



<https://asce.tamus.edu>

THE OPEN SOURCE MEDIA SUMMARY

JULY 22, 2020

U.S. ASKED CHINA TO CLOSE HOUSTON CONSULATE, GLOBAL TIMES EDITOR SAYS

Derek Wallbank | Bloomberg | July 22, 2020

The U.S. gave China 72 hours to close its consulate in Houston, according to Hu Xijin, the editor of the Communist Party's Global Times newspaper. Hu's tweet came hours after Houston police and firefighters descended on the consulate following witness reports that papers were being burned outside in open containers, the Houston Chronicle and two local TV stations reported, citing local police. Hu didn't say in his tweet how he obtained the information. His English-language tweets are closely followed by investors. In videos posted online by local media outlets in Houston, fires could be seen in multiple containers, with smoke rising into the sky. TV stations KPRC and KHOU said firefighters were not allowed inside the complex, and KHOU said the fires were later extinguished. The Chronicle said no injuries were reported.

Read the full article [here](#).

TWO CHINESE HACKERS WORKING WITH THE MINISTRY OF STATE SECURITY CHARGED WITH GLOBAL COMPUTER INTRUSION CAMPAIGN TARGETING INTELLECTUAL PROPERTY AND CONFIDENTIAL BUSINESS INFORMATION, INCLUDING COVID-19 RESEARCH

U.S. Department of Justice Federal Bureau of Investigation | July 21, 2020

A federal grand jury in Spokane, Washington, returned an indictment earlier this month charging two hackers, both nationals and residents of the People's Republic of China (China), with hacking into the computer systems of hundreds of victim companies, governments, non-governmental organizations, and individual dissidents, clergy, and democratic and human rights activists in the United States and abroad, including Hong Kong and China. The defendants in some instances acted for their own personal financial gain, and in others for the benefit of the MSS or other Chinese government agencies. The hackers stole terabytes of data which comprised a sophisticated and prolific threat to U.S. networks.

Read the full article [here](#).



FBI PUBLIC SERVICE ANNOUNCEMENT: FOREIGN GOVERNMENT-SPONSORED TALENT RECRUITMENT PLANS, SUCH AS CHINA'S TALENT PLANS, INCENTIVIZE ECONOMIC ESPIONAGE AND THEFT OF TRADE SECRETS

U.S. Department of Justice Federal Bureau of Investigation | July 16, 2020

The United States welcomes international students, scholars, and researchers in the pursuit of intellectual collaboration and business advancement. It is therefore critical for U.S. businesses, universities, and granting institutions to be aware of potential financial risks and past illegal conduct that has been associated with foreign-government sponsored talent recruitment programs, such as China's so-called "Talent Plans." Such knowledge will enable individuals, businesses, and institutions to take appropriate steps to safeguard themselves and their intellectual property.

Read the full public service announcement attached.

KELVIN DROEGEMEIER: CHINESE THEFT AND SUBVERSION THREATEN US SCIENTIFIC RESEARCH, HEALTH AND NATIONAL SECURITY

Kelvin Droegemeier | Fox News | July 16, 2020

Under President Trump's leadership, our nation's vast research enterprise is fully engaged to confront the COVID-19 pandemic. Ultimate victory depends on our scientific preeminence rooted in the longstanding and often unspoken principles of integrity, transparency, cooperation, openness, impartiality, respect, freedom of inquiry, reciprocity and accountability to the American people. Yet these principles — and the security and integrity of America's research enterprise — are being undermined by some researchers and foreign governments that are robbing the American people of federal research dollars, new discoveries and innovations.

Read the full article [here](#).

CHINA VOWS RETALIATION AFTER U.S. SHUTS DOWN HOUSTON CONSULATE

Bloomberg | July 22, 2020

China vowed retaliation after the U.S. forced the closure of its Houston consulate, prompting stocks to fall in one of the biggest blows to diplomatic ties between the two countries in decades. The U.S. government gave China three days to close its consulate in America's fourth-most populous city in an "unprecedented escalation," Chinese Foreign Ministry spokesman Wang Wenbin told a regular briefing Wednesday in Beijing. China planned to "react with firm countermeasures" if the Trump administration didn't "revoke this erroneous decision," Wang said. The U.S. State Department subsequently confirmed in a statement that it had ordered the consulate closed "to protect American intellectual property and Americans' private information." It said international agreements required diplomats to respect the laws and regulations of the host nation and not interfere in its internal affairs.

