RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE
THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary

January 4, 2024

HOUSE SELECT COMMITTEE ON THE CCP RELEASES REPORT PROPOSING CHANGES TO CFIUS

Nova J. Daly, Daniel P. Brooks, Hon. Nazak Nikakhtar, Paul J. Coyle, and Paul A. Devamithran | Wiley
December 15, 2023

On December 12, 2023, the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (the "Committee"), led by Chairman Mike Gallagher (WI), issued a wide-ranging report with numerous recommendations for addressing ongoing challenges in the U.S. economic relationship with the People's Republic of China (PRC). Regarding foreign investment, the Committee deemed the regulatory approach of the Committee on Foreign Investment in the United States (CFIUS) insufficient to address the PRC's Military-Civil Fusion and proposed several specific updates. The report, entitled Reset, Prevent, Build: A Strategy to Win America's Economic Competition with the Chinese Communist Party, reiterates legislative proposals included in a number of bills currently pending in Congress, which seek to broaden CFIUS's powers and jurisdiction, including those related to U.S. agriculture and real estate sectors. The Committee specifically proposes making the Secretary of Agriculture a voting member of CFIUS for cases involving farmland or agriculture technology and empowering the Secretary to flag potentially problematic land purchases for CFIUS review.

Read the full article here.

THE AGE OF WEAPONIZED LLMS IS HERE

Louis Columbus | VentureBeat | December 18, 2023

The idea of fine-tuning digital spearphishing attacks to hack members of the UK Parliament with Large Language Models (LLMs) sounds like it belongs more in a Mission Impossible movie than a research study from the University of Oxford. But it's exactly what one researcher, Julian Hazell, was able to simulate, adding to a collection of studies that, altogether, signify a seismic shift in cyber threats: the era of weaponized LLMs is here. By providing examples of spearphishing emails created using ChatGPT-3, GPT-3.5, and GPT-4.0, Hazell reveals the chilling fact that LLMs can personalize context and content in rapid iteration until they successfully trigger a response from victims. "My findings reveal that these messages are not only realistic but also cost-effective, with each email costing only a fraction of a cent to generate," Hazell writes in his paper published in the open-access journal arXiv back in May 2023. Since that time, the paper has been cited in more than 23 others in the subsequent six months, showing the concept is being noticed and built upon in the research community.

Read the full article here.

APPLE: 2.5B RECORDS EXPOSED, MARKING STAGGERING SURGE IN DATA BREACHES

Jai Vijayan | DarkReading | December 8, 2023

Data breaches are rapidly accelerating, according to a number-crunching report from Apple this week — heightening the need to finally implement end-to-end data encryption. An Apple-commissioned report this week has highlighted once again why analysts have long recommended the use of end-to-end encryption to protect sensitive data against theft and misuse. The report is based on an independent study of publicly reported breach data that a professor at the Massachusetts Institute of Technology conducted for the tech giant. It showed that ransomware campaigns and attacks on trusted technology vendors contributed to a sharp increase in data breaches and the number of records compromised in these breaches over the past two years. In 2021 and 2022, data breaches exposed a staggering 2.6 billion personal records — some 1.5 billion of them last year alone. That number will likely be even higher in 2023 if trends so far this year are any indication.

Read the full article here.

U.S. AND CHINA RACE TO SHIELD SECRETS FROM QUANTUM COMPUTERS

David Lague | Reuters | December 14, 2023

In February, a Canadian cybersecurity firm delivered an ominous forecast to the U.S. Department of Defense. America's secrets – actually, everybody's secrets – are now at risk of exposure, warned the team from Quantum Defen5e (QD5). QD5's executive vice president, Tilo Kunz, told officials from the Defense Information Systems Agency that possibly as soon as 2025, the world would arrive at what has been dubbed "Q-day," the day when quantum computers make current encryption methods useless. Machines vastly more powerful than today's fastest supercomputers would be capable of cracking the codes that protect virtually all modern communication, he told the agency, which is tasked with safeguarding the U.S. military's communications. In the meantime, Kunz told the panel, a global effort to plunder data is underway so that intercepted messages can be decoded after Q-day in what he described as "harvest now, decrypt later" attacks, according to a recording of the session the agency later made public.

Read the full article here.

