ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

January 6, 2021

TRUMP BARS U.S. TRANSACTIONS WITH EIGHT CHINESE APPS INCLUDING ALIPAY

Alexandra Alper and David Shepardson | Reuters | January 5, 2021

U.S. President Donald Trump on Tuesday signed an executive order banning transactions with eight Chinese software applications, including Ant Group's Alipay mobile payment app, the White House said, escalating tensions with Beijing two weeks before President-elect Joe Biden takes office. The move, first reported by Reuters, is aimed at curbing the threat to Americans posed by Chinese software applications, which have large user bases and access to sensitive data, a senior administration official told Reuters. The order argues that the United States must take "aggressive action" against developers of Chinese software applications to protect national security. It tasks the Commerce Department with defining which transactions will be banned under the directive within 45 days and targets Tencent Holdings Ltd's QQ Wallet and WeChat Pay as well. The order also names CamScanner, SHAREit, Tencent QQ, VMate which is published by Alibaba Group subsidiary UCWeb, and Beijing Kingsoft Office Software's WPS Office. "By accessing personal electronic devices such as smartphones, tablets, and computers, Chinese connected software applications can access and capture vast swaths of information from users, including sensitive personally identifiable information and private information," the executive order states.

Read the full article here.

U.S. INTELLIGENCE COMMUNITY SAYS RUSSIA IS 'LIKELY' BEHIND MAJOR, ONGOING CYBERHACKS OF FEDERAL AGENCIES

Ellen Nakashima | The Washington Post | January 5, 2021

The U.S. intelligence community stated Tuesday that Russia is "likely" behind a major and ongoing series of cyberhacks of federal government agencies — its first official indication of blame. The statement, issued jointly by four agencies in a special task force, counters President Trump's baseless suggestion last month that the intrusions might have been the work of Chinese hackers. Secretary of State Mike Pompeo said previously that the breaches were "clearly" Russian in origin, and U.S. officials have for weeks said privately that Moscow's foreign intelligence service carried them out, but Tuesday's statement is the first official word from the intelligence community saying that officials think Russia is the culprit. The breaches were so alarming that they had government and private-sector personnel working through the holidays, the task force said. That sense of urgency stands in contrast to Trump's effort last month to downplay the significance of the breaches.

Read the full article here.

COMMUNIST INFLUENCE? 14 PROFS BUSTED FOR CHINA CONNECTIONS IN 2020

Alex Munguia | Campus Reform | December 28, 2020

Multiple professors and researchers have been exposed for their alleged ties to China in 2020. Ranging from allegedly lying to federal authorities, to attempting to steal proprietary research and information, the past months have shown several alleged secret Chinese agents working in American higher education. In January, Chinese national and Harvard University medical student Zhaosong Zheng was arrested for allegedly attempting to smuggle cancer research, which the university had been working on for years. He was reported to have received multiple payments from the Chinese Scholarship Council. FBI agent Kara Spice stated, "I believe, based on my training and experience, that Zheng's appointment at (Beth Israel) was not an accident, and that he was knowingly gathering and collecting intellectual property from BIDMC, possibly on behalf of the Chinese government."

Read the full article here.

THE THREATS ARISING FROM THE MASSIVE SOLARWINDS HACK

Deirdre Cohen and Remington Korper | CBS News | January 3, 2021

Like the coronavirus, it came from overseas, arriving, initially, unnoticed. When it was finally, belatedly discovered, the outrage (for a few days at least) was epic. "This is nothing short of a virtual invasion by the Russians into critical accounts of our federal government," said Democratic Senator Dick Durbin. Republican Senator Mitt Romney called it "an extraordinary invasion of our cyberspace." The Russians, it's believed, hacked into the software of a company called SolarWinds, causing them to push out malicious updates – call it a "cyber virus" – infecting the computer systems of more than 18,000 private and government customers. Almost a cyber pandemic. As former Bush Administration official Theresa Payton told Fox News, "This vulnerability allowed these nefarious cyber operatives to actually create what we refer to in the industry as 'God access' or a 'God door,' giving them basically any rights to do anything they want to in stealth mode."

Read the full article here.

