ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

October 21, 2020

NSA WARNS CHINESE STATE-SPONSORED MALICIOUS CYBER ACTORS EXPLOITING 25 CVES

National Security Agency Central Security Service | October 20, 2020

The National Security Agency released a new cybersecurity advisory, detailing 25 vulnerabilities that Chinese state-sponsored malicious cyber actors are currently exploiting or targeting, to encourage stakeholders to apply mitigations. Many of these vulnerabilities can be used to gain initial access to victim networks by exploiting products that are directly accessible from the Internet. Once a cyber-actor has established a presence on a network from one of these remote exploitation vulnerabilities, they can use other vulnerabilities to further exploit the network from the inside. While these CVEs are already publicly known, NSA is sharing knowledge of their active exploitation—with attribution—to encourage all National Security Systems (NSS), U.S. Defense Industrial Base (DIB), and Department of Defense (DoD) system owners to verify that their systems are protected against these threats and if not, take appropriate action.

Read the full article here.

CHINA WARNS U.S. IT MAY DETAIN AMERICANS IN RESPONSE TO PROSECUTIONS OF CHINESE SCHOLARS

Kate O'Keeffe and Aruna Viswanatha | The Wall Street Journal | October 17, 2020

Chinese government officials are warning their American counterparts they may detain U.S. nationals in China in response to the Justice Department's prosecution of Chinese military-affiliated scholars, according to people familiar with the matter. The Chinese officials have issued the warnings to U.S. government representatives repeatedly and through multiple channels, the people said, including through the U.S. Embassy in Beijing. The Chinese message, the people said, has been blunt: The U.S. should drop prosecutions of the Chinese scholars in American courts, or Americans in China might find themselves in violation of Chinese law. China started issuing the warning this summer after the U.S. began arresting a series of Chinese scientists, who were visiting American universities to conduct research, and charged them with concealing from U.S. immigration authorities their active duty statuses with the People's Liberation Army, the people said. The arrests were the subject of a Wall Street Journal article that also reported U.S. allegations that Chinese diplomats were coordinating activities with the researchers, and described that as a factor in ordering China to close its Houston consulate in July and remove the remaining military scientists from the country.

Read the full article here.

NATIONAL STRATEGY FOR CRITICAL AND EMERGING TECHNOLOGIES

White House | October 15, 2020

Throughout our history, American achievements and leadership in science and technology (S&T) have been a driving factor for our way of life, prosperity, and security. However, American leadership in S&T faces growing challenges from strategic competitors, who recognize the benefits of S&T and are organizing massive human and capital resources on a national scale to take the lead in areas with long-term consequences. The National Security Strategy (NSS) lays out a vision for promoting American prosperity; protecting the American people, the homeland, and the American way of life; preserving peace through strength; and advancing American influence in an era of great power competition. It calls for the United States to lead in research, technology, invention, and innovation, referred to here generally as science and technology (S&T), by prioritizing emerging technologies critical to economic growth and security. The NSS also calls for the United States to promote and protect the United States National Security Innovation Base (NSIB), which it defines as the American network of knowledge, capabilities, and people – including academia, National Laboratories, and the private sector – that turns ideas into innovations, transforms discoveries into successful commercial products and companies, and protects and enhances the American way of life.

Read the full document here.

MADE IN GERMANY, CO-OPTED BY CHINA

Emily de La Bruyere and Nathan Picarsic | Foundation for Defense of Democracies | October 14, 2020

In 2015, China's State Council announced "Made in China 2025" (MIC2025), a sweeping plan for China to become a "manufacturing great power," seize the "commanding heights" of global manufacturing, and win the "new industrial revolution." MIC2025 is the first installment of a three-part, three-decade series. That series is itself an extension of decades of Chinese industrial plans, strategies, and projects that comprise Beijing's larger "Go Out" strategy, a long-standing program to deploy Chinese companies and institutions internationally. MIC2025 aligns closely with its predecessor plans under Go Out, including the 2006 "Medium- and Long-Term Plan for Science and Technology Development" and the National Development and Reform Commission's 2013 "Strategic Emerging Industries" initiative. All of these initiatives reflect parallel ambitions and use similar tools to accomplish them. Beijing aims to capture the modern networks, technical standards, and technology platforms that will form the foundation of the 21st-century global economy.

Read the full article here.

OUR UNIVERSITIES HAVE SACRIFICED ACADEMIC LIBERTY FOR CHINESE CASH

Edward Lucas | The Times | October 16, 2020

"It is too late," said the 21-year-old student at one of London's best-known colleges, misery etched on his face. "This university has already gone red." He was talking to the mother of his oldest friend, explaining that he must break off contact. As political refugees from China, she and her family were criminals in the eyes of the regime. Associating with them would endanger him — and his family back in China. There could be no exceptions, he explained. His mobile (using a mandatory Chinese phone number) was monitored and Chinese spies, embedded in the student body and elsewhere, were watching. They would notice if he even left the campus.

Read the full article here.

NSA STEPS OUT OF SHADOWS TO SPOTLIGHT WHERE CHINA HACKERS PROWL

William Turton | Bloomberg | October 20, 2020

The U.S. National Security Agency detailed 25 cyber vulnerabilities frequently used by Chinese state-sponsored hackers in an effort to alert computer security officials to update their systems. Most of the vulnerabilities "can be exploited to gain initial access to victim networks using products that are directly accessible from the internet and act as gateways to internal networks," according to the NSA's statement. The vulnerabilities listed by the agency are already publicly known, in software like Microsoft Corp.'s Windows or Citrix Systems Inc.'s remote work products. Even though the vulnerabilities have already been disclosed, computer security professionals may struggle to adequately apply a fix that mitigates the flaw. In some instances, the vulnerabilities are years old while others were discovered as recently as September. The notice from the NSA may serve as motivation to entities that could be targeted by Chinese hackers to apply the fixes. The advisory is part of a recent effort by the historically secretive agency to increase network security across the country and bolster public trust in the agency.

Read the full article here.

CHINA LAWMAKERS PASS EXPORT CONTROL LAW PROTECTING TECH

Colum Murphy, Karoline Kan, Dong Lyu, and Jing Li | Bloomberg | October 17, 2020

China passed a new law to restrict sensitive exports to protect national security, helping Beijing gain reciprocity against U.S. as tech tensions mount. The country's top legislative body, the National People's Congress Standing Committee, adopted the measure on Saturday that applies to all companies in China, including foreign-invested ones. The law will be effective Dec. 1. Souring ties between China and the U.S. had led Washington to take action against several Chinese companies including Huawei Technologies Co., ByteDance Ltd.'s TikTok app, Tencent Holdings Ltd.'s WeChat and Semiconductor Manufacturing International Corp. The new law provides a framework for Beijing to better fight back. While its existing control list is much narrower than the one used by the U.S., the country's commerce ministry made an amendment in August that included technology such as algorithms and drones. The list could be further expanded to include even more products and technologies. The law stipulates export controls over items of both civilian and military use, military and nuclear products, as well as "goods, technologies and services" that are related to national security, including data related to them. Relevant government departments have been tasked to publish lists of controlled items.

Read the full article here.

OPERATION WARP SPEED AND BEYOND TOOLKIT

Center for Development of Security Excellence

This toolkit has been developed for cleared and uncleared industry partners working on Operation Warp Speed (OWS). It provides OWS partners with the resources they need to better protect the important work they are doing. While some of these resources were developed with cleared contractors participating in the National Industrial Security Program (NISP) in mind, the guidance and information provided apply to any industry partner working on sensitive information that is sought after by an adversary, regardless of classification level or designation. On September 10, 2020, Operation Warp Speed industry partners were invited to participate in a webinar that provided an overview of insider risk, cybersecurity, counterintelligence threats, and industrial security best practices. In case you were unable to attend the live webinar, you may view a recording of the webinar here.

Read the full article here.

