ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

November 16, 2022

2022 ANNUAL REPORT TO CONGRESS

U.S.-China Economic and Security Review Commission | November 2022

2022 was a watershed year for China's Communist Party regime and for America's response to its policies. A confluence of groundbreaking events, including Russia's unprovoked invasion of Ukraine and China's growing military threats to Taiwan, led to new, potentially far-reaching changes in international alignments and in the responses by democratic nations to the CCP's conduct. At the same time, as the result of the CCP's novel coronavirus (COVID-19) containment policies that produced lockdowns of major cities, the Chinese people were obliged to live at a greater distance from the outside world. The CCP gave its leader Xi Jinping unprecedented power over the Party and the country. Xi and the CCP relied ever more heavily on nationalist appeals, as was evident in its escalating rhetoric and menacing military actions toward Taiwan. Faced with a series of crises and unexpected developments, China's Communist Party regime reacted, not by reexamining its assumptions and modifying its approach, but rather by doubling down on existing policies. In the near term these choices have increased the challenge China poses to the security, prosperity, and shared values of the United States and its democratic allies and partners.

Read the full article here.

THREE ARRESTED FOR ILLEGAL SCHEME TO EXPORT CONTROLLED DATA AND DEFRAUD THE DEPARTMENT OF DEFENSE

U.S. Department of Justice | November 9, 2022

A federal indictment was unsealed today following the arrest of three defendants and their initial appearances in the U.S. District Court in the Western District of Kentucky. According to court documents, Phil Pascoe, 60, of Floyds Knobs, Indiana; Monica Pascoe, 45, of Floyds Knobs, Indiana; Scott Tubbs, 59, of Georgetown, Kentucky; and Quadrant Magnetics LLC are charged with wire fraud, violations of the Arms Export Control Act, and smuggling of goods for their roles in an illegal scheme to send export-controlled defense-related technical data to China and to unlawfully supply U.S. Department of Defense (DOD) with Chinese-origin rare earth magnets for aviation systems and military items. The indictment alleges that between January 2012 and December 2018, the defendants conspired to send approximately 70 drawings containing export-controlled technical data to a company located in China without a license from the U.S. government, in violation of the Arms Export Control Act and the International Traffic in Arms Regulations. The technical data drawings were the property of two U.S. companies and related to end-use items for aviation, submarine, radar, tank, mortars, missiles, infrared and thermal imaging targeting systems, and fire control systems for DOD.

Read the full article here.

NATIONAL SECURITY STRATEGY

The White House | October 2022

We are now in the early years of a decisive decade for America and the world. The terms of geopolitical competition between the major powers will be set. The window of opportunity to deal with shared threats, like climate change, will narrow drastically. The actions we take now will shape whether this period is known as an age of conflict and discord or the beginning of a more stable and prosperous future. We face two strategic challenges. The first is that the post-Cold War era is definitively over and a competition is underway between the major powers to shape what comes next. No nation is better positioned to succeed in this competition than the United States, as long as we work in common cause with those who share our vision of a world that is free, open, secure, and prosperous. This means that the foundational principles of self-determination, territorial integrity, and political independence must be respected, international institutions must be strengthened, countries must be free to determine their own foreign policy choices, information must be allowed to flow freely, universal human rights must be upheld, and the global economy must operate on a level playing field and provide opportunity for all.

Read the full article here.

CYBER VULNERABILITY DISCOVERED IN NETWORKS USED BY SPACECRAFT, AIRCRAFT AND ENERGY GENERATION SYSTEMS

Zach Champion, University of Michigan | Tech Xplore | November 15, 2022

A major vulnerability in a networking technology widely used in critical infrastructures such as spacecraft, aircraft, energy generation systems and industrial control systems was exposed by researchers at the University of Michigan and NASA. It goes after a network protocol and hardware system called time-triggered ethernet, or TTE, which greatly reduces costs in high-risk settings by allowing mission-critical devices (like flight controls and life support systems) and less important devices (like passenger WiFi or data collection) to coexist on the same network hardware. This blend of devices on a single network arose as part of a push by many industries to reduce network costs and boost efficiency. That coexistence has been considered safe for more than a decade, predicated on a design that prevented the two types of network traffic from interfering with one another. The team's attack, called PCspooF, was the first of its kind to break this isolation. In one compelling demonstration, the team used real NASA hardware to recreate a planned Asteroid Redirection Test. The experimental setup controlled a simulated crewed capsule, specifically at the point in the mission when the capsule prepared to dock with a robotic spacecraft.