Read the full article [here](#).



THOUSAND TALENTS PROGRAM EXPOSES NEW LEGAL RISKS FOR UNIVERSITIES

William Beasley and Ivan Boatner | JD Supra | July 16, 2020

University professors' involvement in the Peoples' Republic of China's Thousand Talents Plan (the Talents Plan) has been in the news quite a bit recently. In recent months, the Department of Justice (DOJ) has made multiple announcements about the prosecution of university researchers for failing to properly disclose their involvement in the Talents Plan:

- On July 9, 2020, DOJ announced a professor and researcher at The Ohio State University had been charged with grant fraud "for not disclosing that he was engaged in a sophisticated scheme to use approximately \$4.1 million in grants from the National Institutes of Health (NIH) to develop China's expertise in the areas of rheumatology and immunology."
- On June 9, 2020, DOJ announced the indictment of the former chair of Harvard's Chemistry and Biology Department.
- On May 11, 2020, DOJ announced the guilty plea of a former Emory University professor.
- On March 10, 2020, a tenured professor in the West Virginia University's physics program pled guilty to fraud.

Read the full article [here](#).

THOUSAND TALENTS PROGRAM'S CHINESE SCIENTIST ARRESTED ON THE RUN

Christopher Burgess | Clearance Jobs | July 10, 2020

Chinese Scientist, Song Gou Zheng was confronted in early May by one of his U.S. employers, The Ohio State University, regarding his foreign affiliations and failure to comply with rules surrounding National Institutes of Health (NIH) research grants. In other words, Zheng's Chinese affiliations were benefiting from more than \$4.1 million in NIH funded research at Ohio State. Like many participants in China's Thousand Talent Program, they are rewarded handsomely by China for sharing and advancing China's knowledge in their area of specialization.

Read the full article [here](#).

U.S. WEIGHS SWEEPING TRAVEL BAN ON CHINESE COMMUNIST PARTY MEMBERS

Paul Mozur and Edward Wong | The New York Times | July 15, 2020

The Trump administration is considering a sweeping ban on travel to the United States by members of the Chinese Communist Party and their families, according to people familiar with the proposal, a move that would almost certainly prompt retaliation against Americans seeking to enter or remain in China and exacerbate tensions between the two nations. The presidential proclamation, still in draft form, could also authorize the United States government to revoke the visas of party members and their families who are already in the country, leading to their expulsion. Some proposed language is also aimed at limiting travel to the United States by members of the People's Liberation Army and executives at state-owned enterprises, though many of them are likely to also be party members.

Read the full article [here](#).



THE EU'S ROLE IN FIGHTING DISINFORMATION: TAKING BACK THE INITIATIVE

James Pamment | Carnegie Endowment for International Peace | July 15, 2020

Amid the coronavirus pandemic, Europe and the West are grappling with a host of thorny dilemmas posed by disinformation and foreign influence operations. While these problems predate the viral outbreak, the public health crisis has certainly exacerbated them. Brussels has taken some steps to meet this set of challenges, some of which are already paying dividends. But there is more that Europe can do to make its response more effective. Specifically, the EU should formulate shared terminology for combating disinformation, assertively deter adversaries who are spreading disinformation and conducting influence operations, craft sensible nonregulatory interventions to protect online users, and establish an independent, transparent auditing regimen for certain online platform functions.

Read the full article [here](#).

UK AND ALLIES EXPOSE RUSSIAN ATTACKS ON CORONAVIRUS VACCINE DEVELOPMENT

United Kingdom National Cyber Security Centre | July 16, 2020

Russian cyber actors are targeting organisations involved in coronavirus vaccine development, UK security officials have revealed. The National Cyber Security Centre (NCSC), a part of GCHQ, has published an advisory today, detailing activity of the threat group known as APT29, which has exploited organisations globally. The NCSC assesses that APT29, also named "the Dukes" or "Cozy Bear" almost certainly operate as part of Russian intelligence services. This assessment is also supported by partners at the Canadian Communication Security Establishment (CSE), the US Department for Homeland Security (DHS) Cybersecurity Infrastructure Security Agency (CISA) and the National Security Agency (NSA). APT29's campaign of malicious activity is ongoing, predominantly against government, diplomatic, think-tank, healthcare and energy targets to steal valuable intellectual property.

Read the full article [here](#).

