ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

October 27, 2021

ESPIONAGE IS A FUNDAMENTAL ENGINE BEHIND CHINA'S ECONOMIC GROWTH

Stu Cvrk | The Epoch Times | October 19, 2021

The Chinese economy has benefited from decades of purposeful economic espionage focused on acquiring Western technology, intellectual property, and general economic know-how. Communist China's long-term economic strategy is aimed at replacing the U.S.-dominated post-World War II order, which was established by the United Nations and the Bretton Woods international monetary framework, with an "authoritarian capitalist system" controlled by Beijing. A key characteristic of authoritarian capitalism is defined here as "the presence of a capitalist economy on one hand along with the absence or erosion of democracy and civil liberties on the other hand." The strategy involves penetrating, co-opting, and leveraging international institutions in order to gain access to resources, foreign direct investment, advanced technology, and Western methods so that Chinese industry can leap ahead of all foreign competition in the race for next-generation technologies and production capabilities—in short, to achieve world economic dominance over the long haul.

Read the full article here.

US INTEL WARNS CHINA COULD DOMINATE ADVANCED TECHNOLOGIES

Nomaan Merchant | The News & Observer | October 23, 2021

U.S. officials issued new warnings Friday about China's ambitions in artificial intelligence and a range of advanced technologies that could eventually give Beijing a decisive military edge and possible dominance over health care and other essential sectors in America. The warnings include a renewed effort to inform business executives, academics and local and state government officials about the risks of accepting Chinese investment or expertise in key industries, officials at the National Counterintelligence and Security Center said. While the center does not intend to tell officials to reject Chinese investment, it will encourage efforts to control intellectual property and implement security measures. National security agencies under President Joe Biden's administration are making an aggressive public push against China, which some officials have called the greatest strategic threat to the United States. The Biden administration has simultaneously tried to ease some tensions with Beijing dating to the Trump administration and seek common ground on trade and climate change.

Read the full article here.

THE BIGGEST CYBER-THREAT ISN'T HACKERS, IT'S INSIDER THREATS

Misan Etchie | Infosecurity Magazine | October 22, 2021

There is a saying that goes thus, "A man's enemies are those of his own household." This reinforces what many are beginning to realize – insider threats are a bigger danger to enterprise security than external forces are. Insider threats are negligent or malicious activities carried out by employees, contractors or associates in an organization. Insider threats are any cybersecurity hazard and vulnerability that arise either due to employees' maliciousness or carelessness, whether that be someone falling for a phishing attempt or risking security by reusing generic passwords across different sites and applications. A number of individuals affiliated with an enterprise can pose a threat; they include a negligent employee or contractor, a criminal or malicious insider or a credential thief. They can also emerge from ex-employees or third-party vendors with technical knowledge of an organization's systems. Insider threats are every bit as scary as they sound and are rising. Therefore, it is extremely worrisome that these cybersecurity threats to organizations are under-addressed, especially when compared with external threats.

Read the full article here.

STEAL THE FIREWOOD FROM UNDER THE POT – THE ROLE OF INTELLECTUAL PROPERTY THEFT IN CHINESE GLOBAL STRATEGY

Capt. Scott Tosi, U.S. Army | Army University Press | September – October 2020

In September 2015, the United States and China reached an agreement in principle that specified, among other stipulations, that "neither the U.S. or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property [IP]."1 However, less than two years later, China's use of cyber-enabled IP theft was outlined bluntly in the 2017 National Security Strategy, which stated that "every year, competitors such as China steal U.S. intellectual property valued at hundreds of billions of dollars."2 This snapshot of cyber-enabled IP theft represents a broader issue of IP theft by China that spans a wide range of methods and means. According to estimates, China's total annual amount of IP theft ranges from $225 billion to $600 billion; moreover, China is responsible for 50 to 80 percent of all IP theft occurring against the United States. Chinese IP theft has broad implications for the U.S. Army and the Department of Defense (DOD), particularly as U.S. strategic focus shifts from counterinsurgency to large-scale combat operations among great powers.

Read the full article here.