Read the full article here.

PROTECTING U.S. TECHNOLOGICAL ADVANTAGE

National Academies of Sciences, Engineering, and Medicine | National Academies Press | 2022

U.S. leadership in technology innovation is central to our nation's interests, including its security, economic prosperity, and quality of life. Our nation has created a science and technology ecosystem that fosters innovation, risk taking, and the discovery of new ideas that lead to new technologies through robust collaborations across and within academia, industry, and government, and our research and development enterprise has attracted the best and brightest scientists, engineers, and entrepreneurs from around the world. The quality and openness of our research enterprise have been the basis of our global leadership in technological innovation, which has brought enormous advantages to our national interests. In today's rapidly changing landscapes of technology and competition, however, the assumption that the United States will continue to hold a dominant competitive position by depending primarily on its historical approach of identifying specific and narrow technology areas requiring controls or restrictions is not valid.

Read the full article here.

RUSSIA LINKED TO NEARLY 75% OF LATE 2021 RANSOMWARE ATTACKS, PER ANALYSIS

Alexandra Kelley | Nextgov | November 1, 2022

A new analysis from the Department of Justice's Financial Crimes Enforcement Network reveals that Russian actors comprised roughly three-quarters of recorded ransomware incidents during the latter portion of 2021, contributing to the sharp uptick in ransomware attacks experienced over the course of 2021 versus 2020. Building off of data collected from the Bank Secrecy Act and an earlier agency report, FinCEN officials attributed 594 of the ransomware-related activities recorded between July and December 2021 to Russia-linked actors, out of a cumulative 793 reported to the agency during that time frame. The total cost of incidents over that time period was $488 million. "Today's report reminds us that ransomware—including attacks perpetrated by Russian-linked actors— remain a serious threat to our national and economic security," said FinCEN Acting Director Himamauli Das. "It also underscores the importance of BSA filings, which allow us to uncover trends and patterns in support of whole-of-government efforts to prevent and combat ransomware attacks.

Read the full article here.

FBI IS 'EXTREMELY CONCERNED' ABOUT TIKTOK OPERATING IN US

Chris Strohm and Daniel Flatley | Bloomberg | November 15, 2022

FBI Director Christopher Wray reiterated the bureau's longstanding national security concerns about Chinese-owned video app TikTok to lawmakers Tuesday and said the agency is sharing its views with officials who are weighing a deal that would allow it to keep operating in the US. Wray told lawmakers China's government could use the app to control millions of users' data or software, and its recommendation algorithm -- which determines which videos users will see next -- "could be used for influence operations if they so choose." "Under Chinese law, Chinese companies are required to essentially -- and I'm going to shorthand here -- basically do whatever the Chinese government wants them to do in terms of sharing information or serving as a tool of the Chinese government," Wray told the House Homeland Security Committee. "That's plenty of reason by itself to be extremely concerned." The Federal Bureau of Investigation has passed along its concerns to the Committee on Foreign Investment in the United States, the government body that's reviewing the deal.

Read the full article here.

QUANTUM CRYPTOGRAPHY APOCALYPSE: A TIMELINE AND ACTION PLAN

Konstantinos Karagiannis | Informa | November 14, 2022

There is a potential dark side to quantum computing, one that is a threat to how we secure data. Back in 1994, Peter Shor developed an algorithm for factoring large numbers using a quantum computer, which could be used to break encryption. Today, RSA encryption relies on the difficulty a classical computer has with such factorization. With Shor's algorithm in mind, nation-states and nefarious actors started harvesting data packets, dreaming of a future where they would be able to decrypt those packets using a fault-tolerant quantum computer. Currently, there are about three dozen quantum computers in the cloud. These quantum computers are error-prone and lack enough quantum bits (qubits) to run Shor's algorithm against RSA encryption. Some experts claim quantum computing will not be a threat for at least 30 years. However, those claims may be based upon outdated information and there is evidence that quantum computing will have the power to crack encryption sooner than we thought. The day is coming when a quantum threat (Y2Q) to encryption becomes a reality.

