



<https://asce.tamus.edu>

THE OPEN SOURCE MEDIA SUMMARY

April 28, 2021

SPY CHIEFS LOOK TO DECLASSIFY INTEL AFTER RARE PLEA FROM 4-STAR COMMANDERS

Betsy Woodruff Swan and Bryan Bender | Politico | April 26, 2021

America's top spies say they are looking for ways to declassify and release more intelligence about adversaries' bad behavior, after a group of four-star military commanders sent a rare and urgent plea asking for help in the information war against Russia and China. A host of troubling actions from those two countries — including efforts to damage America's relationships with allies and to violate other countries' sovereignty — mean the Intelligence Community must do more to show the world what Russia and China are doing, according to the commanders. The memo from nine regional military commanders last year implored spy agencies to give them more evidence they can make public as a way to combat "pernicious conduct." Only by "waging the truth in the public domain against America's 21st century challengers" can Washington shore up support from American allies, they said. But efforts to compete in the battle of ideas, they added, are hamstrung by overly stringent secrecy practices.

Read the full article [here](#).

MATHEMATICS PROFESSOR AND UNIVERSITY RESEARCHER INDICTED FOR GRANT FRAUD

U.S. Department of Justice | April 21, 2021

Today, a federal grand jury in Carbondale, Ill. returned an indictment charging a mathematics professor and researcher at Southern Illinois University – Carbondale (SIUC) with two counts of wire fraud and one count of making a false statement. According to court documents, Mingqing Xiao, 59, of Makanda, Illinois, fraudulently obtained \$151,099 in federal grant money from the National Science Foundation (NSF) by concealing support he was receiving from the Chinese government and a Chinese university. "Again, an American professor stands accused of enabling the Chinese government's efforts to corruptly benefit from U.S. research funding by lying about his obligations to, and support from, an arm of the Chinese government and a Chinese public university," said Assistant Attorney General John C. Demers for the Justice Department's National Security Division (NSD). "Honesty and transparency about funding sources lie at the heart of the scientific research enterprise. They enable U.S. agencies to distribute scarce grants for scientific research fairly and equitably. And they allow other researchers to evaluate potential conflicts of interest and conflicts of commitment. When researchers fall short of fulfilling these core academic values in ways that violate the law, the Department stand ready to investigate and prosecute."

Read the full article [here](#).



RUSSIAN FOREIGN INTELLIGENCE SERVICE (SVR) CYBER OPERATIONS: TRENDS AND BEST PRACTICES FOR NETWORK DEFENDERS

U.S. Joint Cybersecurity Advisory | April 26, 2021

The Federal Bureau of Investigation (FBI) and US Department of Homeland Security (DHS) assess Russian Foreign Intelligence Service (SVR) cyber actors—also known as Advanced Persistent Threat 29 (APT 29), the Dukes, CozyBear, and Yttrium—will continue to seek intelligence from US and foreign entities through cyber exploitation, using a range of initial exploitation techniques that vary in sophistication, coupled with stealthy intrusion tradecraft within compromised networks. The SVR primarily targets government networks, think tank and policy analysis organizations, and information technology companies. On 15 April 2021, the White House released a statement on the recent SolarWinds compromise, attributing the activity to the SVR. For additional detailed information on identified vulnerabilities and mitigations, see the National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and FBI Cybersecurity Advisory titled “Russian SVR Targets U.S. and Allied Networks,” released on 15 April 2021.

Read the full article [here](#).

GAO: NIH SHOULD TAKE FURTHER ACTION TO ADDRESS FOREIGN INFLUENCE

Homeland Security Today | April 23, 2021

The National Institutes of Health (NIH), which is a major source of research funding for U.S. universities, has raised concerns over the fruits of this funding going abroad and undisclosed conflicts of interest. For example, in 2020, investigators found a U.S. university researcher involved in a Chinese-government talent recruitment program failed to disclose hundreds of thousands of dollars in foreign income. The federal government reported expending about \$44.5 billion on university science and engineering research in fiscal year 2019. The Department of Health and Human Services funds over half of all such federal expenditures, and NIH accounts for almost all of this funding. The Government Accountability Office (GAO) says U.S. research may be subject to undue foreign influence in cases where a researcher has a foreign conflict of interest. Federal grant-making agencies, such as NIH, can address this threat by implementing conflict of interest policies and requiring the disclosure of information that may indicate potential conflicts.

Read the full article [here](#).

SENATE HELP COMMITTEE HOLDS HEARING ON FOREIGN INFLUENCE IN BIOMEDICAL RESEARCH

Christa Wagner | AAMC | April 23, 2021

NIH Deputy Director for Extramural Research Michael Lauer, MD, testified on the NIH’s efforts to combat foreign influence in biomedical research in an April 22 hearing before the Senate Health, Education, Labor, and Pensions (HELP) Committee. Lauer testified that the NIH’s main areas of concern regarding foreign government influence on the NIH research enterprise are the failure of researchers to disclose outside funding from other organizations or foreign governments, “diversion of proprietary information included in grant applications or produced by NIH-supported biomedical research to other entities,” and a breach of confidentiality in the peer review system. “As of April 2021, we have contacted more than 90 awardee institutions regarding concerns involving over 200 scientists,” he stated.

Read the full article [here](#).



RUSSIAN FOREIGN INTELLIGENCE SERVICE EXPLOITING FIVE PUBLICLY KNOWN VULNERABILITIES TO COMPROMISE U.S. AND ALLIED NETWORKS

National Security Agency Central Security Service | April 15, 2021

The National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) jointly released a Cybersecurity Advisory, "Russian SVR Targets U.S. and Allied Networks," today to expose ongoing Russian Foreign Intelligence Service (SVR) exploitation of five publicly known vulnerabilities. This advisory is being released alongside the U.S. Government's formal attribution of the SolarWinds supply chain compromise and related cyber espionage campaign. We are publishing this product to highlight additional tactics, techniques, and procedures being used by SVR so that network defenders can take action to mitigate against them. Mitigation against these vulnerabilities is critically important as U.S. and allied networks are constantly scanned, targeted, and exploited by Russian state-sponsored cyber actors. In addition to compromising the SolarWinds Orion software supply chain, recent SVR activities include targeting COVID-19 research facilities via WellMess malware and targeting networks through the VMware vulnerability disclosed by NSA.

Read the full article [here](#).

US LAWMAKERS BACK \$100 BILLION SCIENCE PUSH TO COMPETE WITH CHINA

Reuters | New York Post | April 22, 2021

A bipartisan group of US lawmakers on Wednesday introduced legislation calling for \$100 billion in government spending over five years on basic and advanced technology research and science in the face of rising competitive pressure from China. The measure, sponsored by Senate Democratic Leader Chuck Schumer, Republican Senator Todd Young and others, would also authorize another \$10 billion to designate at least 10 regional technology hubs and create a supply chain crisis response program. The bill called the "Endless Frontier Act," represents a significant effort by the government to shore up private sector and university research efforts in advanced technologies with federal funding. "There is a bipartisan consensus that the United States must invest in the technologies of the future to out-compete China," Schumer said, adding "whichever nation develops new technologies first – be they democratic or authoritarian – will set the terms for their use."

Read the full article [here](#).

CHINESE STUDENTS ARE NOT A FIFTH COLUMN

Remco Zwetsloot and Zachary Arnold | Foreign Affairs | April 23, 2021

Getting tough on China is the rare goal that unites people across the political spectrum in a bitterly divided Washington. As the administration of U.S. President Joe Biden works to turn this unifying sentiment into policy, one thorny question stands out: What should be done about students from China in U.S. universities? There are around 120,000 Chinese students in U.S. STEM (science, technology, engineering, and mathematics) programs today, up from 30,000 in 2005. Officials fear that some of these students are moonlighting as "collectors" of intellectual property for the Chinese Communist Party (CCP). In recent years, prominent figures such as Senator Tom Cotton, Republican of Arkansas, and Senator Marsha Blackburn, Republican of Tennessee, have gone so far as to push for an outright ban on Chinese STEM students.

Read the full article [here](#).



CHINA OPENS NEW FRONT IN NATIONAL FIGHT AGAINST SPY THREATS

Jun Mai | South China Morning Post | April 27, 2021

China's state security apparatus will compile lists identifying key Chinese entities for counter-espionage work, according to a new regulation rolled out on Monday by the Ministry of State Security (MSS). Once included on a list, the entity must conduct counter-espionage vetting and training for all personnel with access to secrets, the regulation said. Those personnel must sign non-disclosure agreements before taking on their jobs. In these organisations, counter-espionage training is required before any worker leaves on an overseas trip. Personnel returning from abroad must be interviewed on national security grounds, according to the new rules. The document released on Monday contains the first counter-espionage working regulations at a national level and across different sectors in China. It covers government departments, social groups and companies and requires more regular effort to maintain national security education across the country.

Read the full article [here](#).

