ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

August 5, 2020

NSA WARNS OF SECURITY THREATS FROM MOBILE LOCATION DATA

Maggie Miller | The Hill | August 4, 2020

The National Security Agency (NSA) on Tuesday rolled out guidance warning that location data from mobile and other internet-connected devices could pose a security threat for users if it were accessed by adversaries. The guidance was rolled out as a warning for Defense Department personnel and others with access to sensitive federal systems, but the NSA noted that it could be "useful to a wide range of users." "Using a mobile device—even powering it on—exposes location data," the NSA warned in the guidance. "Mobile devices inherently trust cellular networks and providers, and the cellular provider receives real-time location information for a mobile device every time it connects to the network." "This means a provider can track users across a wide area," the agency noted. "In some scenarios, such as 911 calls, this capability saves lives, whereas for personnel with location sensitivities, it may incur risks. If an adversary can influence or control the provider in some way, this location data may be compromised." The NSA noted that location data could be tracked even if the GPS and cellular data are switched off, warning that a mobile device can track location through WiFi and Bluetooth connections, while websites and apps can also access or guess the location of the user.

Read the full article here.

JAPAN CONSIDERS TOUGHER RULES ON RESEARCH INTERFERENCE AMID US-CHINA TENSIONS

Smriti Mallapaty | Nature | August 4, 2020

The Japanese government is considering tougher rules to address the risk of foreign interference in scientific research, such as more thorough vetting of visa applications from international students and researchers and requiring institutions to declare foreign sources of income. Last month, Japan's cabinet approved an innovation strategy for 2020, which asks government agencies, research institutes and companies to strengthen codes of conduct around research integrity and conflicts of interest, and prevent the outflow of sensitive research and technologies linked to national security, such as quantum computing, artificial intelligence and semiconductor manufacturing. The strategy also proposes that government agencies consider withholding funding from institutions that fail to declare foreign income.

Read the full article here.

RESEARCHER PLEADED GUILTY TO CONSPIRING TO STEAL SCIENTIFIC TRADE SECRETS FROM OHIO CHILDREN'S HOSPITAL TO SELL IN CHINA

U.S. Department of Justice | July 30, 2020

Former Ohio woman Li Chen, 46, pleaded guilty today via video conference in U.S. District Court today to conspiring to steal scientific trade secrets and conspiring to commit wire fraud concerning the research, identification and treatment of a range of pediatric medical conditions. "Once again we see the People's Republic of China (PRC) facilitating the theft of our nation's ingenuity and hard work as part of their quest to rob, replicate and replace any product they don't have the ability to develop themselves," said John C. Demers, Assistant Attorney General for National Security. "Far from being an isolated incident, we see the PRC implicated in around 60 percent of all trade secret theft cases. This continued economic belligerence runs contrary to the values and norms that facilitate the success of our industries and countering it remains among our highest priorities."

Read the full article here.

WHY ARE U.S. INSTITUTIONS WORKING WITH SCIENTISTS LINKED TO CHINA'S MILITARY MODERNIZATION?

John Pomfret | The Washington Post | July 30, 2020

The recent Justice Department case charging four Chinese military officers with visa fraud on suspicion of lying about their service in the People's Liberation Army so they could conduct research in the United States appears to be the tip of an iceberg. As a Hoover Institution report released Thursday documents, researchers from Chinese institutions with the central mission of modernizing China's military have co-authored hundreds of scientific articles with American colleagues. Among those partnering with American researchers are Chinese scientists involved in stealth technology and classified weapons studies, those employed by the PLA's General Arms Department and those engaged in work on high-tech naval systems. The report does not say whether any of the studies done with American partners were directly related to weapons development. Regardless, the report questions why so many academies that serve the advancement of China's military are intent on sending researchers to the United States.

Read the full article here.

