ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

December 7, 2022

ANNUAL REPORT TO CONGRESS ON MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA

U.S. Department of Defense | 2022

The 2022 National Security Strategy identifies the People's Republic of China (PRC) as the only competitor with the intent and, increasingly, the capacity to reshape the international order. The Department of Defense (DoD) annual report on military and security developments involving the PRC charts the current course of the PRC's national, economic, and military strategy and offers Congress insight on the tenets of Beijing's ambitions and intentions. The PRC's strategy entails a determined effort to amass and harness all elements of its national power to place the PRC in a "leading position" in an enduring competition between systems. As expressed in the 2022 National Defense Strategy, the PRC presents the most consequential and systemic challenge to U.S. national security and the free and open international system. In this decisive decade, it is important to understand the contours of the People's Liberation Army's (PLA) way of war, survey its current activities and capabilities, and assess its future military modernization goals. In 2021, the PRC increasingly turned to the PLA as an instrument of statecraft as it adopted more coercive and aggressive actions in the Indo-Pacific region.

Read the full article here.

IT'S FINALLY HERE: PENTAGON RELEASES PLAN TO KEEP HACKERS OUT OF ITS NETWORKS

Lauren C. Williams | Defense One | November 23, 2022

Defense agencies have until 2027 to convert their networks to architectures that continually check to make sure no one's accessing data they shouldn't. This shift to zero trust principles is at the core of the Pentagon's new five-year plan to harden its information systems against cyberattacks. The strategy and roadmap were released on Tuesday. To get there, agencies can improve their existing environments, adopt a commercial cloud that already meets DOD's zero trust specifications, or copy a prototype of a private cloud, David McKeown, the Pentagon's acting principal deputy chief information officer, told reporters. And to help enforce it, the DOD chief information office will track their spending. "We will hold them accountable by asking them to build a plan," McKewon said. "And as a part of that capability planning guidance…they have to come back to us and show us in their budgets how much they're spending on zero trust and what they're getting for that." McKeown said implementation shouldn't change the user experience much, other than extra authentication steps to make sure the right people are accessing information.

Read the full article here.

HOW CHINA IS TRYING TO TURN THE US CHIPS ACT TO ITS FAVOR

SZ Tan and Peter W. Singer | Defense One | November 16, 2022

When the Chips and Science Act (frequently referred to as the CHIPS Act) was signed into law in August, President Biden and Congressional lawmakers celebrated. The legislation included subsidies to bolster America's domestic semiconductor industry and tackle supply chain vulnerabilities, addressing key national security concerns with China. The Biden administration boasted that the CHIPS Act would lower costs, create jobs, strengthen supply chains, and counter China. But China has not taken the news lying down. The PRC has mobilized a strategic communications campaign to undermine support for the Act. "A perfect example of overreacting and coercion," tweeted Hua Chunying, a spokesperson for the PRC's Ministry of Foreign Affairs, shortly after the bill became law. Hua drew an analogy of the world as a classroom, where everyone is studying hard to get good grades, and suddenly, one student cuts the electricity and threatens the other students in the name of upholding classroom order. "Anyone like this guy? Seriously?" she added. As Hua's tweet suggests, the PRC counter-offensive aims to depict the U.S. as a fading global hegemon trying to tip the global playing field back in its favor.

Read the full article here.

DOES THE UK WANT MORE OR FEWER INTERNATIONAL STUDENTS?

Nic Mitchell | University World News | December 2, 2022

Just as British Council Education Director Maddalaine Ansell was stressing the importance of showing that the United Kingdom "values our international students" and wants to "make their journey as easy as possible" at the first Going Global Asia Pacific conference in Singapore, the UK government was struggling to hold a common line over whether it wants more or fewer foreign students studying at British universities. Higher education leaders in the United Kingdom must have felt a sense of déjà vu when they saw newspaper headlines warning of a 'Student visa crackdown' and 'Foreign students face ban from universities' after a government briefing to political correspondents sought to clarify how Prime Minister Rishi Sunak intended to respond to record levels of migration. This is because arguments from some government ministers, including Home Secretary Suella Braverman, had echoes of previous cabinet infighting when Theresa May was the Conservative Party prime minister in 2017.