JUSTICE DEPARTMENT ANNOUNCES COURT-AUTHORIZED EFFORT TO DISRUPT EXPLOITATION OF MICROSOFT EXCHANGE SERVER VULNERABILITIES

U.S. Department of Justice | April 13, 2021

The Justice Department today announced a court-authorized operation to copy and remove malicious web shells from hundreds of vulnerable computers in the United States running on-premises versions of Microsoft Exchange Server software used to provide enterprise-level e-mail service. Through January and February 2021, certain hacking groups exploited zero-day vulnerabilities in Microsoft Exchange Server software to access e-mail accounts and place web shells (which are pieces of code or scripts that enable remote administration) for continued access. Other hacking groups followed suit starting in early March after the vulnerability and patch were publicized. Although many infected system owners successfully removed the web shells from thousands of computers, others appeared unable to do so, and hundreds of such web shells persisted unmitigated. Today's operation removed one early hacking group's remaining web shells, which could have been used to maintain and escalate persistent, unauthorized access to U.S. networks.

Read the full article [here](#).

'CHINA EXPERT' TO EXAMINE USYD'S 'FOREIGN INFLUENCE' RISKS

Max Shanahan | Honi Soit | April 20, 2021

The University of Sydney has engaged "China expert" John Garnaut, through consultancy firm McGrath Nicol, "as part of a range of initiatives...to manage the risks of foreign interference." Garnaut is a former Sydney Morning Herald China correspondent and aide to former PM Malcolm Turnbull. A University spokesperson described Garnaut as "a respected China expert with a deep understanding of Chinese institutions." An article written by Garnaut in 2015 was the subject of a successful defamation claim by businessman Chau Chak Wing. In 2015, Chau Chak Wing donated \$15 million to the University to fund the construction of the Chau Chak Wing museum. Garnaut has also been engaged by UNSW and Monash. The Herald reported that, in at least one of these three institutions, Garnaut will "audit academics...to see if they have secondary jobs." The University declined to answer whether its academics would be the subject of such an audit.

Read the full article [here](#).



COLLEGE FOREIGN CASH AT RISK AS SENATE TARGETS CHINA'S CLOUT

Daniel Flatley, David McLaughlin, and Janet Lorin | Bloomberg | April 20, 2021

A broad attempt by Congress to stem China's influence could put at risk research collaborations and funding that U.S. universities count on by subjecting some foreign gifts and contracts to national security reviews. Senators are seeking increased oversight of grants and contracts to universities from overseas as part of a bipartisan package of legislation designed to increase U.S. competitiveness with China in science and technology. The proposal would give U.S. national security officials new authority to scrutinize foreign gifts and contracts of more than \$1 million to schools if the funding is related to research and development of "critical technologies" and provides access to material nonpublic technical information. The American Council on Education said it identified about 700 contracts and gifts that were reported to the Department of Education worth \$1 million or more in 2019 that could potentially be subject to national security reviews under the proposal. The trade group said the proposal could "severely hinder" international research collaborations. Although funding from any overseas source would be subject to scrutiny, the target of the measure is clear.

Read the full article [here](#).

THE US SHOULD LISTEN TO SCIENTISTS ABOUT HOW TO COUNTER INFLUENCE FROM CHINA

Xiaoxing Xi | Nature Review Physics | April 19, 2021

The US government has attempted to counter foreign influence on American research by pursuing criminal investigations into scientists linked to China. Xiaoxing Xi — 2020 recipient of the American Physical Society's Andrei Sakharov Prize — believes that non-criminal approaches, such as those recommended by the independent group JASON, address the problem better.

Read the full article [here](#).

SCIENTIFIC RESEARCH INTEGRITY DEMANDS TRANSPARENCY — THE LAW SHOULD REQUIRE IT TOO

Cortney Weinbaum | The Hill | April 10, 2021

China may be using the U.S.'s system of scientific openness to advance its military power while stealing future US economic growth. China pays scientific researchers in the U.S. to "share" their innovations in exchange for money, access to research laboratories and access to speaking and publication opportunities. They do this irrespective of the researchers' ethnicities or countries of citizenship and they require the researchers to keep these agreements secret from their employers or the U.S. government. Perhaps it is time for the U.S. to codify scientific transparency into law. In November 2019, the Senate Homeland Security and Government Affairs Permanent Subcommittee on Investigations published 150 pages of evidence that the government of China has been systematically, aggressively, clandestinely and strategically stealing from America's scientific research enterprise, exploiting the fact that this enterprise was built on American values of "reciprocity, integrity, merit-based competition, and transparency." Bill Priestap, Assistant Director of Counterintelligence for the FBI, said, "The Chinese government is attempting to acquire or steal, not only the plans and intentions of the United States government, but also the ideas and innovations of the very people that make our economy so incredibly successful."

Read the full article [here](#).



SENATE EYES NEW ROLE FOR CFIUS IN COMBATING ‘FOREIGN MALIGN INFLUENCE OR ESPIONAGE ACTIVITIES’ TARGETING ‘INSTITUTIONS OF HIGHER EDUCATION’

John Gurtunca and David Hanke | JD Supra | April 19, 2021

New legislation may soon expand the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS) as part of a broader push by Congress to position the United States to “out-compete” China in the coming decades and counter China’s increasing global influence. On April 8, 2021, the US Senate Foreign Relations Committee publicly released a draft of the Strategic Competition Act of 2021, a 281-page bill that aims “to mobilize all US strategic, economic, and diplomatic tools for an Indo-Pacific strategy that will allow our nation to truly confront the challenges China poses to our national and economic security.” Among other things, the bill calls for hundreds of millions of dollars in funding for foreign military sales and Indo-Pacific security initiatives, while also seeking to deter further human rights and anti-democratic actions by China, particularly in relation to Hong Kong and the treatment of Uighur Muslims. The Strategic Competition Act comes as part of a broader congressional initiative to bolster the United States’ ability to compete with China.

Read the full article [here](#).

XI JINPING'S CULTURE WAR COMES TO CHINA'S CAMPUSES AS COMMUNIST PARTY PREPARES TO MARK 100 YEARS

James Griffiths | CNN | April 20, 2021

When it comes to making history, Beijing's universities have played an outsized role: they were the source of the demonstrations which kicked off the May Fourth Movement, to which the Chinese Communist Party traces its roots, and the Tiananmen Square protests, perhaps the biggest challenge to the CCP since it took power. So it makes sense then that President Xi Jinping, as he looks to further consolidate his rule ahead of the Party's centennial later this year, would pay special attention to the country's top schools. In a visit to Tsinghua University this week, Xi praised the Beijing institution for cultivating a "glorious tradition of patriotism" and encouraged students to be "both red and professional," a phrase which dates to the Mao Zedong era. "Be firm in your beliefs, always stand with the Party and the people, and be a firm believer and faithful practitioner of socialism with Chinese characteristics," said Xi, adding that "a splendid flower blooms in the unrelenting struggle." Along with several other elite Beijing institutions, Tsinghua is one of China's top universities, and graduates can be expected to take up key roles in the future in government and business.

Read the full article [here](#).

HUNDREDS OF U.S. SCIENTISTS FEARED COMPROMISED BY CHINA

Ryan Lovelace | The Washington Times | April 22, 2021

More than 500 federally funded scientists are under investigation for being compromised by China and other foreign powers, the National Institutes of Health revealed Thursday. The federal health officials told a Senate committee that they are fighting to keep up with large-scale Chinese efforts to corrupt American researchers and steal intellectual property that scientists hope will lead to biomedical advances. NIH has contacted more than 90 institutions about more than 200 scientists they’re concerned about, said Dr. Michael S. Lauer, NIH deputy director for extramural research. But the investigations’ workload is weighing down the nation’s top medical research agency, and new cases are turning up constantly across the government.

Read the full article [here](#).



CHINA-LINKED HACKERS USED VPN FLAW TO TARGET U.S. DEFENSE INDUSTRY -RESEARCHERS

Christopher Bing and Raphael Satter | Reuters | April 20, 2021

At least two groups of China-linked hackers have spent months using a previously undisclosed vulnerability in American virtual private networking devices to spy on the U.S. defense industry, researchers and the devices' manufacturer said Tuesday. Utah-based IT company Ivanti said in a statement the hackers took advantage of the flaw in its Pulse Connect Secure suite to break into the systems of "a very limited number of customers." Ivanti said that while mitigations were in place, a fix for the issue would be unavailable until early May. Ivanti provided no detail about who might be responsible for the espionage campaign but, in a report timed to Ivanti's announcement, cybersecurity company FireEye Inc(FEYE.O) said it suspected that at least one of the hacking groups operates on behalf of the Chinese government. "The other one we suspect is aligned with China-based initiatives and collections," said Charles Carmakal, a senior vice president of Mandiant, an arm of Fireeye, ahead of the report's release.

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.tamug.edu>