NEW REPORT EXPLORES HOW CHINA LEGALLY ACCESSES FOREIGN TECHNOLOGIES TO BUILD MILITARY CAPABILITIES

Rose Tenyotkin, April Herlevi, Alison Kaufman, and Anthony Miller | CNA | June 2020

CNA's China and Indo-Pacific Security Affairs Division provides senior leaders across the US government with timely, high-quality political-military insights to assist them in making informed decisions as they formulate plans and policies for this critical region of the world. As China's global presence has increased, it is necessary to examine the economic dimensions of China's activity and its potential implications for US national security interests. CNA is helping US leaders and officials understand China's economic statecraft in the Indo-Pacific and beyond. Our expanding domains of analysis include international economic engagement, foreign direct investment, technology acquisition, and assessing PRC state-owned and private investments globally, including within the United States.

Read the full report here.

REPORT SHEDS LIGHT ON CHINA'S USE OF MILITARY-LINKED RESEARCHERS

Kate O'Keeffe and Aruna Viswanatha | The Wall Street Journal | July 30, 2020

Researchers in the U.S. have engaged in extensive collaboration with counterparts affiliated with the Chinese military, potentially boosting China's potency as a rival, according to a new report published Thursday by Stanford University's Hoover Institution. The report, from the conservative think tank, identifies 254 papers in a publicly accessible Chinese government-backed academic database. They were written by researchers from 115 U.S. universities and government research labs working with counterparts from seven key research universities and institutes with ties to China's People's Liberation Army. Papers cover a range of topics, from material science to naval engineering, and the Hoover report found instances of the Chinese researchers allegedly hiding or not making clear their defense affiliations. The report concludes that any collaboration and assistance that could boost China as a strategic and military competitor are inimical to U.S. interests "even if the relevant research is unclassified, considered basic or fundamental, and is ultimately published."

Read the full article here.

SCHOLARS CHARGED WITH LYING ABOUT CHINESE MILITARY TIES

Elizabeth Redden | Inside Higher Ed | July 28, 2020

Federal prosecutors last week announced visa fraud charges against three visiting researchers and a graduate student from China accused of lying about their affiliations with the Chinese military on their U.S. visa applications. Prosecutors initially accused the Chinese government of harboring one of the four researchers, Tang Juan, formerly a visiting cancer researcher at the University of California, Davis, at the Chinese consulate in San Francisco. The U.S. Attorney's Office for the Eastern District of California subsequently announced Friday that Tang had been arrested and taken into custody. The charges come at a time of heightened tensions between the U.S. and China -- and at a time when disagreements over issues related to research and allegations of technology theft are front and center in the overall China-U.S. relationship.

Read the full article here.

RECIPIENTS ADVISED TO REPORT UNSOLICITED MYSTERY SEED SHIPMENTS

Kay Ledbetter | Homeland Security Today | July 28, 2020

Texas residents are now among those across the nation receiving mysterious seeds delivered by mail in tiny bags marked as jewelry. U.S. Department of Agriculture officials are on alert because these seeds are unsolicited. Kevin Ong, Ph.D., Texas A&M AgriLife Extension Service plant pathologist and director of the Texas Plant Disease Diagnostic Laboratory in College Station, said the concern arises because these packages have seeds in them instead of what is listed, and there is no information on what type of seeds they might be. "We don't know what kind of seeds they are," Ong said. "Not knowing what the seeds are could potentially open our agriculture industry up to noxious weeds. If that proves to be the case, if they take hold, they could impact agriculture negatively."

Read the full article here.

HOW EUROPE IS FIGHTING CHINESE INFLUENCE

Jimmy Quinn | National Review | July 31, 2020

In July alone, European governments have spurned Huawei and criticized Beijing's handling of human rights. Just this week, the European Union imposed sanctions for the crackdown in Hong Kong. This deterioration of relations has coincided with an awakening to Beijing's influence operations and coercive diplomacy in the months since the start of the coronavirus pandemic. Chinese diplomats have pressured European officials into accepting their preferred outcomes, occasionally with some success. In April, they convinced EU officials to water down a report that initially cast blame on China for the spread of the virus. But these efforts have also triggered a backlash, such as when the Chinese embassy in France published an article that falsely claimed that French nursing-home caregivers had left elderly patients to die. And in June, another EU report called out Beijing for its disinformation efforts.

Read the full article here.

THEFT OF U.S. COMPANIES' IP ASSETS AND OTHER NATIONAL SECURITY ISSUES INVOLVING FOREIGN GOVERNMENTS AND FOREIGN-CONTROLLED ENTITIES

Nick Oberheiden | JD Supra | July 29, 2020

Federal authorities have recently described the threat of economic espionage from foreign entities as one of the greatest threats to the economic vitality of the United States, and this has led to an increase in investigations and prosecutions targeting foreign nationals as well as U.S. citizens who control foreign entities. At present, the threat is primarily linked to the Chinese government and China-controlled entities; however, entities controlled by other foreign governments and non-governmental entities also represent a significant concern as well.

Read the full article here.

ICE REVERSES INTERNATIONAL STUDENT POLICY FOR UPCOMING SCHOOL YEAR AFTER BACKLASH

Jessica Fetrow | The Tower | July 26, 2020

The United States' Immigration and Customs Enforcement (ICE) has rescinded its decision to bar international students from entering the country if all of their courses are online-only for the fall 2020 semester. The initial decision to prohibit foreign students from residing in the country was met with significant backlash from universities, states, and lawmakers. The Department of Homeland Security announced on July 6 that it was prohibiting students from residing in the country on F-1 or M-1 visas if their classes were all held online. Under the proposed restrictions, the department would not issue any more of those visas and individuals residing in the country under those visas would be asked to leave or face removal proceedings. While the U.S. Student and Exchange Visitor Program (SEVP) does not typically allow international students to reside in the country under F-1 or M-1 visas if their coursework is strictly online, ICE issued an exception to this standard in March in light of the rapidly-evolving coronavirus pandemic. The U.S. had announced that this policy would not apply for the fall 2020 semester.

Read the full article here.

SOME ILLEGALLY MAILED MYSTERY SEEDS FROM CHINA IDENTIFIED: USDA

Courtney Moore | Fox Business | August 2, 2020

The U.S. Department of Agriculture's division of Animal and Plant Health Inspection Service has identified some of the mysterious seed packets that seem to have been sent from China to more than 1,000 American households. As of Wednesday, 14 of the seed species had been identified, according to the agency's Deputy Administrator Osama El-Lissy. This includes food staples like mustard and cabbage as well as herbs like mint, sage, rosemary and lavender. Flower breeds such as morning glory, hibiscus and roses were also discovered. "At this time, we don't have any evidence indicating this is something other than a 'brushing scam' where people receive unsolicited items from a seller who then posts false customer reviews to boost sales," the agency wrote in a statement. "[The] USDA is currently collecting seed packages from recipients and will test their contents and determine if they contain anything that could be of concern to U.S. agriculture or the environment."

Read the full article here.

PENTAGON PLANNING FOR THE NEXT 25 YEARS OF CYBERSECURITY

Billy Mitchell | FedScoop | July 27, 2020

The Department of Defense isn't just focused on the cybersecurity of today — it's looking 25 years into the future. The Pentagon's undersecretary of research and engineering — essentially the department's CTO — issued a request for information late last week, asking for help building out a roadmap of science and technology activities related to advances in cybersecurity over the next two-and-a-half decades in line with the 2018 National Defense Strategy. The solicitation asks interested parties to help inform the Pentagon's future cybersecurity guideposts by sharing "their R&D projections, technical capabilities, and demonstrated experiences in cybersecurity and cyberspace operations," the RFI says.

Read the full article here.