Read the full article here.

IMPROVED EXPORT CONTROLS ENFORCEMENT TECHNOLOGY NEEDED FOR U.S. NATIONAL SECURITY

Gregory C. Allen, Emily Benson, and William Alan Reinsch | Center for Strategic and International Studies
December 5, 2022

As technology has become increasingly central to strategic competition with Russia and China, export controls have moved to the forefront of U.S. foreign policy on technology issues. Most notably, restricting Russia's access to advanced technology through export controls is a key part of the U.S. response to Russia's invasion of Ukraine, as U.S. government officials have repeatedly stated. Unfortunately, nearly all the debate is focused on whether and when to apply export controls, not how to ensure that export controls are effectively administered and enforced once applied. The Bureau of Industry and Security (BIS) at the Department of Commerce oversees most export controls. Unfortunately, BIS is increasingly challenged by worldwide smuggling and export control evasion networks, especially those that are supported by Russia and China. Investigators have examined the wreckage of downed Russian weapons systems in Ukraine and found that they contain U.S. and allied components, including electronics that were manufactured years after the implementation of the 2014 Russia export controls.

Read the full article here.

INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (ITAR) COMPLIANCE PROGRAM GUIDELINES

U.S. Department of State | Bureau of Political-Military Affairs, Directorate of Defense Trade Controls, and Office of Defense Trade Controls Compliance | December 5, 2022

This document contains information on the elements of an effective ITAR Compliance Program (ICP) and how to design and implement an ICP for organizations that manufacture, export, broker, or temporarily import defense articles and defense services described on the United States Munitions List (USML). The purpose of an ICP is to establish robust policies and procedures to ensure that organizations and their staff who engage in ITAR-controlled activities do so in compliance with the ITAR, Title 22 of the Code of Federal Regulations in parts 120- 130, issued pursuant to the Arms Export Control Act (AECA) (22 U.S.C. § 2751 et seq.), as amended. Operating an effective ICP helps organizations integrate ITAR requirements into their business and research processes and helps mitigate the risk of violating the regulations. The elements in this document provide a foundation for an ICP's basic structure and function and are not intended to be exhaustive.

Read the full article here.

MARYLAND PROHIBITS TIKTOK FOR EXECUTIVE BRANCH OF STATE GOVERNMENT

FOX 5 DC Digital Team | FOX 5 Washington DC | December 6, 2022

Maryland Governor Larry Hogan has announced that the state has issued an emergency directive to prohibit the use of TikTok for the executive branch of the state government. The directive specifically prohibits certain Chinese and Russian-influenced products and platforms including TikTok. Gov. Hogan's office says these entities present an unacceptable level of cybersecurity risk to the state and may be involved in activities such as cyber-espionage, surveillance of government entities and inappropriate collection of sensitive personal information. "There may be no greater threat to our personal safety and our national security than the cyber vulnerabilities that support our daily lives," said Gov. Hogan. "As the cyber capital of America, Maryland has taken bold and decisive actions to prepare for and address cybersecurity threats.

Read the full article here.

CONTRACTORS' RELUCTANCE TO WORK WITH PENTAGON ON CYBERSECURITY IS LEAVING VULNERABILITIES, DOD OFFICIAL SAYS

Lauren C. Williams | Defense One | November 16, 2022

Waiting for defense contractors to voluntarily talk about their cybersecurity efforts and problems is leaving gaps in security, a top defense cyber official said Wednesday. "There is a little bit of reluctance for a company to share anything with us. Like if we were to go in and take a look at their network and find out that it is abysmal. They wouldn't want that information to be leaked," David McKeown, the Pentagon's acting principal deputy CIO, said at Politico's Defense Summit. "We're not prescriptive in nature, as to them coming to us and working with us. And that's the failing point right now: that it's all voluntary." Companies are supposed to adhere to a set of cybersecurity standards, NIST 800-171, but DOD assessments show most vendors fail, he said. McKeown listed various ways the Defense Department's cyber experts can help its vendors, free of charge: on-site network assessments, sharing threat intelligence, shoring up email security, providing protective DNS, and more. But vanishingly few companies take advantage of the offerings: around 1 percent of DOD's hundreds of thousands of contractors, he said.