SCRUTINY OVER HUAWEI UNIVERSITY TIES INCREASES AFTER BAN

Yojana Sharma | University World News | July 16, 2020

The British government's decision this week to ban Chinese technology giant Huawei from its national telecommunications infrastructure has prompted renewed scrutiny over Huawei's links with universities in the United Kingdom and renewed calls for transparency in university dealings with the Chinese company. The UK government announced on 14 July that the purchase of new Huawei equipment for high speed 5G networks will be banned at the end of 2020, and all Huawei equipment will be removed from UK 5G networks by 2027 following a review by the government's National Cyber Security Centre. The United States and Australia have also banned Huawei from public contracts.

Read the full article [here](#).



US CRACKDOWN HARMS CHINESE COLLABORATIONS

Andrew Silver | Nature | July 16, 2020

Scientists in China have told Nature that they are reluctant to travel to the United States for conferences or other research activities, even when pandemic travel restrictions lift. They fear being caught up in the US government's crackdown on foreign interference in science, and in ongoing political tensions between the two nations. The scrutiny has led some researchers in China to dial back on collaborations with US colleagues and form new partnerships with teams in Europe or Japan. Researchers in both countries say that US policies, such as increasingly onerous visa restrictions on Chinese scientists and students, and tightened export controls, are also having a chilling effect on research partnerships. If researchers in China reduce their travel to the United States — because of political tensions, visa restrictions or pandemic travel restrictions — that will affect collaborations, says Caroline Wagner, a science and technology policy researcher at the Ohio State University in Columbus. Most research collaborations start from face-to-face meetings, she says, but researchers need to travel for those to happen: "Zoom is not a good substitute."

Read the full article [here](#).

IRANIAN STATE HACKERS CAUGHT WITH THEIR PANTS DOWN IN INTERCEPTED VIDEOS

Dan Goodin | ARS Technica | July 17, 2020

Iranian state hackers got caught with their pants down recently when researchers uncovered more than 40GB of data, including training videos showing how operatives hack adversaries' online accounts and then cover their tracks. The operatives belonged to ITG18, a hacking group that overlaps with another outfit alternatively known as Charming Kitten and Phosphorous, which researchers believe also works on behalf of the Iranian government. The affiliation has long targeted US presidential campaigns and US government officials. In recent weeks, ITG18 has also targeted pharmaceutical companies. Researchers generally consider it a determined and persistent group that invests heavily in new tools and infrastructure.

Read the full article [here](#).

U.S. POLITICIANS EXPRESS NATIONAL SECURITY CONCERNS OVER TIK TOK APP

Sara Maslar-Donar | WKOW News | July 16, 2020

There are renewed security concerns over TikTok, the popular short-video app with more than two billion downloads worldwide. While the Chinese company that owns TikTok, ByteDance, doesn't operate in China and functions independently, policy-makers are still worried that it could be forced to hand over its data on U.S. users to the Chinese government under the country's national security laws. Within the last week, Secretary of State Mike Pompeo said that they are "looking at" banning TikTok and other Chinese apps. India banned the use of the app country-wide and the U.S. Armed Forces have also banned the use of the app on government-issued phones.

Read the full article [here](#).



RUSSIA TRIED TO HACK CORONAVIRUS VACCINE RESEARCH, US, UK AND CANADA SAY

Guy Davies | ABC News | July 16, 2020

A "cyber espionage group" associated with the Russian intelligence services has attempted to hack into coronavirus vaccine research in the U.S., Britain and Canada, according to a report from the U.K.'s National Cyber Security Center. The U.S. National Security Agency agreed with that report. "Throughout 2020, APT29 has targeted various organizations involved in COVID-19 vaccine development in Canada, the United States and the United Kingdom, highly likely with the intention of stealing information and intellectual property relating to the development and testing of COVID-19 vaccines," the NCSC report said. APT29, also known as "the Dukes" or "Cozy Bear," is one of the Russian Intelligence Service entities identified in the FBI's assessment of malicious cyber activity in the 2016 presidential election. "It is completely unacceptable that the Russian Intelligence Services are targeting those working to combat the coronavirus pandemic," Dominic Raab, the U.K.'s foreign secretary, said in response to the advisory. "While others pursue their selfish interests with reckless behavior, the U.K. and its allies are getting on with the hard work of finding a vaccine and protecting global health."

Read the full article [here](#).