CYBERCRIMINALS GAIN A HACKING EDGE ON GOVERNMENT AND HIGHER ED

Tod Newcombe | Governing | July 28, 2020

COVID-19 is fueling an uptick in ransomware attacks and giving cybercriminals an edge. According to Government Technology's* cybersecurity reporter Lucas Ropek, a report from cybersecurity vendor Check Point Research shows that COVID-themed phishing attacks increased globally across all sectors between February and late April, jumping from 5,000 per week to over 200,000 per week. These attacks occurred in almost all sectors, including "governments, industry, healthcare, service providers, critical infrastructure and consumers." For state and local governments, that has meant that hackers have increased their "focus on so-called 'soft targets' — local governments, public administration agencies, education, and even hospitals," reports vendor SonicWall in their 2020 mid-year report. Some states have been hit more heavily than others, with Maryland, Florida, Michigan, and Tennessee having some of the highest rates.

Read the full article here.

EXCLUSIVE: U.S. TO ORDER DRASTIC REDUCTION IN CHINESE DIPLOMATS AMID SURGE IN SPY CASES

Bill Gertz | The Washington Times | July 28, 2020

The Trump administration is preparing to order China to sharply reduce the number of diplomats posted in the United States to levels equal to the number of American diplomats stationed in China, senior State Department officials said. The action seeks in part to reduce the burden on FBI counterintelligence agents, who in recent months have devoted 2,000 special agents to catching Chinese spies and their agents, the senior official said. FBI Director Christopher A. Wray said recently that the bureau is opening a new Chinese-related case on average every 10 hours. "By August, we want reciprocal levels and access" for U.S. diplomats abroad, said one senior U.S. official, who spoke on background in advance of the formal announcement expected this week.

Read the full article here.

DISTANCE LEARNING MAKES UNIVERSITIES MORE VULNERABLE TO CYBERATTACK

Karen Roby | TechRepublic | July 28, 2020

TechRepublic's Karen Roby spoke with Carlos Morales of VP and general manager of DDoS Security Services at NetScout Systems, which provides application and network performance management products, about security concerns with remote learning at universities. The following is an edited transcript of their conversation. Carlos Morales: We had a really interesting thing. We've been seeing distributed denial of service attacks (DDoS), against universities for years. But we had a particular incident recently where a university in the US was attacked, and they asked us to help forensically, or basically trace back, what the attack sources were, trying to figure out if it was a student, or if it was some type of malicious actor. And the thing that was very unusual about this was we were able to trace back the attack to another university in the same state, in fact. So it was a rival university that was actually generating the traffic.

Read the full article here.

CMMC RULE CHANGE 'UNDETERRED' BY PANDEMIC, WITH REQUIREMENTS COMING SOON

Jackson Barnett | FedScoop | July 31, 2020

The last step for the Department of Defense to start putting its new cybersecurity requirements into contracts is on course, after concerns the coronavirus pandemic would delay its implementation.

The Cybersecurity Maturity Model Certification (CMMC) program is now just waiting for the Office of Management and Budget to approve a rule change to the Defense Federal Acquisition Regulations (DFAR) that would allow the DOD to write clauses into requests for proposals requiring CMMC in all contracts. CMMC is a five-level cybersecurity maturity model for which all defense contractors will need to receive a third-party verification before they can bid for work with the Pentagon. The DOD program office in charge of CMMC had previously said some delays would occur since the rule change process requires a public hearing, which is difficult to schedule while group gatherings are unsafe.

Read the full article here.

RANSOMWARE CRIMINALS ARE TARGETING U.S. UNIVERSITIES

Nir Kshetri | Nextgov | July 20, 2020

As COVID-19 cases in the U.S. continue to climb, government and higher education leaders have been focused on doing what it takes to protect campus communities from the global pandemic. But college and university leaders would be wise if they were just as vigilant about protecting their sensitive data from the cybercriminals who are becoming increasingly sophisticated about encrypting the colleges' data and making the colleges pay a ransom to get it back. One of the latest examples is a ransomware attack that struck the University of California, San Francisco on June 1. In that case, cybercriminals used the NetWalker malware to encrypt data on the servers of the university's school of medicine. This malware targets corporate networks and encrypts the data it finds on the attacked devices. This means that the device owner cannot access data on the device until a ransom in cryptocurrency demanded by the criminal is paid. The criminal gang behind NetWalker has victimized dozens of organizations.