ACADEMICS FEAR NEW LAW IN SINGAPORE

John Ross | Inside Higher Ed | October 22, 2021

Singapore's new foreign interference law will exacerbate the "pervasive culture of academic self-censorship," critics have warned, despite assurances that routine university activities will not be affected. The Foreign Interference (Countermeasures) Act empowers the government to investigate and obstruct "hostile information campaigns" designed to incite social discord in Singapore, influence its political processes or undermine its sovereignty. The legislation specifically targets online activity with foreign origins. It allows the authorities to force internet providers, social media platforms and website operators to block content and disclose information about their users. The bill passed Parliament on Oct. 4 -- just three weeks after it had been tabled -- and will be enacted following presidential assent, which is normally a formality. During parliamentary debates, the home affairs minister, Kasiviswanathan Shanmugam, said the bill would not affect academic activities. "We value the intellectual output, collaborations, exchange of ideas, the work our academics do. They need to link with the rest of the world. It is important for Singapore," he said.

Read the full article here.

WORLD AWAKENS TO DANGER OF IP THEFT – AGAIN. WHAT'S CHANGED THIS TIME?

John Blyler | Design News | October 19, 2021

There was a time when, if you wanted to make semiconductor integrated circuits and chips, you had to have your own fabrication facility or fab. Back then, the semiconductor industry was vertically integrated, with companies owning and operating their fabs and performing the assembly and testing of their own chips. But that began to change in the 1980s with the introduction of the fabless business model, based on intellectual property (IP). Engineers at new startup companies could focus on unique designs without incurring the expense and management associated with owning a fab. Their designs, contained in IP, could be manufactured at a foundry like TSMC. The idea quickly caught on as the fabless IP business model helped create such billion-dollar companies as Apple, Arm, NVIDIA, Qualcomm, and others. Each of these companies now holds vast portfolios of IP related to semiconductor design with revenues from royalty steams earn on IP licensing agreements that reach tens of billions of dollars each. One of the downsides of semiconductor IP is that it's easier to steal than to reverse engineer existing chips. The relentless attacks on the IP of US and European tech companies have been well documented. To appreciate the accelerated pace of these attacks, it helps to have a historical understanding of events.

Read the full article here.

AMERICA MUST PROTECT THESE 5 TECHNOLOGIES IF IT WANTS TO REMAIN A SUPERPOWER, INTELLIGENCE OFFICIALS WARN

Eamon Javers | CNBC | October 22, 2021

U.S. intelligence officials have issued a stark warning: America's status as a global superpower depends on maintaining a lead in five key technologies – and America's rivals are trying to steal every one of them. Officials said they are concerned that foreign theft of American technologies could not only rob the United States of economic leadership in the key sectors, but could threaten the country's ability to even remain active in the industries at all. Officials cited legal and illegal activities, particularly those conducted by China, that have crippled competitiveness in sectors such as steel and solar panels. They also pointed to China's wipeout of the Australian rail industry as an example. "We don't want what happened in those other industries to happen here," said Michael Orlando, acting director of the National Counterintelligence and Security Center, which falls under the Director of National Intelligence. When asked what the impact would be if the U.S. loses supremacy, he said: "It could be severe. We've got to focus on these industries because we can't afford to lose them." In a new report, the NCSC wrote that "these sectors produce technologies that may determine whether America remains the world's leading superpower or is eclipsed by strategic competitors in the next few years."

Read the full article here.

IS U.S. FOREIGN POLICY TOO HOSTILE TO CHINA?

Alkis Konstantinidis | Foreign Affairs | October 19, 2021

We at Foreign Affairs have recently published a number of pieces on U.S. foreign policy toward China and whether it has become too hostile. To complement these articles, we decided to ask a broad pool of experts for their take. As with previous surveys, we approached dozens of authorities with specialized expertise relevant to the question at hand, together with leading generalists in the field. Participants were asked to state whether they agreed or disagreed with a proposition and to rate their confidence level in their opinion. Their answers are below.

Read the full article here.

FEDERAL RESEARCH: AGENCY ACTIONS NEEDED TO ADDRESS FOREIGN INFLUENCE

United States Government Accountability Office | October 5, 2021

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 such as the National Science Foundation (NSF) can address this threat through COI policies and requiring the disclosure of information that may indicate conflicts. In a December 2020 report, GAO reviewed five agencies, including NSF, which together accounted for almost 90 percent of all federal research and development expenditures at universities in fiscal year 2018. GAO found that three of the agencies it reviewed have agency-wide COI policies and two do not (see figure). The three agencies with existing COI policies focus on financial interests and do not specifically address or define non-financial interests, which may include multiple professional appointments. In the absence of agency-wide COI policies and definitions for 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.

Read the full article here.