PROTECTING ACADEMIC FREEDOM IN INTERNATIONAL PARTNERSHIPS

John Heathershaw and Eva Pils | University World News | October 15, 2020

We live in an age of academic internationalisation, especially pronounced in the United Kingdom. This has in many ways been a good thing. It has become more common for research institutions across the globe to establish collaborative research and joint degree programmes, often hugely benefiting research and teaching. Individual scholars and students travel more easily and frequently today, too, and their ideas and arguments travel with them. Moreover, even when physical travel is interrupted, as it is at the moment, academic communities can interact and stay connected remotely. But internationalisation has also produced new risks, especially in the context of engagement, exchange and collaboration with non-democratic countries. In an age of 'democratic retrogression' and deepening authoritarianism affecting many countries, many members of the global academic community face growing challenges – including censorship and travel restrictions, disciplinary measures and dismissals, criminal prosecutions and even physical attacks, as has been well documented by Scholars At Risk and other groups.

Read the full article here.

WHAT HAPPENS WHEN CHINA LEADS THE WORLD

Michael Schuman | The Atlantic | October 5, 2020

What kind of superpower will China be? That's the question of the 21st century. According to American leaders such as Secretary of State Mike Pompeo, China will be a rapacious authoritarian nightmare, intent on destroying democracy itself. Beijing, needless to say, doesn't quite agree. Fortunately for those of us seeking answers to this question, China was a major power for long stretches of history, and the foreign policies and practices of its great dynasties can offer us insights into how modern Chinese leaders may wield their widening power now and in the future. Of course, Chinese society today is not the same as it was 100 years ago—let alone 1,000 years. But I've long been studying imperial China's foreign relations, and clear patterns of a consistent worldview emerge that are likely to shape Beijing's perceptions and projection of power in the modern world. In an address to the United Nations General Assembly in September, Chinese President Xi Jinping repeated Beijing's oft-stated claim that it was committed to peaceful development, and there is a widely held view that Chinese emperors of the past generally eschewed the use of force.

Read the full article here.

PLURALISATION OF RESEARCH POWER IS DIVERSIFYING SCIENCE

Simon Marginson | University World News | October 17, 2020

After the internet emerged in 1990, universities and scientific institutes across the world became joined in a single collaborative research network for the first time in history, and in the manner of networks, global science began to expand continually with exceptional speed. World research is shaped by five simultaneous trends that feed into each other and are transforming the processes whereby human societies create and share knowledge. First, rapid growth in investment in research and in science paper output. Second, expansion in the number of research-active countries with their own science systems. Third, growth in the proportion of papers co-authored from more than one country. Fourth, the increasing weight of the networked global science system compared to national systems. Fifth, the distribution of leading research power among more countries. OECD data shows that, between 1995 and 2018, almost every country expanded its spending on research.

Read the full article here.

U.S. INTELLIGENCE OFFICIAL SAYS SOCIAL MEDIA 'BIG VULNERABILITY'

Alyza Sebenius and Chris Strohm | Bloomberg | October 15, 2020

A top U.S. intelligence official said disinformation on social media is a "big vulnerability" and warned of an "existential threat" to democracy and elections. "The public in the democratic nations around the world really doesn't understand what disinformation and influence looks like and feels like when you see it," said William Evanina, director of the U.S. National Counterintelligence and Security Center. "Social media and the ability to promulgate information expediently on the web is going to be a big vulnerability for democracies going forward," he added during a conference hosted by cybersecurity company Crowdstrike Inc. on Thursday. "We have not succeeded across our democratic countries in explaining to our populace how important and how fragile our democracy is," he added. "The core fundamental basis of that fragility is free and open elections." Evanina and other government officials have repeatedly warned that foreign powers are trying to hack presidential campaigns as well as other political targets and spread disinformation to influence elections. In August, Evanina shared intelligence that concluded China and Iran are working to sway U.S. voters against President Donald Trump while Russia is working against his rival, Joe Biden.

Read the full article here.

NEW GUIDANCE ON SECURITY THREATS TO INTERNATIONALISATION

Brendan O'Malley | University World News | October 16, 2020

Universities can introduce 'Chatham House rules' of non-attribution in relation to seminars and tutorial discussions and allow students to submit coursework anonymously under new guidance issued by Universities UK (UUK) to combat the growing impact of security threats on academic freedom and internationalisation. Of particular concern is the impact of the threats on international partnerships and international researchers and students, which MPs have separately warned are growing due to the rise of authoritarian regimes. "The sector has historically done a good job of managing the risks associated with internationalisation. However, the risks are increasingly dynamic and growing in complexity," wrote Professor Sir Peter Gregson, chair of a UUK-convened task force which drafted the guidance, and Professor Anthony Finkelstein, in the foreword to the guidance. "In this context, institutions will need to review and adapt their risk-management processes."

Read the full article here.

CHINA'S TRUE TECH AMBITIONS

Jordan Schneider | China Talk | October 16, 2020

The past two ChinaTalk podcasts were a ton of fun. Most recently, yesterday I put out a show with Nate Duncan of the Dunk'd On Podcast on China and the NBA. But last week's with Emily De La Bruyere deserved the full transcript treatment. Her paper on China's approach to scientific research is the best piece of China policy analysis I've read in 2020, deeply sourced in policy documents, and coming to powerful conclusions about the nature of the CCP's tech ambitions. Our discussion touches on why the CCP prioritizes applied over basic scientific research, the most important tech standards fight you've never heard of, the sad state of the US intelligence community's open-source research, and why rare earths have led to these cows in Inner Mongolia having to graze on a moonscape. Do read the transcript below or have a listen.

Read the full article here.

WHAT MAKES INTERNATIONAL STUDENTS WANT TO STAY ON OR GO?

Jan Petter Myklebust | University World News | October 17, 2020

Three-quarters of bachelor degree graduates and two-thirds of masters and doctoral graduates live on in Finland for three or more years after their degree, according to new research. The study by Charles F Mathies and Hannu Karhunen, researchers at Jyväskylä University and the Helsinki Institute of Labour Economics, tracked a sample of 13,046 international students graduating at 24 universities of technology and 14 universities in Finland between 1999 and 2011, via the Finnish personal identity code. They observed that 74% of bachelors, 67% of masters and 65% of doctoral graduates were residing in Finland three years after graduation. This is high compared with findings in similarly framed studies in other Scandinavian countries: Denmark (58% two years after graduation); Norway (44% five years after degree start), they reported.

Read the full article here.

HARVARD OPPOSES U.S. PLAN TO LIMIT STAY OF FOREIGN STUDENTS

Janet Lorin | Bloomberg | October 19, 2020

Harvard University is joining other colleges and higher-education groups in opposing another federal proposal aimed at foreign students, this one limiting the length of stay at U.S. schools to four years or less. The plan is "an inappropriate intrusion into academic matters," Harvard President Lawrence Bacow wrote to Sharon Hageman, acting regulatory unit chief of U.S. Immigration and Customs Enforcement in an Oct. 16 letter. "The proposed rule would create negative and cascading consequences for U.S. research, scholarship and training." The government, which says the move will reduce fraud and enhance national security, has already collected more than 20,000 comments and will keep accepting more until the Oct. 26 deadline. The proposal put forth last month by the Department of Homeland Security may add to financial hardships at U.S. colleges. Schools already are getting less revenue because of lower enrollment, especially from international students who often pay the full price. In July, Harvard and the Massachusetts Institute of Technology obtained a court order to stop the U.S. from enforcing new visa guidelines that would have cast international students out of the country if schools offer only online classes.

Read the full article here.

COVID-19: CYBERCRIMINALS LIKELY TO SEE OPPORTUNITY TO EXPLOIT ACADEMIC ENTITIES' ONLINE DISTANCE LEARNING PLATFORMS AND USERS

U.S. Department of Homeland Security | April 24, 2020

This Article warns federal, state, and local departments of education and school administrators, information technology staff, network defenders, and law enforcement personnel of financially motivated cyber threats facing academic institutions, faculty, and students during the COVID-19 pandemic. For the purposes of this assessment, we define academic institutions as private and public pre-kindergarten through 12th grade schools, institutions of higher education, and business and trade schools. This Article considers cybercriminals to include actors seeking to profit from as well as save money through illicit cyber activity. This Article is the latest in a series of assessments on COVID-19 cyber threats, including those associated with telework. While this Article similarly addresses cyber threats associated with conducting legitimate activities remotely, it focuses on unique threats to educational institutions vis-à-vis schools that rely on distance learning alternatives.