FEDERAL RESEARCH: AGENCIES NEED TO ENHANCE POLICIES TO ADDRESS FOREIGN INFLUENCE

U.S. Government Accountability Office | December 17, 2020

U.S. research may be subject to undue foreign influence in cases where a researcher has a foreign conflict of interest (COI). Federal grant-making agencies can address this threat by implementing COI policies and requiring the disclosure of information that may indicate potential conflicts. GAO reviewed five agencies which together accounted for almost 90 percent of all federal research and development expenditures at universities in fiscal year 2018—and found that three have agency-wide COI policies, while two do not (see figure). The three agencies with existing policies focus on financial interests but do not specifically address or define non-financial interests, such as multiple professional appointments. In the absence of agency-wide COI policies and definitions on non-financial interests, researchers may not fully understand what they need to report on their grant proposals, leaving agencies with incomplete information to assess the risk of foreign influence. GAO found that, regardless of whether an agency has a conflict of interest policy, all five agencies require researchers to disclose information—such as foreign support for their research—as part of the grant proposal that could be used to determine if certain conflicts exist.

Read the full report here.

"ROAD KILL IN A GAME OF CHICKEN": CHINA, CANADA, AND THE UNITED STATES

Christopher W. Bishop | Council on Foreign Relations | January 5, 2021

It has now been over two years since Chinese officials detained Canadians Michael Kovrig and Michael Spavor for "endangering state security"—ten days after the Royal Canadian Mounted Police arrested Huawei Chief Financial Officer Meng Wanzhou on an extradition warrant from the United States, where she had been indicted for bank fraud. Since being taken into custody on December 10, 2018, the "two Michaels" have been held in solitary confinement for prolonged periods and questioned repeatedly about their activities, with very limited access to Canadian consular officials or legal counsel. (Kovrig had served as a Canadian diplomat in Beijing before joining the International Crisis Group, while Spavor worked as a consultant arranging tours and cultural exchanges with North Korea.) By contrast, Meng has been living in one of her two Vancouver mansions, albeit with an ankle bracelet and 24-hour surveillance that she pays for herself, as her case moves through a British Columbia court.

Read the full article here.

AUSTRALIA TO TOUGHEN EXPORT CONTROLS OVER FEARS TECHNOLOGY COULD FALL INTO HANDS OF FOREIGN ARMIES

Daniel Hurst | The Guardian | January 5, 2021

The Morrison government is looking at tightening laws to curb the export of sensitive technologies that could be used by foreign militaries, amid broader concerns over national security risks in the research sector. The defence department has told an inquiry it is working on ways to toughen up the export controls "while not unnecessarily restricting trade, research and international collaboration". Parliament's security committee is investigating how universities and research bodies are dealing with foreign interference risks, after the home affairs minister, Peter Dutton, agreed to calls from Coalition backbenchers to launch an inquiry. In a submission, the defence department said Australian universities and academics were "attractive targets for foreign interference given their access to sensitive information, research in a range of fields and the resulting intellectual property". The Australian defence force could lose its technological advantage, it said, if sensitive research and its potential use were not properly "protected from foreign interference and potential adversaries".

Read the full article here.

RESEARCHERS TARGETED BY FOREIGN ACTORS: ASIO

Katie Burgess | The Canberra Times | January 2, 2021

Universities are bristling against the prospect of more regulation to combat foreign interference, as Australia's domestic spy agency warns the threat cannot be left unchecked. ASIO has told the parliamentary joint committee on intelligence and security's inquiry on foreign interference in the university sector it has learnt of researchers and their families who have been threatened or coerced by actors seeking to provide their sensitive research to a foreign state. The agency said it was also aware that some universities have been threatened with funding cuts should critical research continue, and of academics self-censoring to avoid being punished. "In ASIO's view, we cannot leave harmful foreign interference unchecked, given the serious nature of the threat and the corrosive impact it can have on our democratic society," their submission reads. However the Group of Eight chief executive Vicki Thomson told the inquiry Australia risked damaging important research collaborations if it over-reacted.

Read the full article here.