CYBER-THREATS INCREASING FOR UNIVERSITIES UNDER LOCKDOWN

Kamal Bechkoum | University World News | July 18, 2020

Universities around the world are bombarded on a daily basis with information about cyber-crime and threats to their IT infrastructure, almost to the point where it feels like there is little else that needs to be done, except trust in the IT department's skills and get on with life. But does this mean that students and academic staff are safe, that their research and partner companies' data is secure, that payments can be made in a secure way and that the university's computers, libraries and facilities will continue to function without hiccups? In a word, 'No'. Like any other business, universities will never be 100% secure because no one is completely safe when it comes to cyber-security.

Read the full article [here](#).

HOW THE CHINESE REGIME INFILTRATED ACADEMIA IN THE WEST: RACHELLE PETERSON

Jan Jekielek | NTD | July 17, 2020

How has the Chinese Communist Party infiltrated American universities? How are Confucius Institutes involved? While some Confucius Institutes are being shut down, is it possible some are staying, simply under a different guise? And, how does the Chinese regime use the Thousand Talents Program and similar operations to steal American research? In this episode, we sit down with Rachele Peterson, Director of Policy at the National Association of Scholars. This is American Thought Leaders, and I'm Jan Jekielek.

Watch the full video [here](#).



ATTORNEY GENERAL WILLIAM P. BARR DELIVERS REMARKS ON CHINA POLICY AT THE GERALD R. FORD PRESIDENTIAL MUSEUM

U.S. Department of Justice Federal Bureau of Investigation | July 16, 2020

Thank you, Andrew for that very kind introduction and for the excellent work that you and your team have done in protecting the people of the Western District of Michigan. I would like to thank the leadership and staff of the Gerald R. Ford Presidential Museum — especially Director Elaine Didier — for hosting today's event. I'd also like to offer a special thanks to the Ford Presidential Foundation and Executive Director Joe Calvaruso. Even under normal circumstances, hosting an event can be a challenge, but these days, I know it is especially challenging. Thank you for accommodating us. I am also grateful to you, the audience, for honoring me with your presence today. It is a privilege to be here to speak about what may prove to be the most important issue for our nation and the world in the twenty-first century — that is, the United States' response to the global ambitions of the Chinese Communist Party. The CCP rules with an iron fist over one of the great ancient civilizations of the world.

Read the full remarks [here](#).

REP. DONNA SHALALA INTRODUCES BIPARTISAN BILL TO LIMIT CHINESE GOVERNMENT INFLUENCE IN HIGHER EDUCATION

Carlos Condarco | Congresswoman Donna Shalala | July 14, 2020

Today, Congresswoman Donna Shalala (D-FL), alongside Rep. Anthony Gonzalez (R-OH), introduced the Concerns Over Nations Funding University Campus Institutes in the United States Act (CONFUCIUS Act), bipartisan legislation to address concerns about the Chinese government's influence on college campuses. Specifically, the bill would seek to limit the influence of Confucius Institutes – cultural and language exchange programs at American universities funded by the Chinese government – by barring Department of Education funds from going to any college or university that does not comply with the provisions of the bill. This would not include funding disbursed to students, such as Pell grants. "Confucius Institutes are directly funded by the Communist Chinese government, which suppresses freedom of speech, academic freedom, and other democratic values," said Congresswoman Shalala.

Read the full article [here](#).

CRIMINAL CHARGES FOR UNDECLARED CHINESE RESEARCH TIES MOUNT IN THE US

Rebecca Trager | Chemistry World | July 15, 2020

The US Justice Department has charged another professor at an American university with committing research grant fraud to benefit China. Ohio State University's Song Guo Zheng used more than \$4 million (£3.2 million) in grant money from the US National Institutes of Health (NIH) to develop rheumatology and immunology expertise for the Chinese government, according to a criminal complaint unsealed following his 9 July detention hearing. The 57-year-old Zheng has also allegedly been a participant in the Chinese government's Thousand Talents programme – a scheme to recruit and cultivate high-profile scientists – since 2013. He is charged with making false statements about maintaining employment in China at the same time he was working for US universities. Zheng, who was previously at the University of Southern California and Pennsylvania State University, faces up to 15 years in prison if convicted.

Read the full article [here](#).