Read the full article here.

UNIVERSITY 'NAIVE' TO PARTNER WITH CHINESE INSTITUTE, SECURITY EXPERT SAYS

Eleisha Foon | RNZ | July 27, 2020

In April 2018, the University of Canterbury signed an agreement with Harbin Institute of Technology to collaborate on teaching and research. China has been accused of stealing sensitive technologies and intellectual property through academic exchanges and some experts warn the university could be putting the country's national security at risk for jumping into a partnership before doing its homework. Experts have called the University of Canterbury "naive" to enter into an agreement in April 2018 with Harbin Institute of Technology (HIT), which is widely known to have links to the Chinese military. UC's Deputy Vice-Chancellor Professor Ian Wright said no inquiries about HIT's defence links were made at the time, but said New Zealand's university sector had been increasingly aware of the sensitivity of some specific areas of research and technology.

Read the full article here.

FORMER TENURED WVU PROFESSOR SENTENCED FOR FRAUD AGAINST THE UNIVERSITY, FEDERAL GOVERNMENT

WAJR | July 30, 2020

Former WVU professor, Dr. James Patrick Lewis, of Fairview, has been sentenced to three months in prison for fraud involving West Virginia University, according to the U.S. Department of Justice. Lewis was also fined $9,363 for the cost of the incarceration and ordered to pay $20,189 in restitution to WVU, which is paid in full. Lewis was a tenured professor at West Virginia University in the physics department, specializing in molecular reactions used in coal conversion technologies. In July 2017, Lewis entered into a contract of employment with the People's Republic of China through its "Global Experts 1000 Talents Plan." China's Thousand Talents Plan is one of the most prominent Chinese Talent recruit plans that are designed to attract, recruit, and cultivate high-level scientific talent in furtherance of China's scientific development, economic prosperity and national security. These talent programs seek to lure overseas talent and foreign experts to bring their knowledge and experience to China and reward individuals for stealing proprietary information.

Read the full article here.

UNIVERSITY OF ARKANSAS PROFESSOR INDICTED FOR WIRE FRAUD, PASSPORT FRAUD

KTLO | July 29, 2020

Acting United States Attorney for the Western District of Arkansas David Clay Fowlkes, Assistant Attorney General for National Security John C. Demers and FBI Special Agent in Charge Diane Upchurch of the FBI Little Rock Field Office, announced Wednesday Simon Saw-Teong Ang, 63, of Fayetteville was indicted by a federal grand jury in the Western District of Arkansas on 42 counts of wire fraud and two counts of passport fraud. "This case is the result of the tireless efforts of our federal law enforcement partners at the FBI and the Diplomatic Security Service," Acting US Attorney Fowlkes states. "The wire fraud in this case affected not only the University of Arkansas, but several other important United States Government agencies, such as the National Aeronautics and Space Administration (NASA) and the United States Air Force. It is our sincere hope that this investigation sends a strong message to those who would attempt to defraud the federal government."

Read the full article here.

WHAT'S THIS? A BIPARTISAN PLAN FOR AI AND NATIONAL SECURITY

Tom Simonite | Wired | July 30, 2020

U.S. Representatives Will Hurd and Robin Kelly are from opposite sides of the ever-widening aisle, but they share a concern that the US may lose its grip on artificial intelligence, threatening the American economy and the balance of world power. Thursday, Hurd (R-Texas) and Kelly (D-Illinois) offered suggestions to prevent the US from falling behind China, especially, on applications of AI to defense and national security. They want to cut off China's access to AI-specific silicon chips and push Congress and federal agencies to devote more resources to advancing and safely deploying AI technology. Although Capitol Hill is increasingly divided, the bipartisan duo claim to see an emerging consensus that China poses a serious threat and that supporting US tech development is a vital remedy.

Read the full article here.