Read the full article here.

BALANCING INSTITUTIONAL AUTONOMY AND NATIONAL POLICY

Roger Chao, Jr. | University World News | October 17, 2020

As we count the months during which the COVID-19 pandemic has disrupted the world, including higher education, various national governments have taken different actions, from initiating e-learning programmes to applying health regulations to the higher education sector. What seems to be forgotten is the fact that higher education institutions and their management teams are tasked with delivering quality education and have the capacity to adapt their curriculum, delivery methods and decide the best options (including establishing health protocols) to ensure the health of their students and faculty. In short, the institutional autonomy of higher education institutions has a significant role to play in the midst of the COVID-19 pandemic and beyond. Furthermore, that institutional autonomy needs to be respected, considering that higher education institutions are mandated to mould and empower the future citizens and leaders of the world.

Read the full article here.

HOW TO SECURE YOUR DEVICES AT HOME AND AT WORK

University of California | October 12, 2020

Securing devices from hackers and other bad actors online is extremely important. Here are some basic tips you can use to stay safe.

Secure your home router: By default, most routers do not have a password, or the password is the word "admin." One of the most important things you can do is to set a password for your router. Change this by logging into your router (use 192.168.1.1 or 192.168.1.0 in your web browser). The procedure will be slightly different for each brand of router.

Encrypt your devices: UCOP laptops are encrypted automatically. If you have a personal laptop, you'll want to follow the instructions for Windows encryption or Mac encryption to encrypt the data in case your laptop is ever lost or stolen.

Back up your devices: Always make a backup of your devices so that if they fail, they can be restored. An alternative is to use secure online storage, such as Box, to save all of your work-related files.
Set PINs on your smartphones and tablets: Use as long a PIN as possible. A six-digit PIN has one million possible combinations, compared to a four-digit PIN which can only have about 10,000.
Keep your computer and devices up to date: When your computer or device informs you that an update is available, install it as soon as you can.

Enable automatic locking: Set your device to lock if it is not used for more than a few minutes. If you walk away from your computer at the office, lock it.

Don't reuse passwords: If a hacker breaks into one of your accounts, odds are they will try that same password on other accounts you may have. Use a different password for each account. Use a password manager to help you set up and remember your passwords.

Read the full article here.

ALABAMA A&M, TROY RESPOND TO CONCERNS ABOUT CONFUCIUS INSTITUTES

Mike Cason | AL.com | October 18, 2020

Alabama A&M University and Troy University have responded to questions from Congressman Mo Brooks about the Confucius Institutes that operate on their campuses. Confucius Institutes at American colleges have come under fire from federal and state officials who say they could be used for propaganda and influence favorable to China's government, such as by suppressing discussion of its authoritarian policies. Brooks called on Alabama A&M and Troy to shut down their Confucius Institutes. "The Communist Chinese Party cannot be allowed to gain influence over America's education system or undermine American national security," Brooks wrote to university officials last month. Confucius was a philosopher and teacher who lived more than 2,500 years ago in China. Confucius Institutes operate under Hanban, an organization based in Beijing with the stated purpose of promoting the teaching of the Chinese language and understanding of the culture.

Read the full article here.

