations (ITAR), which regulate items on the USML. BIS implements and enforces the Export Administration Regulations (EAR), which regulate items on the CCL. These regulations cover more than just the export of physical items. They cover re-exports between countries, transfers within countries, and releases of software, technology, technical data and technical assistance (collectively "items").

Read the full article here.

ACTIVISTS, EXPERTS AND POLICY MAKERS SPEAK OUT ON CHINESE STATE INFLUENCE IN CANADA

Christy Somos | CTV News | April 29, 2021

Activists, experts and policy makers are speaking out on what they describe as an ever-growing "influence" of the Chinese Communist Party (CCP) in Canadian business, academic and political circles. There has been mounting scrutiny on the CCP's increased flexing of its intelligence muscles since the ascension of President Xi Jinping in 2013. Canada's intelligence agencies have taken the rare step of naming China as a significant threat to the country's sovereignty, with CSIS director David Vigneault publicly saying in a February 2021 speech that Canadians are being "aggressively" targeted by foreign interests – and Beijing was engaged in "activities that are a direct threat to our national security and sovereignty." The redacted version of the 2020 National Security and Intelligence Committee of Parliamentarians (NSICOP) annual report said "the threat from espionage and foreign interference is significant and continues to grow" and that "intelligence shows that China and Russia remain the primary culprits."

Read the full article here.

IT'S NOT JUST CHARLES LIEBER: NIH'S ONGOING INVESTIGATION HAS SWEPT UP 54 SCIENTISTS WHO VIOLATED RULES ABOUT FOREIGN TIES

Amber Tong | Endpoints News | July 23, 2020

The NIH's working group for foreign influences on research integrity has opened cases against 189 scientists suspected of violations related to overseas ties since launching an ongoing, sweeping investigation almost two years ago, newly available statistics showed, leading to the terminations and resignations of 54 scientists. Of those who have been investigated, 41% have also been removed from the NIH system, barred from seeking further grants. Michael Lauer, NIH's head of extramural research, presented a comprehensive set of these and other numbers in a virtual update on Friday, just a day after Charles Lieber — the former head of Harvard's chemistry department — was indicted in federal court for lying about his Chinese connections. While high-profile cases like Lieber's, as well as those at MD Anderson, Emory University and Moffitt before him, have gripped the biomedical field, they merely represent individual snapshots of when institutions respond to the NIH's warnings about hidden foreign ties. The official data shine light on the broader picture.

Read the full article here.

THE CHINA SCHOLARSHIP COUNCIL: AN OVERVIEW

Ryan Fedasiuk | Center for Security and Emerging Technology | July 2020

Since the 2010s, U.S. officials have voiced concerns that the Chinese government may attempt to influence or exploit Chinese students on study abroad programs in its quest for foreign technology. Some Chinese student associations at U.S. universities have spoken out about the Chinese government's efforts to provide unwanted "guidance." However, in the first half of 2020, the U.S. Department of Justice charged several Chinese students with committing visa fraud and acting as agents of the People's Republic of China. The extent to which the PRC government may attempt to influence Chinese students, by what means, and how to respond, remain the subjects of debate in the United States. One avenue by which the Chinese government could exert influence over students is through scholarship and exchange programs. This paper synthesizes Chinese-language resources on the China Scholarship Council—the primary vehicle by which the Chinese government provides scholarships. It describes the characteristics and features of the CSC's largest programs but does not attempt to assess the intent of these programs beyond what is explicitly stated by Chinese primary sources.

Read the full article here.