ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

June 8, 2023

U.S., ROK AGENCIES ALERT: DPRK CYBER ACTORS IMPERSONATING TARGETS TO COLLECT INTELLIGENCE

National Security Agency | June 1, 2023

The National Security Agency (NSA) is partnering with several organizations to highlight the Democratic People's Republic of Korea's (DPRK) use of social engineering and malware to target think tanks, academia, and news media sectors. To help protect against these DPRK attacks, NSA and partners are publicly releasing the Cybersecurity Advisory (CSA), "North Korea Using Social Engineering to Enable Hacking of Think Tanks, Academia, and Media." "DPRK state-sponsored cyber actors continue to impersonate trusted sources to collect sensitive information," said Rob Joyce, NSA director of Cybersecurity. "Education and awareness are the first line of defense against these social engineering attacks." The agencies — the Federal Bureau of Investigation (FBI), U.S. Department of State, and the Republic of Korea's (ROK) National Intelligence Service, National Policy Agency, and Ministry of Foreign Affairs — have observed sustained information gathering efforts originating from a specific set of DPRK cyber actors known collectively as Kimsuky, THALLIUM, or VELVETCHOLLIMA.

Read the full article here.

DESPITE RISKS, EU CONTINUES TO FUND RESEARCH WITH CHINESE MILITARY-LINKED UNIVERSITIES

David Matthews and Richard L. Hudson | Science Business | May 16, 2023

Despite efforts to prevent EU technology leaking to China's military, the European Commission is continuing to fund at least five research projects involving some of China's top military-linked universities. The projects, research by *Science|Business* finds, involve heat transfer, data security and other technologies that could have dual civilian and military use. China's participation includes four of its so-called Seven Sons of National Defence, top-ranked universities controlled by the industry ministry and producing most technical graduates that work for its state defence industry. Under standard EU rules, the Chinese get their own funding for their work in the projects, but as official "participants" they can share in the European research, meetings and staff exchanges. The projects in question are five on-going Marie Skłowdowska Curie Actions (MSCA), that facilitate staff exchanges and network-building among research institutions. Four of the five were started under the EU's old Horizon 2020 programme, but a fifth began only this March under the Horizon Europe programme. They include €437,000 to improve heat dissipation in electronic devices, €639,400 for low-carbon cooling systems, and €1.1 million for electric motors.

Read the full article here.

CHINA INVESTING IN OPEN-SOURCE INTELLIGENCE COLLECTION ON THE U.S.

Julian E. Barnes | The New York Times | June 1, 2023

A new report outlines Chinese efforts to mine public information from the Pentagon, think tanks and private companies to gain insight on the American military. China's intelligence agencies are investing deeply in open-source intelligence to learn more about the capabilities of the American military in the Pacific and beyond, according to a new report. The analysis, by the threat intelligence company Recorded Future, details efforts by China's government and companies to collect publicly available data from the Pentagon, think tanks and private firms — information Beijing's military can use to help plan for a potential conflict with the United States.

Read the full article here.

FORMER CHIEF SCIENTIST FOR GTRI PLEADS GUILTY TO CONSPIRING TO DEFRAUD GEORGIA TECH AND THE CIA

Homeland Security Today | May 28, 2023

Maloney suggested that they try to force Georgia Tech to shut down the audit by telling the auditors that the items charged to Fraley's PCard were purchased for use on a classified CIA contract. James G. Maloney, who served as the Chief Scientist for the Georgia Tech Research Institute (GTRI), has pleaded guilty to conspiring to defraud Georgia Tech and the Central Intelligence Agency (CIA). Maloney's conspirators, James J. Acree and James D. Fraley, III, pleaded guilty to the same charge in 2016. "These defendants violated the trust placed in them by Georgia Tech and the CIA in allowing their judgment to be clouded by greed," said U.S. Attorney Ryan K. Buchanan. "The seven-year delay in resolving Maloney's case resulted from Maloney's ploy to evade criminal liability by threatening to reveal classified information during the course of his trial in a failed attempt to force the government to dismiss the case. But as Maloney discovered, the government will not be bullied or threatened by a criminal defendant." "Maloney's guilty plea should send a clear message to anyone seeking to abuse their positions for personal gain, the FBI will find you and hold you accountable", said Keri Farley, Special Agent in Charge of FBI Atlanta.

Read the full article here.

JUSTICE DEPARTMENT ANNOUNCES FIVE CASES AS PART OF RECENTLY LAUNCHED DISRUPTIVE TECHNOLOGY STRIKE FORCE

U. S. Department of Justice | May 16, 2023

The Justice Department today announced criminal charges in five cases and four arrests from five different U.S. Attorney's offices in connection with the recently launched multi-agency Disruptive Technology Strike Force. The Disruptive Technology Strike Force is co-led by the Departments of Justice and Commerce to counter efforts by hostile nation-states to illicitly acquire sensitive U.S. technology to advance their authoritarian regimes and facilitate human rights abuses. The Strike Force's work has led to the unsealing of charges against multiple defendants in five cases accused of crimes including export violations, smuggling and theft of trade secrets. Two of these cases involve the disruption of alleged procurement networks created to help the Russian military and intelligence services obtain sensitive technology in violation of U.S. laws. In the Eastern District of New York, a Greek national was arrested on May 9 for federal crimes in connection with allegedly acquiring more than 10 different types of sensitive technologies on behalf of the Russian government and serving as a procurement agent for two Russian Specially Designated Nationals (SDNs) operating on behalf of Russia's intelligence services.

Read the full article here.