DISSECTING THE TWITTER HACK WITH A CYBERSECURITY EVANGELIST

Louis Columbus | Forbes | July 18, 2020

Targeting the most influential celebrities on Twitter, hackers orchestrated a social engineering-based attack Wednesday promoting a cryptocurrency scam. Business leaders, celebrities, politicians and billionaires' accounts were hacked using Twitter's administrative tools. Personal Twitter accounts hacked include those of Amazon CEO Jeff Bezos, Joe Biden, Tesla CEO Elon Musk, President Barack Obama, Bill Gates, Warren Buffet and others. Apple and Uber's Twitter accounts were also hacked. Using SIM swapping, in which threat actors trick, coerce or bribe employees of their victims to gain access to privileged account credentials and administrative tools, hackers were able first to change the email address of each targeted account. Next, two-factor authentication was turned off so when an alert was sent of the account change it went to the hacker's email address. With the targeted accounts under their control, hackers began promoting their cryptocurrency scam.

Read the full article [here](#).

CHINESE STUDENTS TURN AWAY FROM US UNIVERSITIES

Bangkok Post | July 19, 2020

It was a tough decision for mainland university graduate Zancy Duan to give up her coveted place at a US Ivy League school. It was a tough decision for mainland university graduate Zancy Duan to give up her coveted place at a US Ivy League school. Duan, from China's eastern province of Zhejiang, had been admitted by Cornell University as a candidate for a master's degree, along with admissions from several other American schools. But at the end of April, with the coronavirus pandemic at its peak, she rushed to apply for European universities.

Read the full article [here](#).

HOW BRITAIN TEACHES CHINA TO CONQUER THE WEST: UK'S TOP UNIVERSITIES SHARE ULTRA SENSITIVE MILITARY AND COMPUTING RESEARCH WITH CHINESE COLLEGES LINKED TO THE MODERN RED ARMY... AND TAKE MILLIONS FROM THEM IN FUNDING

Sian Boyle | The Daily Mail | July 17, 2020

As relations between the West and China plummet to new depths, we can at least take comfort from the fact that many of our leading academic institutions are still enjoying a healthy collaboration with their Chinese equivalents. Or can we? At times of conflict, the very word 'collaboration' has unfortunate connotations. An investigation by the Mail has found China's 'collaboration' with British universities often smacks more of infiltration and is potentially lethal to our national interest. Research from Britain's most eminent academic institutions may be ending up in the hands of the Chinese military at a time when we can ill-afford such security breaches. Many of our top universities — some from the prestigious Russell Group — are unwittingly sharing their most advanced research with secretive elements of the Chinese military which specialise in state-of-the-art fighter jets, hypersonic missiles and supercomputers used to develop nuclear weapons.

Read the full article [here](#).



TRUMP TARGETS FULBRIGHT IN CHINA, HONG KONG

Elizabeth Redden | Inside Higher Ed | July 16, 2020

President Trump on Tuesday ordered his administration to take steps to end the U.S. government's flagship Fulbright exchange program in China and Hong Kong. Trump stated his intent to end Fulbright exchanges with China and Hong Kong as part of an executive order directing the suspension or elimination of various policy exemptions in U.S. law that give Hong Kong preferential treatment in relation to mainland China. The order was prompted by the imposition by Beijing of a new national security law governing Hong Kong, a step that the executive order describes as "merely China's latest salvo in a series of actions that have increasingly denied autonomy and freedoms" to Hong Kong, a semiautonomous region of China. The provision about Fulbright was buried deep in the order, in Section 3, provision (i) -- right after a provision ordering the suspension of a collaboration in the earth sciences involving the U.S. Geological Survey and an institute at the Chinese University of Hong Kong. The presidential-level intervention in the Fulbright program -- which comes about six months after the Peace Corps ended its China program and during a time of worsening U.S.-Chinese relations -- prompted concerns among scholars, who argued that canceling academic exchange programs is self-defeating.

Read the full article [here](#).

SECURITY LAW: HONG KONG SCHOLARS FEAR FOR ACADEMIC FREEDOM

Jerome Taylor and Su Xinqi | Hong Kong Free Press | July 15, 2020

China's new security law has sent a chill through Hong Kong's schools and universities with many teachers fearful the city's reputation for academic freedom and excellence is now at risk. Just a week after the sweeping legislation was imposed on the territory, staff at some institutions have already been warned by their administrators to be careful how they teach. "Remain neutral in your teaching and be mindful of the language you use," read one email to staff of HKU SPACE, a college attached to the prestigious University of Hong Kong (HKU). "Any behaviour in eliciting further discussion on sensitive issues MUST be avoided," the email from the program director of the humanities and law faculty said.