Read the full article here.

CHINA:EFFORTS UNDERWAY TO ADDRESS TECHNOLOGY TRANSFER RISK AT U.S. UNIVERSITIES, BUT ICE COULD IMPROVE RELATED DATA

U.S. Government Accountability Office | November 15, 2022

U.S. Immigration and Customs Enforcement (ICE) has incomplete data that may indicate whether foreign students and scholars pose risks for transferring technology from U.S. universities to foreign entities. ICE's foreign student and scholar database contains data on the number of graduate students from countries of concern for technology transfer, such as the People's Republic of China (PRC). Graduate students studying in a science, technology, engineering, and math (STEM) field have also been identified as more likely to be involved in sensitive research (see fig.). However, ICE has not established milestones to complete a required assessment of whether it needs to modify its database to collect additional data related to some risk factors, in part because it has focused available resources on other priorities. Further, information related to students' employment in the U.S., which may indicate whether they have access to technology, is incomplete.

Read the full article here.

SAFEGUARDING SCIENCE – AN OUTREACH INITIATIVE FOR PROTECTING RESEARCH AND INNOVATION IN EMERGING TECHNOLOGIES

Office of the Director of National Intelligence | The National Counterintelligence and Security Center

An informed, empowered scientific community is best positioned to assess emerging technologies and their applications and to design measures to guard against the potential misuse or theft of these technologies. The National Counterintelligence and Security Center (NCSC) has partnered with multiple federal agencies to develop an outreach initiative, “Safeguarding Science,” designed to raise awareness of the spectrum of risk in emerging technologies and to help stakeholders in these fields to develop their own methods to protect research and innovation. The initiative focuses on emerging technology sectors where the stakes are potentially greatest for U.S. economic and national security, including the following: artificial intelligence, bioeconomy, autonomous systems, quantum, and semiconductors. Safeguarding science goals include promoting a U.S. research ecosystem that emphasizes collaboration, openness, equity, integrity, and security, all of which facilitate innovation and providing curated resources for our stakeholders to support best practices in protecting research and innovation.

Read the full article here.

MICROSOFT PUBLISHES NEW REPORT ON HOLISTIC INSIDER RISK MANAGEMENT

Bret Arsenault | Microsoft | October 6, 2022

The risk landscape for organizations has changed significantly in the past few years. The amount of data captured, copied, and consumed is expected to grow to more than 180 zettabytes through 2025.[1] Traditional ways of identifying and mitigating risks don’t always work. Historically, organizations have focused on external threats; however, risks from within the organization can be just as prevalent and harmful. These internal risks include unprotected and ungoverned data, accidental or intentional data oversharing, as well as the risks for failing to meet ever-changing regulations. Not to mention, with more than 300 million people working remotely, data is being created, accessed, shared, and stored outside of the traditional borders of business. Core to a security team’s mission is protecting the company’s assets, especially its data.

Read the full article here.

LINKEDIN PROFILES INDICATE 300 CURRENT TIKTOK AND BYTEDANCE EMPLOYEES USED TO WORK FOR CHINESE STATE MEDIA—AND SOME STILL DO

Emily Baker-White | Forbes | August 11, 2022

Three hundred current employees at TikTok and its parent company ByteDance previously worked for Chinese state media publications, according to public employee LinkedIn profiles reviewed by Forbes. Twenty-three of these profiles appear to have been created by current ByteDance directors, who manage departments overseeing content partnerships, public affairs, corporate social responsibility and "media cooperation." Fifteen indicate that current ByteDance employees are also concurrently employed by Chinese state media entities, including Xinhua News Agency, China Radio International and China Central / China Global Television. (These organizations were among those designated by the State Department as "foreign government functionaries" in 2020.) Fifty of the profiles represent employees that work for or on TikTok, including a content strategy manager who was formerly a Chief Correspondent for Xinhua News. The LinkedIn profiles reviewed by Forbes reveal significant connections between TikTok's parent company, ByteDance, and the propaganda arm of the Chinese government, which has been investing heavily in using social media to amplify disinformation that serves the Chinese Communist Party.

Read the full article here.