DISRUPTIVE TECHNOLOGY STRIKE FORCE TO ENFORCE U.S. LAWS PROTECTING ADVANCED TECHNOLOGIES

Hogan Lovells, Kelly Zhang, and Andrea Fraser-Reid | JD Supra | March 7, 2023

On February 16, 2023, the Department of Justice (DOJ) and the Department of Commerce (Commerce) announced the creation of a joint Disruptive Technology Strike Force (Strike Force). The Strike Force will be co-led by the Assistant Attorney General for the DOJ's National Security Division and the Assistant Secretary for Export Enforcement at the Bureau of Industry and Security (BIS). The Strike Force is intended to strengthen supply chains and target illicit actors who attempt to acquire and use critical technological assets to threaten U.S. national security. Countries of concern for the Strike Force include China, Iran, Russia, and North Korea. The Strike Force will work closely with experts throughout government – including the FBI, BIS, Homeland Security Investigations (HSI) and 14 U.S. Attorneys' Offices in 12 metropolitan regions across the country.

Read the full article here.

OPTIMIZING EXPORT CONTROLS FOR CRITICAL AND EMERGING TECHNOLOGIES

William Alan Reinsch, Emily Benson, Thibault Denamiel, and Margot Putnam | Center for Strategic & International Studies | May 31, 2023

Using a trade lens to evaluate geostrategic competition and how best to maintain U.S. military superiority, this report assesses what the optimal export control policy should be, knowing that there are serious political constraints domestically as well as with key allies. The first in a series of three, this report seeks to reimagine the current approach to export controls in particularly sensitive areas of emerging technologies that pose the greatest challenges. It begins by comparing current control lists to see where they overlap, which in turn provides greater clarity on the current U.S. definition of national security critical sectors. After comparing control lists, the report evaluates quantum computing, artificial intelligence, semiconductors, biotechnology, and intangible goods to determine whether additional controls are necessary—and, if so, what economic costs such controls would entail.

Read the full article here.

INSIDER RISK MANAGEMENT: WHERE YOUR PROGRAM RESIDES SHAPES ITS FOCUS

Christopher Burgess | CSO | May 29, 2023

There's no getting around it, I am long in the tooth and have been dealing with individuals who break trust within their work environment for more than 30 years, both in government (where we called it counterespionage or counterintelligence) and in the private sector. Today we call programs that help prevent or identify breaches of trust insider risk management (IRM). Over the years I have hypothesized that where such IRM programs reside within an organization will have a material impact on its focus and possibly its overall effectiveness. In 2019, a CSO article raised the question "Insider risk management — who's the boss?" and examined where the buck should stop in terms of taking responsibility for threats from within. Here we are four years later and the predicted growth of the role of an individual with a unique focus on the "insider threat" or "insider risk management" program hasn't yet settled — it continues to evolve. At a recent Insider Threat Summit, it was nearly unanimously presented that the effective IRM program sits within the information security realm, as that is where all data resides. Joe Payne, CEO of CODE42, with whom I spoke at the end of March, agreed.

Read the full article here.

INSIDER THREATS SURGE ACROSS US CNI AS ATTACKERS EXPLOIT HUMAN FACTORS

Michael Hill | CSO | May 17, 2023

Economic pressures and remote working could be increasing critical national infrastructure insider threats while nation-state actors and ransomware attacks continue to pose significant risks. Over three-quarters (77%) of organizations across US critical national infrastructure (CNI) have seen a rise in insider-driven cyberthreats in the last three years, according to new research from cybersecurity services firm Bridewell. The Cyber Security in CNI: 2023 report surveyed 525 cybersecurity decision makers in the US in the transport and aviation, utilities, finance, government, and communications sectors. It revealed that increased insider threat could be linked to heightened economic pressures and remote working. Threats from within range from criminal intent to individual negligence, with those surveyed stating that an act of intentional destruction by an employee was committed at an average of at least every other week within the last year. Bridewell's findings come amidst a growing international focus on insider-driven cyberthreats against critical infrastructure.

Read the full article here.

A LONG MARCH: CHINA'S MILITARY-INDUSTRIAL ESPIONAGE

Michael G. McLaughlin and William J. Holstein | Asia Times | June 2, 2023

Recent revelations that Chinese state-sponsored hackers penetrated US critical infrastructure and have the ability to disrupt oil and gas pipelines, rail systems, and the US Navy's communications in the Pacific theater should come as no surprise. China's pursuit of digital dominance has been decades in the making. Reveille for China's planners was sounded in the early 1990s during the Gulf War, in which the United States and its allies effortlessly toppled Iraqi forces. The first conflict of the digital era demonstrated to Chinese strategists the critical role of information technology on and off the battlefield. Chinese leaders watched with dismay as the American military routed and dismantled the Iraqi military in what is considered one of the most one-sided conflicts in the history of modern warfare.

Read the full article here.

THE GREAT CISO RESIGNATION: WHY SECURITY LEADERS ARE QUITTING IN DROVES

Taryn Plumb | SDX Central | May 29, 2023

With ransomware becoming increasingly commoditized and generative AI tools like ChatGPT broadening hackers' arsenal, organizations are increasingly under attack in what some are calling a cyber cold war. This places greater and greater pressure on security leaders dealing with shrinking budgets, skeleton crew staff and a conglomeration of security tools and protocols — so much so that they are increasingly up and quitting. This so-called Great CISO Resignation is concerning, experts warn — because what happens when there's nobody guarding the gate and rallying the troops? "The CISO is the leader of the front line of defense against threat actors," said Rick Crandall, chairman of the National Cybersecurity Center's Cyber Committee, which recently made a call to action to reverse what some are calling the Great CISO Resignation.

Read the full article here.