Read the full article [here](#).

RUSSIAN HACKERS BLAMED FOR ATTACKS ON CORONAVIRUS VACCINE-RELATED TARGETS

Jeremy Strasburg and Dustin Volz | The Wall Street Journal | July 16, 2020

U. S. and U.K. government officials said a prominent state-backed Russian hacking group is responsible for ongoing cyberattacks against organizations involved in the development of coronavirus vaccines and other healthcare-related work, a sign of escalating security concerns amid the global response to Covid-19. The National Cyber Security Centre, part of the U.K.'s GCHQ electronic-intelligence agency, said Thursday it worked with U.S. and Canadian security officials to assess the source of persistent hacking activity.

Read the full article [here](#).



RUSSIA IS TRYING TO HACK AND STEAL CORONAVIRUS VACCINE DATA, U.S., CANADIAN AND UK OFFICIALS CLAIM

Ryan Browne | CNBC | July 16, 2020

Hackers linked to Russian intelligence services are trying to steal information about coronavirus vaccine research in the U.S., Canada and the U.K., security officials said Thursday. Officials said a group known as APT29 — also known as “Cozy Bear” — was likely to blame for the attack. They said the group, which is believed to be associated with Russian intelligence, used spear phishing and custom malware to target vaccine researchers. The U.S. Department for Homeland Security, the Cybersecurity Infrastructure Security Agency, the National Security Agency, Canada’s Communications Security Establishment and the U.K.’s National Cyber Security Centre joined forces in accusing Russia of the hacking campaign. “It is completely unacceptable that the Russian Intelligence Services are targeting those working to combat the coronavirus pandemic,” U.K. Foreign Secretary Dominic Raab said in a statement. “While others pursue their selfish interests with reckless behaviour, the U.K. and its allies are getting on with the hard work of finding a vaccine and protecting global health.”

Read the full article [here](#).

AMERICA’S CAMPAIGN AGAINST HUAWEI IS FINALLY PAYING OFF

Eli Lake | Bloomberg | July 16, 2020

At the beginning of this year, President Donald Trump’s push to get U.S. allies to ban China’s largest telecommunications firm from their 5G wireless networks appeared to be in shambles. Despite two years of diplomacy and warnings, America’s closest friend in Europe, the U.K., had signaled that it would allow Huawei equipment into its network. This week Prime Minister Boris Johnson began the process of walking back that decision. The U.K. has now pledged to eliminate Huawei equipment from its 5G networks by 2027 and will ban the purchase of new Huawei gear after December. This decision shows that a strategy of risk mitigation — that a nation could prevent the Chinese government from using Huawei circuits and other gear as international listening posts — doesn’t work. In January, the British government said Huawei equipment would be vetted to make sure that the Chinese could not exploit it. That approach is no longer viable. As Oliver Dowden, the U.K. minister overseeing telecommunications, told Parliament this week: “As facts have changed, so has our approach.”

Read the full article [here](#).

VACCINE HACK SHOWS DARK SIDE OF WORLD DESPERATE FOR COVID RELIEF

James Paton and John Lauerman | Bloomberg | July 16, 2020

A half year into a pandemic that’s killed almost 600,000 people, the international race for protection from the virus escalated to a treacherous new level with allegations that vaccine development has become a target of Russian cyber-attacks. Vaccine nationalism is already a concern as countries jockey to secure doses of future shots, desperate for a way out of a global crisis that’s slammed their economies. Science and money have been the main drivers so far, with the U.S. spending billions on deals for experimental shots and other countries trying to keep up. Government reports that Russian intelligence hacked international research centers developing inoculations against Covid-19 add a plot line reminiscent of Cold War spy thrillers.

Read the full article [here](#).



SECURITY CLEARANCE REFORMERS TOUT PROGRESS AMID COVID-19

Aaron Boyd | Nextgov | July 16, 2020

The federal government is in the midst of the biggest overhaul of the security clearance process in the program's 50-year history, and COVID-19 is pushing some of those reforms along. After the breach of Office of Personnel Management databases in 2015, the government began a comprehensive restructuring of the clearance process, including establishing the National Background Investigations Bureau, or NBIB. Last year, that office was officially dissolved and merged within the Pentagon's Defense Counterintelligence and Security Agency—formerly the Defense Security Service. But the process and administrative changes created a hefty backlog of investigations and put a spotlight on archaic processes, such as requiring all interviews—neighbors, spouses, former colleagues—to be conducted in person.