HOW CAN STATE LEGISLATURES COUNTER CHINESE INFLUENCE IN AMERICAN HIGHER EDUCATION?

Rachelle Peterson | National Association of Scholars | October 20, 2021

Good afternoon. My thanks to Senator Roger Roth for inviting me, and to this committee for taking so seriously the issue of international security in institutions of higher education. My name is Rachelle Peterson, and I am a senior research fellow at the National Association of Scholars. I'm honored to be with you today. My research focuses on Confucius Institutes, most recently how they are morphing into new and increasingly sophisticated tools of Chinese government influence on American college campuses. Confucius Institutes, as you may know, are Chinese government-sponsored centers that began appearing on American college campuses in 2004. In recent years, as these Confucius Institutes have sparked controversy, most have closed down. However, many have been replaced with other, extremely similar programs under new names.

Read the full article here.

PROSECUTOR: CHINESE GOVERNMENT AT CENTER OF ESPIONAGE CASE INVOLVING GE AVIATION

Kevin Grasha | Cincinnati Enquirer | October 19, 2021

In 2018, Yanjun Xu and another man who prosecutors say was a Chinese spy traveled 8,000 miles from China to Belgium to meet with an engineer for GE Aviation. Xu and the other accused intelligence officer, a federal prosecutor said Tuesday in opening statements in Xu's trial, believed the GE Aviation engineer was bringing a hard drive containing confidential information about commercial jet engines. The alleged espionage was part of a Chinese government policy to steal trade secrets from aviation companies, Assistant U.S. Attorney Emily Glatfelter told jurors. She said China wanted to build its own jet engine modeled after GE Aviation's, which she called the most successful in the world. China relies on spies, she said, "to steal what they cannot develop themselves." When FBI agents and Belgian authorities arrested Xu and the other accused spy, the two had multiple cellphones, photos of the engineer and his family and thousands of dollars in U.S. currency wrapped in brown envelopes, Glatfelter said. Xu also had been using an alias, she said.

Read the full article here.

TO PROTECT SENSITIVE DATA, IT SECURITY AND RESEARCHERS MUST ACT AS TEAMMATES

Emily Bamforth | Scoop News Group | October 19, 2021

Colleges and universities are more widely implementing tools like multi-factor authentication and anti-phishing software to protect research data, but the best defense against threats remains the connection between information technology security teams and well-informed researchers, experts told EdScoop. Protecting the data produced through research and development spending at universities, estimated at nearly $84 billion in 2019, is becoming more difficult because of rising cyber threats against the education sector. Protecting data is tricky because these workers often use non-standard software, work on fast-paced, competitive timelines and use unique technology or remote lab environments, said Michael Corn, the chief information security officer at the University of California, San Diego.

Read the full article here.

PROTECTING CRITICAL AND EMERGING U.S. TECHNOLOGIES FROM FOREIGN THREATS

The National Counterintelligence and Security Center | October 2021

Given the unique opportunities and challenges posed by emerging technologies, the National Counterintelligence and Security Center (NCSC) today announced it is prioritizing its industry outreach efforts in a select few U.S. technology sectors where the stakes are potentially greatest for U.S. economic and national security. These sectors produce technologies that may determine whether America remains the world's leading superpower or is eclipsed by strategic competitors in the next few years. These sectors include, but are not limited to: artificial intelligence, bioeconomy, autonomous systems, quantum, semiconductors. As mandated by Congress, a core NCSC mission is to conduct counterintelligence (CI) outreach to the U.S. private sector, academic and research communities, as well as other external stakeholders to arm them with information about foreign intelligence threats to their organizations and ways to mitigate risk.

Read the full article here.

CHINA WIELDS NEW LEGAL WEAPON TO FIGHT CLAIMS OF INTELLECTUAL PROPERTY THEFT

Kevin Colleran | Techi Live Update | September 26, 2021

In four major cases since 2020, Chinese courts granted so-called anti-suit injunctions blocking foreign companies from taking legal action anywhere in the world to protect their trade secrets. Three of the rulings were in favor of Chinese telecom companies—Huawei Technologies Co., Xiaomi Inc. and BBK Electronics. The fourth supported South Korea's Samsung Electronics Corp. in a dispute with Swedish telecom giant Ericsson AB. In the Xiaomi case, the Beijing-based company was granted an anti-suit injunction against InterDigital Inc., a Delaware firm that holds patents on wireless and digital technology used in smartphones.

Read the full article here.