DOJ NATIONAL SECURITY BOSS IS MOVING ON — BUT CYBER, CHINA THREATS AREN'T

Ryan Lucas | NPR | December 31, 2020

When John Demers came in to lead the Justice Department's national security division, the United States was grappling with the fallout from Russia's cyberattack on the 2016 election. Now, as he and the Trump administration prepare to leave office, the U.S. is dealing with another massive hack that American officials have again pinned on Moscow. "Well, there is a certain symmetry to all of this," Demers said in an interview with NPR as his time at the Justice Department draws to a close. Those bookends illustrate how the threats the U.S. is facing have shifted since his last stint at the department, during the George W. Bush administration. "A big difference in my time here, the first time and the second time, is the rise of a nation state threat actors and in particular, their use of cyber to protect their nation state interests and their power," Demers said. "So it's fitting, I think, that we began with a significant election interference hack ... and then here we are at the end dealing with a different kind of cyber activity."

Read the full article here.

US TECH FIRMS MUST STOP HELPING CHINA'S DEFENSE-LINKED ORGANIZATIONS

Ryan Fedasiuk and Emily Weinstein | Defense One | December 23, 2020

When the U.S. Commerce Department expanded its blacklist by 77 institutions last Friday, it added five Chinese universities: Nanjing University of Aeronautics and Astronautics, Nanjing University of Science and Technology, Beijing University of Posts and Telecommunications, Tianjin University, and Beijing Institute of Technology. Sanctioning schools might seem strange or severe at first glance, but the Chinese Communist Party relies heavily on universities in its broader strategy of technology acquisition from abroad and military-civil fusion. The sanctions illustrate why U.S. companies must step up due diligence when collaborating with Chinese universities. Some have questioned the move, insisting there is no harm in working with educational institutions. After all, it is in the United States' interest to preserve an open and collaborative global research environment; international partnerships are the lifeblood of the U.S. science and technology ecosystem. However, a number of Chinese institutions pose clear risks to U.S. national security, and it's long past time that U.S. companies operating in China recognized this fact.

Read the full article here.

FROM THE BOOKSHELF: 'CHINESE SPIES: FROM CHAIRMAN MAO TO XI JINPING'

Robert Wihtol | Australian Strategic Policy Institute | December 21, 2020

As China expands its reach around the globe, it is important to understand not only its foreign, economic and security policies but also its massive covert operations. Roger Faligot, an investigative journalist who specialises in studying intelligence agencies, first published Chinese spies in French. It proved so successful that he recently had a significantly expanded version translated into English. Faligot's ambitious book spans a century of Chinese espionage, from the beginnings of the Chinese Communist Party to the Xi Jinping era. In the 1920s, a youthful Zhou Enlai organised Chinese communist cells, in Hong Kong under the alias Stephen Knight and in France as Wu Hao, while Deng Xiaoping, then a factory worker in Paris, spent his evenings mimeographing underground pamphlets. The Chinese secret services modelled themselves on the Soviets, who trained many of their operatives. Both wove complex webs, spying on factions, dissidents and each other.

Read the full article here.

REPORT FINDS HOLES IN U.S. POLICIES ON FOREIGN INFLUENCE IN RESEARCH

Jeffrey Mervis | Science | December 28, 2020

A new report by a congressional watchdog says U.S. agencies need to flesh out and clarify their policies for monitoring the foreign ties of the researchers they fund. The report, by the Government Accountability Office (GAO), is likely to spur efforts in Congress aimed at preventing China and other nations from using funding and other connections to gain improper access to research funded by the U.S. government. But at least one of the agencies under scrutiny—the National Science Foundation (NSF)—is pushing back on the idea that its policies are lax. It is warning that tougher rules could hinder its ability to fund the best science. The GAO report was requested by Senator Chuck Grassley (R–IA), chairman of the Senate Committee on Finance, who in hearings has prodded research agencies to "pick up their game" when it comes to preventing improper foreign influence. It examines the practices of the government's five biggest funders of academic research: the National Institutes of Health (NIH), NSF, NASA, the Department of Energy (DOE), and the Department of Defense (DOD). The report recommends they adopt explicit and uniform policies on what grantees need to do to comply with federal laws relating to three issues: financial conflicts of interest (CoI); nonfinancial conflicts that include unrealistic time commitments or duplication of research; and disclosure of all sources of research funding, both foreign and domestic.

Read the full article here.