FBI UNVEILS REVISED CYBER SECURITY STRATEGIES AT AUBURN VIRTUAL EVENT

Preston Sparks | Yellow Hammer

Leaders from the Federal Bureau of Investigation unveiled the organization's revised strategies for dealing with cyber attacks at an hour-long virtual event hosted by Auburn University's McCrary Institute on Thursday morning. FBI Cyber Division Assistant Director Matt Gorham and FBI Deputy Assistant Directors Tonya Ugoretz and Clyde Wallace joined McCrary Institute Director Frank Cilluffo live on YouTube for the panel discussion, outlining the bureau's evolving policies for dealing with online attacks. The agents stressed the importance of streamlining cohesion with other agencies—both foreign and domestic, as well as governmental and from the private sector—and made an official promise to victims of cyber crimes to pursue and indict perpetrators who have victimized them. "We will always treat victims with dignity and respect, protecting their privacy and data and rigorously adhering to the U.S. Constitution, applicable laws, regulations and policies and the FBI's core values," Gorham said, stating his division's official mission.

Read the full article here.

STATE DEPARTMENT TO CALL ON AMERICAN THINK TANKS TO DISCLOSE FOREIGN FUNDING

Brittany Bernstein | National Review | October 13, 2020

Secretary of State Mike Pompeo on Tuesday will push American think tanks to disclose their foreign donors, signifying a crack down on the significant growth of foreign funding to the organizations in recent years, according to a new report. While disclosure is not legally required, the Department will ask think tanks to "disclose prominently on their websites" funding they receive from foreign sources, according to a statement Pompeo is slated to make on Tuesday, first obtained by the Washington Free Beacon. "To protect the integrity of civil society institutions, the Department requests henceforth that think tanks and other foreign policy organizations that wish to engage with the Department disclose prominently on their websites funding they receive from foreign governments, including state-owned or state-operated subsidiary entities," Pompeo will say in a statement.

Read the full article here.

OVERSEAS PROFESSIONALS AND TECHNOLOGY TRANSFER TO CHINA

Ryan Fedasiuk and Emily Weinstein | Center for Security and Emerging Technology | July 21, 2020

Since the 1990s, the government of the People's Republic of China (PRC) and the Chinese Communist Party (CCP) have encouraged members of the Chinese diaspora to "serve the nation" from abroad, in part by promoting technical exchanges between established groups of overseas professionals and entities in China.1 Many Chinese professional associations (CPAs) operate independent of Party influence, and simply provide networking opportunities and social support to ethnic Chinese living outside China. But some CPAs serve as access points to technical information and expert personnel for Chinese laboratories and state-owned enterprises. This report highlights the scale of China's technology transfer efforts that leverage professional associations abroad.

Read the full article here.

IMMIGRATION POLICY AND THE GLOBAL COMPETITION FOR AI TALENT

Tina Huang and Zachary Arnold | Center for Security and Emerging Technology | June 2020

The United States has historically led the world in technological innovation through its internationally renowned education institutions, innovative industries, top-tier research laboratories and, critically, its unique ability to attract talent worldwide. Immigrants play a key role in sharpening America's technological edge.1 In recent years, the demand for artificial intelligence talent has greatly exceeded domestic supply, leading to a large share of foreign-born AI students, workers and entrepreneurs in the United States.2 Although important, efforts to increase the domestic AI workforce are insufficient to fill the immediate demand for AI talent. At the same time, other countries are developing their own capabilities and institutions in AI and aggressively recruiting AI talent through new immigration policies.

Read the full article here.

AS U.S. VIEWS OF CHINA GROW MORE NEGATIVE, CHINESE SUPPORT FOR THEIR GOVERNMENT RISES

Emily Feng | NPR | September 23, 2020

Polls show widespread distrust toward China is growing in the U.S. over how China initially handled its coronavirus outbreak and ongoing human rights abuses. At the same time, Chinese attitudes toward the U.S. are souring — while popular satisfaction with the Chinese state has grown since the central government quickly brought the pandemic under control through sometimes brutal methods. These recent trends in public sentiment run parallel to a dramatic deterioration in U.S.-China relations, as nationalistic officials in each government play on popular fears and perceptions. U.S. levels of anxiety about China are at historic highs. The latest Pew Research poll, from July, found 73% of American respondents have negative attitudes toward China — the highest percentage since Pew began collecting such data in 2005, when 35% reported negative attitudes toward China.

Read the full article here.