Read the full article [here](#).

POMPEO ANNOUNCES VISA RESTRICTIONS ON SOME HUAWEI EMPLOYEES

Zachary Basu | Axios | July 15, 2020

The U.S. will impose visa restrictions on certain employees of Chinese telecom Huawei and other companies that "provide material support to regimes engaging in human rights violations globally," Secretary of State Mike Pompeo said Wednesday. Why it matters: The Trump administration's latest escalation against Huawei, which U.S. intelligence officials view as a threat to national security due to its ties to the Chinese military, comes the day after the U.K. announced it will no longer allow the telecom to access its 5G network. The U.K. decision was a big win for the Trump administration, which has sought to firewall Huawei from networks around the world while putting intense pressure on its closest ally to make such a move. Pompeo commended the decision and announced he would visit the U.K. and Denmark, which has also banned Huawei from its 5G network, next week.

Read the full article [here](#).

LETTER TO THE EDITOR: 'AS CHINA SHOWS ITS TRUE COLORS, AMERICA MUST UNITE AGAINST THE REAL THREAT,' STEWART WARNS

St. George News | July 13, 2020

Anyone who still thinks of China and the Chinese Communist Party (CCP) as a viable business partner is sadly mistaken. It is not a country that values human rights, freedom or mutual respect among nations. The reality is, the world has a China problem and it's time we found the fortitude to deal with it. Consider the reality of CCP rule. More than a million Chinese Muslim Uighurs are imprisoned in inhumane reeducation camps, targeted for nothing but their ethnicity and religion. A staggering 1.3 billion Chinese citizens are suppressed and controlled through social monitoring. This incredibly powerful tool is used by the CCP to brutally punish even the slightest infraction from approved speech, act or thought.

Read the full article [here](#).



CHINA IS BECOMING INCREASINGLY ASSERTIVE – SECURITY LAW IN HONG KONG IS JUST THE LATEST EXAMPLE

James S. Abdul-Alim | The Conversation | July 13, 2020

China's enforcement of a new security law in Hong Kong marks the de facto end of the "one country, two systems" model that came into effect following the British handover in 1997. This has repercussions that go far beyond Hong Kong. The Sino-British Joint Declaration, signed by both China and the UK in 1984, paved the way for the handover. It states clearly that the territory shall enjoy "basic rights and freedom" and "a high degree of autonomy" for 50 years – until 2047. The treaty was lodged with the UN and so any breach of it is a breach of international law. Arguing that the new security law prematurely removed Hong Kong's high degree of autonomy, the UK proposed a pathway for an estimated 3 million Hong Kongers to gain British citizenship. China was quick to assert that this decision breached the terms of its agreements with the UK.

Read the full article [here](#).

CHINA ENGAGED IN LARGE-SCALE CAMPAIGN TO SUBVERT U.S. GOVERNMENT, PRIVATE SECTOR: FBI

Bill Gertz | The Washington Times | July 7, 2020

Chinese intelligence agents and diplomats are actively subverting U.S. policies through bribery, blackmail and covert influence operations, FBI Director Christopher A. Wray said Tuesday in a major policy address. The operations, the FBI chief said, are part of large-scale intelligence activities by China to recruit spies and steal information. "The greatest long-term threat to our nation's information, intellectual property and to our economic vitality is the counterintelligence and economic espionage threat from China," Mr. Wray told an audience at the Hudson Institute think tank. The Chinese operations range from traditional spying – recruiting agents inside government – to cyberattacks and data theft aimed at obtaining cutting-edge U.S. technology. The theft has hit Fortune 100 companies down to small startup businesses.

Read the full article [here](#).

USC RESEARCHERS BIOENGINEER FIRST-LINE DEFENSE AGAINST COVID-19

Association of American Universities | June 26, 2020

Researchers at the USC Dr. Allen and Charlotte Ginsburg Institute for Biomedical Therapeutics, the USC Institute for Technology and Medical Systems and the USC School of Pharmacy are developing an antimicrobial fluid to bolster the body's first-line defenses against COVID-19. The biocompatible coating is intended to block the virus from entering the body through membranes in the nose, eyes and mouth. If successful, the invention could change the way medicine prevents certain infectious diseases. Severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), the infectious agent that causes COVID-19, latches onto structures on the surface of our cells in order to invade. One of these membrane structures, known as a lipid raft, contains cholesterol and fats and acts as the subcellular equivalent of a dock at a seaport. Viral particles traversing our respiratory and gastrointestinal tracts hook onto lipid rafts, then enter our cells and use our cellular machinery to replicate.