Read the full article here.

MOST US DEFENSE CONTRACTORS FAIL BASIC CYBERSECURITY REQUIREMENTS

Menghan Xiao | SC Media | December 1, 2022

Nearly nine out of ten US defense contractors fail to meet basic cybersecurity minimums, according to research commissioned by CyberSheath. CyberSheath's survey of 300 US-based Department of Defense (DoD) contractors found that just 13% of respondents have score of 70 or above in the Supplier Performance Risk System (SPRS), the Department of Defense's primary system for assessing supplier and product risk for contractors who handle unclassified information. According to the Defense Federal Acquisition Regulation Supplement (DFARS), a score of 110 is required for full compliance. While the researchers noted that critics of the system have anecdotally considered a score of 70 to be "good enough," most contractors still have not met even that baseline. "The report's findings show a clear and present danger to our national security," said Eric Noonan, CEO of CyberSheath. "We often hear about the dangers of supply chains that are susceptible to cyberattacks. The [defense industrial base] is the Pentagon's supply chain, and we see how woefully unprepared contractors are despite being in the threat actors' crosshairs."

Read the full article here.

LEADING RESEARCH UNIVERSITIES REPORT

Association of American Universities | Business Roundtable | December 2, 2022

AAU and the Business Roundtable published a joint report last month on ways the United States should reform its immigration policies to continue attracting and retaining the world's top STEM talent to study, conduct research, and work here. As the organizations representing the presidents of America's leading research universities and the CEOs of America's leading corporations, AAU and BRT understand that international students, scientists, and engineers help drive cutting-edge research and development, fill jobs in critical STEM fields, advance national security, and bolster the U.S. economy by generating new domestic startups and businesses. The report outlines the massive contributions that international scholars and workers make to our country and makes several recommendations to reduce or eliminate current barriers preventing these individuals from studying or working in the United States.

Read the full article here.

US STATE AND LOCAL GOVERNMENTS CONTINUE TO BUY RISKY CHINESE TELECOMS EQUIPMENT

Matthew Humphries | PCMag | October 27, 2022

Despite all the warnings, schools, colleges, universities, prisons, hospitals, and public transit systems across the US continue to purchase equipment and services from Chinese companies viewed as a national security concern. As Axios reports(Opens in a new window), that's the findings of a 53-page report(Opens in a new window) from the Center for Security and Emerging Technology (CSET), and it may come as a surprise considering there has been a federal ban on purchasing equipment from Huawei, ZTE, Hikvision, Dahua, and Hytera since the 2019 National Defense Authorization Act. However, federal bans don't apply to state and local governments, and so sales have continued. The CSET report found that 1,681 state and local government entities purchased equipment and services from suppliers associated with those five Chinese companies between 2015 and 2021. Purchases have fallen more recently, but over 600 were made last year alone for smartphones, surveillance cameras, and network hardware. The total spend is roughly $45 million over the seven year period, with most of the equipment being installed in public schools, colleges, and universities.

Read the full article here.

‘TIMELY VERSUS ACCURATE’ DOD STRUGGLES SHED LIGHT ON CYBER INCIDENT REPORTING CHALLENGES

Justin Doubleday | Federal News Network | November 21, 2022

The Defense Department has fewer reported cyber incidents today than it did seven years ago, but DoD cybersecurity organizations and defense contractors are struggling to share timely, accurate information about those events, according to a new report from the Government Accountability Office. GAO’s report sheds light on the challenges DoD faces in sharing information about network intrusions and other cyber events as cybersecurity remains a perennial top management challenge for the Pentagon. It also comes at a time when the Biden administration is developing new rules that will require critical infrastructure sectors to report cyber incidents to the government. DoD reported more than 12,000 cyber incidents between 2015 and 2021, the report shows. However, the number of reported incidents dropped off starkly in recent years. In 2015 alone, DoD reported 3,880 cyber incidents in 2015. But in 2021, the department reported just 948 incidents. Jennifer Franks, director of GAO’s IT and cybersecurity team, said the finding correlates with how DoD and other agencies have improved their perimeter defenses and intrusion detection technologies over the past seven years.

Read the full article here.