PENTAGON RELEASES PROPOSED RULE ON CYBERSECURITY STANDARDS FOR CONTRACTORS

Mark Pomerleau | DefenseScoop | December 22, 2023

At long last, the Department of Defense has released its proposed rule on cybersecurity standards for contractors. Following several years of development, the DOD in late 2021 shifted gears and unveiled the Cybersecurity Maturity Model Certification 2.0, which includes enhancements to the initial program first developed during the Trump administration. After reforming the program, the Pentagon has been working on a final rule that will mandate contractors that work with the department's controlled unclassified information be CMMC certified, or risk losing their business. The CMMC program is based upon a tiered cybersecurity framework that sets requirements for companies based on the level of security necessary for their work. The initiative was conceived to protect contractor information from being exploited by adversaries. An unpublished version of the proposed rule appeared on the Federal Register Dec. 22 — a few days before its official publication on Dec. 26.

Read the full article here.

HOW TO STOP PATENT TROLLS FROM GAINING ACCESS TO SENSITIVE INFORMATION

John Ratcliffe | The Dallas Morning News | December 20, 2023

Foreign adversaries like China, Russia and Iran use the full scope of their political and economic power to spread their influence and undermine the United States' global standing. In particular, U.S. technologies face a significant threat from global competitors as the National Counterintelligence and Security Center has warned that China, among other adversaries, is "increasingly asserting itself by stealing our technology and intellectual property in an effort to erode United States economic and military superiority." To counter this threat, the U.S. must put controls in place that limit foreign adversaries' ability to manipulate intellectual property to their advantage. Yet, because our courts are operating with a near-total lack of transparency around litigation funding, foreign actors can exploit a vulnerable American judicial system.

Read the full article here.

CHINA IS STEALING AI SECRETS TO TURBOCHARGE SPYING, U.S. SAYS

Robert McMillan, Dustin Volz, and Aruna Viswanatha | The Wall Street Journal | December 25, 2023

On a July day in 2018, Xiaolang Zhang headed to the San Jose, Calif., airport to board a flight to Beijing. He had passed the checkpoint at Terminal B when his journey was abruptly cut short by federal agents. After a tipoff by Apple's security team, the former Apple employee was arrested and charged with stealing trade secrets related to the company's autonomous-driving program. It was a skirmish in a continuing shadow war between the U.S. and China for supremacy in artificial intelligence. The two rivals are seeking any advantage to jump ahead in mastering a technology with the potential to reshape economies, geopolitics and war. Artificial intelligence has been on the Federal Bureau of Investigation's list of critical U.S. technologies to protect, just as China placed it on a list of technologies it wanted its scientists to achieve breakthroughs on by 2025. By funding patent trolls — shell companies whose sole purpose is to file patent infringement lawsuits — nefarious third parties, including foreign adversaries, can use intellectual property to attack U.S. companies through lawsuits and even gain access to sensitive information.

Read the full article here.

CYBERSECURITY MATURITY MODEL CERTIFICATION PROGRAM PROPOSED RULE PUBLISHED

U.S. Department of Defense | December 26, 2023

Today, the Department of Defense publishes for a 60-day comment period a proposed rule for the Cybersecurity Maturity Model Certification (CMMC) program at https://www.regulations.gov/docket/DOD-2023-OS-0063. CMMC is designed to ensure that defense contractors and subcontractors are compliant with existing information protection requirements for federal contract information (FCI) and controlled unclassified information (CUI) and are protecting that sensitive unclassified information at a level commensurate with the risk from cybersecurity threats, including advanced persistent threats. The proposed rule published today revises certain aspects of the program to address public concerns in response to DoD's initial vision for the CMMC 1.0 program, as originally published on Sep. 29, 2020.

Read the full article here.

CSIS ASKING FOR AUTHORITY TO DISCLOSE FOREIGN-INTERFERENCE THREATS TO UNIVERSITIES, PROVINCES AND CITIES

Steven Chase and Robert Fife | The Globe and Mail | December 29, 2023

Canada's spy agency is proposing that it be given the legal authority to disclose intelligence to entities such as universities, provinces and municipalities to help combat foreign interference. The Canadian Security Intelligence Service recently released a consultation paper seeking input on a number of proposed changes to the CSIS Act, one of which would allow it to discuss sensitive intelligence with parties beyond the federal government. A public inquiry into foreign interference in Canada by the Chinese government and other hostile states is under way with hearings set to begin Jan. 29. At the same time, Ottawa is considering changes to national-security laws. CSIS said its governing legislation as currently written prevents it from speaking frankly to academic institutions about the threats they face. Canadian universities have been targets for espionage.