Read the full article [here](#).



PREPARING FOR CHANGES TO THE DEPARTMENT OF EDUCATION'S FOREIGN GIFTS AND CONTRACTS REPORT

Amanda Ferguson | LinkedIn | July 10, 2020

Universities have long been required to comply with Section 117 of the Higher Education Act[1], which requires institutions to file disclosures with the U.S. Department of Education regarding gifts received from and contracts entered into with foreign sources via a Foreign Gifts and Contracts Report (hereby referred to as Report). Recent enforcement, legislative and administrative activity surrounding these reports and foreign influence has increased scrutiny for institutions subject to these requirements.

Read the full article [here](#).

PENTAGON: MAJOR CHINESE COMPANIES HAVE CLOSE MILITARY LINKS

Bill Gertz | The Washington Times | June 25, 2020

The Pentagon on Thursday revealed the names of 20 Chinese companies linked to the People's Liberation Army operating directly or indirectly in the United States, in a bid to halt Beijing from obtaining military-related goods. The list includes Huawei Technologies, the global telecommunications company the Trump administration has identified as a potential electronic spying threat. Other firms include the major missile and aircraft manufacturer Aviation Industry Corp. of China, and Hikvision, a company that make surveillance cameras that have been used in the mass repression of Uighurs in western China. Hikvision in a statement denied it was a Chinese military company and said the U.S. list was "baseless." Most of the companies on the list have been subject to U.S. economic sanctions and export controls in the past. They include China North Industries Group Corp., linked in the 1990s to an arms smuggling ring for street gangs in Los Angeles, and China's main missile manufacturers — China Aerospace Science and Technology Corp. and China Aerospace Science and Industry Corp.

Read the full article [here](#).

EUROPEAN DEFENSE COMPANIES THE TARGET OF CYBER ESPIONAGE OVER LINKEDIN

Byron Muhlberg | CPO Magazine | July 3, 2020

By posing as recruiters on LinkedIn, a new tactic has emerged by which advanced persistent threat (APT) hackers have been able to commit cyber espionage. This was evidenced by the findings of a recent report, which found that cybercriminals—believed to be affiliated with the North Korean government—posed as recruiters working at the U.S. defense groups Collins Aerospace and General Dynamics in order to break into the networks of European defense companies. According to Slovakia-based cybersecurity firm ESET, the cyber espionage attempts took place between September and December of last year, and were uncovered after a collaborative investigation with two of the affected defense companies in Europe.

Read the full article [here](#).



OPINION | FREE TRADE WITH CHINA IS NEITHER FREE NOR TRADE

Shashwat Alok and Aditya Kuvalekar | Live Mint | June 30, 2020

Amid the covid-19 induced economic lockdowns, there is an increasing chorus around the world to increase self-reliance in sectors critical to a nation's sovereignty and integrity. Many commentators have raised concerns, particularly regarding their nation's over-dependence on China. At the same time, free-market pundits have been crying hoarse on why this rising protectionism goes against the tenets of free trade and is likely to harm the very consumers it seeks to protect. Much of China's rise has been fueled on benefitting from the paradigm of "free-trade being good for humanity"—a narrative that has rarely been questioned.

Read the full article [here](#).

PENTAGON RESHUFFLES R&D PRIORITIES

John Harper | National Defense | June 5, 2020

The Defense Department is shaking up its list of research-and-development priorities as the Pentagon builds new roadmaps for pursuing future capabilities. When Undersecretary of Defense for Research and Engineering Mike Griffin first came into office in 2017, hypersonic weapons were his top focus area. But not anymore. "We've made a lot of progress in hypersonics," said Mark Lewis, director of defense research and engineering for modernization. "We love them all the same, but our No. 1 priority, frankly, right now is microelectronics." The primary aim of the effort is to ensure that the United States and its allies have access to state-of-the-art capabilities, he noted during remarks at the Pacific Operational Science and Technology Conference in Honolulu, Hawaii, hosted by the National Defense Industrial Association.

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>