SOCIAL ENGINEERING: HACKING BRAINS…IT'S EASIER THAN HACKING COMPUTERS

Chris Orr | Trip Wire | July 29, 2020

The audience in the room is weirdly quiet. The contestant is in a small plexiglass booth with nothing but a phone, a laptop computer and some notes. On a set of speakers outside, the booth broadcasts the sounds of a dial tone as a woman on the stage begins to dial a number. It is apparent she is not phoning a friend. The dial tone changes to a ring tone, and moments later, the other end picks up. And with those words, the game begins. Human beings—well most of us anyways—are wired to help. If we see someone in trouble, we want to assist them. It is what has kept our rather soft and squishy species alive when there were lions and tigers and bears trying to eat us. Strength in numbers and all that. When we see a car broken down on the side of the road, and if we notice that little, old lady trying to cross the street, there is that instinct to lend aid. In the social engineering world, attackers depend on and exploit this instinct. There is a rather common cliché in InfoSec: the weakest link in computer security is the human. You can have the strongest firewalls, the most expensive intrusion detection, and/or the most complex security system in the world, but none of that matters if the janitor leaves the doors unlocked or if the front desk staff freely gives out information about your company.

Read the full article here.

UNIVERSITY OF CANTERBURY COLLABORATING WITH INSTITUTE LINKED TO CHINESE MILITARY

Martin Van Beynen | Stuff | July 27, 2020

The University of Canterbury (UC) decided to collaborate with a top Chinese university that has strong links with the Chinese military without asking about the organisation's defence connections. In April 2018, UC signed an agreement with Harbin Institute of Technology (HIT), based in Harbin, Weihai and Shenzhen, to collaborate on teaching and research. According to work done by The Australian Strategic Policy Institute (ASPI), a Canberra-based think tank partially funded by the Australian Government, the Harbin Institute is one of the main Chinese universities doing research in "sensitive civil-military technologies". As one of 'Seven Sons of National Defence' the university is prominent in research on ballistic missiles, information and cyber warfare and nuclear engineering, ASPI says.

Read the full article here.

INCLUSION IS OUR ROADMAP BACK TO GLOBAL SCIENCE DOMINANCE

Dr. Kafui Dzirasa | The Hill | July 26, 2020

Inclusion is our roadmap back to global science dominance
© Getty
Every tax-payer dollar invested in biomedical research yields up to three times the benefit to the U.S. economy, making our push towards science dominance more imperative than ever. The emergence of COVID19 has prompted a global vaccine race, the need to protect national assets in lower earth orbit has motivated the creation of the U.S. Space Force, and strategies to ameliorate the impacts of global climate change continue to shape our international alliances. Each of these U.S. science thrusts offers the potential for profound economic benefits in the geopolitical arena. They also highlight important security risks. With a growing appreciation for foreign threats to our scientific, technology, engineering, and math (STEM) research enterprise, some have proposed mitigation policies centered on expunging or banning foreign scientists from preventing their access to U.S. technology and intellectual property. At their worst, these policies have the potential to demolish our nation's long-held and growth-promoting strategy of facilitating the immigration of science talent from across the world. Even under the best circumstances, for which these policies are selectively and surgically applied to the foreign scientists that truly present a security threat, they only amount to playing defense. The pathway back to global science dominance will require a decisive offensive strategy as well. Adopted into law in January 2017, the American Innovation and Competitiveness Act (AICA) sponsored by Sen. Corey Gardner (R-Colo.) laid out such an offensive strategy for promoting U.S. innovation and maintaining our nation's competitiveness in the global arena.

Read the full article here.

LIMITING LOCATION DATA EXPOSURE

U.S. National Security Agency | August 2020

Mobile devices store and share device geolocation data by design. This data is essential to device communications and provides features—such as mapping applications—that users consider indispensable. Mobile devices determine location through any combination of Global Positioning System (GPS) and wireless signals (e.g., cellular, wireless (Wi-Fi®), or Bluetooth® (BT)). Location data can be extremely valuable and must be protected. It can reveal details about the number of users in a location, user and supply movements, daily routines (user and organizational), and can expose otherwise unknown associations between users and locations.

Read the full article here.

FBI LOOKING INTO POSSIBLE CHINESE SPYING ON UT'S COVID RESEARCH

Brittany Britto | Houston Chronicle | July 30, 2020

The FBI is investigating whether the Chinese government attempted to illegally obtain COVID-19 research from American universities, including the University of Texas campuses in Austin and San Antonio, UT officials confirmed to the Houston Chronicle. The federal law enforcement agency told UT-Austin officials last week that the closure of the Chinese Consulate in Houston sparked the probe, Daniel Jaffe, UT's interim executive vice president and provost, wrote in an email to the university's faculty, graduate and post-doctorate students on Monday. As a result of this "ongoing and evolving national situation," the FBI will contact UT researchers "about the role of the consulate and efforts by the Chinese government to illegally procure research from American universities," Jaffe said. The University of Texas at San Antonio received similar contact from the FBI.

Read the full article here.

CAN CHINA'S MILITARY WIN THE TECH WAR?

Anja Manuel and Kathleen Hicks | Foreign Affairs | July 29, 2020

As the Chinese government has set out to harness the growing strength of the Chinese technology sector to bolster its military, policymakers in the United States have reacted with mounting alarm. U.S. officials have described Beijing's civil-military fusion effort as a "malign agenda" that represents a "global security threat." And as China's defense capabilities have grown, some Western policymakers have started to wonder whether the United States needs to adopt its own version of civil-military fusion, embracing a top-down approach to developing cutting-edge technologies with military applications. Chinese President Xi Jinping formalized the concept of civil-military fusion as part of the extensive military reforms laid out in his 2016 five-year plan. He established a new Central Commission for Integrated Military and Civilian Development, with himself as its head. The commission's goal is to promote the development of dual-use technology and integrate existing civilian technologies into the arsenal of the People's Liberation Army (PLA).

Read the full article here.

DOD TASK FORCE FOCUSES ON PREVENTING TECHNOLOGY THEFT

Jack Browne | Microwaves & RF | December 4, 2019

Technology theft plagues not just commercial and industrial businesses but advanced military electronic systems as well. Attempts are made each year by foreign governments to steal technological resources and intellectual property (IP) worth billions of U.S. dollars, prompting the Department of Defense (DoD) to establish its Protecting Critical Technology Task Force. Although the technology theft usually occurs via the communications networks of contracting companies and their computer networks, the results are as devastating to the DoD as to the company. The officer leading the DoD's Protecting Critical Technology Task Force, Air Force Major General Thomas E. Murphy, admits that the technology theft is in the area of billions of dollars, although it is the negative effects on this country's military capabilities that is a much greater concern: "The consequence is the erosion of the lethality of the joint force. You cannot put a price on that." He explains that it may not be possible to prevent a country from hacking into a company's computer network to steal technology, but it is important for the DoD to learn about the loss as quickly as possible.

Read the full article here.

‘CHINA IS STEALING OUR STUFF AND THEY’RE NOT EVEN HIDING IT’: US TECH PROTECTION TASK FORCE ‘IT’S NO WONDER WHY THEIR STUFF LOOKS REMARKABLY LIKE OURS’: PROTECTING CRITICAL TECHNOLOGY TASK FORCE DIRECTOR

Tim Hinchliffe | The Sociable | October 31, 2019

In China there is a saying, “Picking flowers in the US to make honey in China.” The US DoD tech protection task force has another saying, “China is stealing our stuff!” “China and the others are stealing our stuff, and it is causing the erosion of the lethality of the joint force,” said Air Force Maj. Gen. Thomas E. Murphy, who is the director of the Protecting Critical Technology Task Force of the Department of Defense (DoD). In response to China stealing technology from the US and eroding the force’s lethality, Murphy called upon everyone working in technology to “up your game, and get your cybersecurity in order,” at the Association of the US Army (AUSA) forum on Russia and China.

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