Read the full article here.

WHY IS THE US PATENT SYSTEM WORKING AGAINST US INTERESTS?

Julie Burke | The Hill | December 28, 2023

In August, President Biden issued an executive order restricting U.S. investments into several Chinese technology sectors related to military, intelligence, surveillance and cyber-enabled capabilities. Last week, an annual Pentagon report revealed a rapidly expanding Chinese military. And according to a recent study that received funding from the U.S. State Department, China now outperforms the U.S. in 37 of 44 critical technology areas. Those include artificial intelligence (AI), defense, space, robotics, advanced materials, energy, biotechnology and critical quantum tech areas. The study also cited a high risk for a Chinese monopoly in advanced optical communications, drones, swarming, collaborative robots and synthetic biology, among others.

Read the full article here.

INFORMATION AND COMMUNICATIONS TECHNOLOGY AND THE SUPPLY CHAIN RISK

The National Counterintelligence and Security Center | April 2022

Developed nations rely on technology for all types of industries, from communications to entertainment, safety to medicine, transportation to national security. Technology is so commonplace that consumers do not question where or how the technology in computers, phones, televisions, or other devices is sourced. What many around the world do not realize is that numerous components, often from across the world, go into creating these devices. This paper analyzes Information and Communications Technology (ICT) supply chain vulnerabilities and suggests steps to mitigate and strengthen the ICT supply chain. The National Institute of Standards and Technology (NIST) defines "supply chain" as "a system of organizations, people, activities, information, and resources, possibly international in scope that provides products or services to consumers."

Read the full article here.

USEFUL RESOURCES

SAFEGUARDING OUR FUTURE
U.S. BUSINESS RISK: PEOPLE'S REPUBLIC OF CHINA (PRC) LAWS EXPAND BEIJING'S OVERSIGHT OF FOREIGN AND DOMESTIC COMPANIES

The National Counterintelligence and Security Center | June 20, 2023

Since 2015, the PRC has passed or updated comprehensive national security, cybersecurity, and data privacy laws and regulations, expanding Beijing's oversight of domestic and foreign (including U.S.) companies operating within China. Beijing views inadequate government control of information within China and its outbound flow as a national security risk. These laws provide the PRC government with expanded legal grounds for accessing and controlling data held by U.S. firms in China. U.S. companies and individuals in China could also face penalties for traditional business activities that Beijing deems acts of espionage or for actions that Beijing believes assist foreign sanctions against China.

View the full resource here.

OPERATIONS SECURITY (OPSEC)
UNDERSTANDING OPSEC

The National Counterintelligence and Security Center | Bulletin 1 | January 2023

Operations security means taking appropriate steps to make it harder for adversaries to collect unclassified and seemingly innocent information about your organization. Basic steps can exponentially improve overall security. National Operations Security (OPSEC) Awareness Month is an opportunity for government agencies, public and private-sector entities, and individuals to reflect on ways to mitigate the various vulnerabilities, risks, and threats to their organizations.

View the full resource here.

SAFEGUARDING INTERNATIONAL SCIENCE
RESEARCH SECURITY FRAMEWORK

The National Counterintelligence and Security Center

The National Institute of Standards and Technology (NIST) has released the "Safeguarding International Science Research Security Framework," which is designed to enable organizations to implement a mission-focused, integrated, risk-balanced program through the application of research security principles and best practices that fosters the safeguarding of international science while mitigating risks to the integrity of the open collaborative environment. This NIST Framework is a living document and will continue to be updated and improved as its users provide feedback on implementation of review procedures or to address new or emerging risks. This will ensure it is meeting the needs of Research Security practitioners in a dynamic and challenging environment of new threats, risks, and creative solutions.

View the full resource here.

SMART TRAVELER ENROLLMENT PROGRAM (STEP)

The National Counterintelligence and Security Center

STEP is a free service to allow U.S. citizens/nationals traveling abroad to enroll with the local U.S. Embassy or Consulate.

View the full resource here.

EMERGING TECHNOLOY AND DEMOCRACY

National Endowment for Democracy

A Curated List of Materials on Emerging Technology and Democracy from The International Forum for Democratic Studies, Journal of Democracy, and Center for International Media Assistance.

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute