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

Open Source Media Summary

December 7, 2023

SPECIAL REPORT: COMMON CYBERSECURITY WEAKNESSES RELATED TO THE PROTECTION OF DOD CONTROLLED UNCLASSIFIED INFORMATION ON CONTRACTOR NETWORKS (DODIG-2024-031)

Department of Defense Office of Inspector General | December 4, 2023

Inspector General Robert P. Storch announced today that the Department of Defense Office of Inspector General released the "Special Report: Common Cybersecurity Weaknesses Related to the Protection of DoD Controlled Unclassified Information on Contractor Networks." The report outlines 24 open recommendations from previous DoD OIG audit reports aimed at addressing cybersecurity vulnerabilities among DoD contractors, including common weaknesses in the cybersecurity protocols of DoD contractors who process, store, and transmit controlled unclassified information (CUI). One of the most prevalent weaknesses identified in this report was the failure of DoD contractors to enforce multifactor authentication and lack of strong passwords. This report summarizes a series of DoD OIG audit projects focused on cybersecurity challenges facing DoD contractors. From 2018 through 2023, the DoD OIG issued five audits that consistently found DoD contracting officials failed to establish processes to verify that contractors complied with selected Federal cybersecurity requirements for CUI, as required by the National Institute of Standards and Technology (NIST).

Read the full article here.

MOBILE APP SECURITY THREAT ALERT: WECHAT BY TENCENT

NÚKIB | November 30, 2023

The National Cyber and Information Security Agency (hereinafter the „Agency") is issuing a security threat alert regarding the use of Tencent's WeChat mobile application. The Agency is concerned about the possibility of misuse of the data collected by the app, due to a combination of several factors: excessive collection of user data and methods of their collection which may facilitate precise targeting of cyberattacks; the legal environment of the People's Republic of China (PRC); and the PRC's influence operations in the Czech Republic. While the number of active users of WeChat in the Czech Republic is significantly lower compared to other social media platforms, Czech users of the app may include high-risk individuals such as diplomats, businesspeople, scholars, or Chinese dissidents. These individuals may then be targeted for collection of sensitive information that can later be used, for example, for blackmail or other forms of coercion by malicious actors. WeChat is a social media and messaging mobile app with many additional features. It is developed and operated by Tencent, a company based in Shenzhen, China. The platform is used by approximately 1.3 billion active users worldwide.

Read the full article here.

HOW TO NOT GET HACKED BY A QR CODE

David Nield | Wired | December 3, 2023

For every form of communication or messaging out there, you can be sure that scammers and hackers are trying to find a way to take advantage of you—from emails to texts to calls. This threat extends to QR (quick response) codes too. Earlier this year, we saw a QR code scam targeted at a major US energy company, for example, and security analysts are warning that these so-called quishing attacks are on the rise. Quishing is an amalgamation of "QR code" and "phishing"—where malicious actors "fish" (often over email) for private information and personal details. If we didn't already have enough to worry about, now we need to be on guard against quishing. The good news is that the security practices you hopefully already have in place should serve you well here too. By now we should all be familiar with QR codes: a grid of black-and-white squares that act as a sort of hieroglyph that can be translated by the camera on your phone or another device. Most often, QR codes translate into website URLs, but they can also point to a plain text message, app listings, map addresses, and so on.

Read the full article here.

WHY PSYCHOLOGY MATTERS TO CYBERSECURITY

Shruthi Mugunthan | LinkedIn | December 3, 2023

Cyber-criminals are infamous for their ability to exploit human psychology as part of their nefarious activities – such as playing on fear and invoking a sense of urgency to entice victims into clicking on malicious links or give away log in credentials. Tapping into the human mind through social engineering techniques, such as phishing, vishing and smishing, continues to be highly successful. For example, Verizon's 2023 Data Breach Investigations Report found that the human element is present in three-quarters (74%) of data breaches. Psychology plays a crucial role in cybersecurity because understanding human behavior is essential to creating effective security measures. Here are several reasons why psychology matters in the context of cybersecurity: 1. Social Engineering Attacks: Many cyberattacks involve some form of social engineering, where attackers manipulate individuals into divulging sensitive information or performing actions that compromise security. Understanding human psychology helps cybersecurity professionals anticipate and mitigate the impact of such attacks.

Read the full article here.

CISA AND UK NCSC UNVEIL JOINT GUIDELINES FOR SECURE AI SYSTEM DEVELOPMENT

Cybersecurity and Infrastructure Security Agency | November 26, 2023

Today, in a landmark collaboration, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the UK National Cyber Security Centre (NCSC) are proud to announce the release of the Guidelines for Secure AI System Development. Co-sealed by 23 domestic and international cybersecurity organizations, this publication marks a significant step in addressing the intersection of artificial intelligence (AI), cybersecurity, and critical infrastructure. The Guidelines, complementing the U.S. Voluntary Commitments on Ensuring Safe, Secure, and Trustworthy AI, provide essential recommendations for AI system development and emphasize the importance of adhering to Secure by Design principles. The approach prioritizes ownership of security outcomes for customers, embraces radical transparency and accountability, and establishes organizational structures where secure design is a top priority.

Read the full article here.

SECURING SEMICONDUCTOR SUPPLY CHAINS

Sujai Shivakumar | Issue in Science and Technology | Fall 2023

Global supply chains, particularly in technologies of strategic value, are undergoing a remarkable reevaluation as geopolitical events weigh on the minds of decisionmakers across government and industry. The rise of an aggressive and revisionist China, a devastating global pandemic, and the rapid churn of technological advancement are among the factors prompting a dramatic rethinking of the value of lean, globally distributed supply chains. These complex supply networks evolved over several decades of relative geopolitical stability to capture the efficiency gains of specialization and trade on a global scale. Yet in today's world, efficiency must be recast in terms of reliable and resilient supply chains better adapted to geopolitical uncertainties rather than purely on the basis of lowest cost. Indeed, nations worldwide have belatedly discovered a crippling lack of redundancy in supply chains necessary to produce and distribute products essential to their economies and welfare, including such diverse goods as vaccines and medical supplies, semiconductors and other electronic components, and the wide variety of technologies reliant on semiconductors.

Read the full article here.

INSIDE U.S. EFFORTS TO UNTANGLE THE AI GIANT'S TIES TO CHINA

Mark Mazzetti and Edward Wong | New York Times | November 28, 2023

When the secretive national security adviser of the United Arab Emirates, Sheikh Tahnoon bin Zayed, visited the White House in June, his American counterpart, Jake Sullivan, raised a delicate issue: G42, an artificial intelligence firm controlled by the sheikh that American officials believe is hiding the extent of its work with China. In public, the company has announced its staggering growth with a steady cadence of news releases. They have included agreements with European pharmaceutical giants like AstraZeneca and a $100 million deal with a Silicon Valley firm to build what the companies boast will be the "world's largest supercomputer." Last month, G42 announced a partnership with OpenAI, the creator of ChatGPT. But in classified American intelligence channels, there have been more concerning reports about the company. The CIA and other American spy agencies have issued warnings about G42's work with large Chinese companies that U.S. officials consider security threats, including Huawei, the telecommunications giant that is under U.S. sanctions.

Read the full article here.

NO WINNERS IN THIS GAME-ASSESSING THE U.S. PLAYBOOK FOR SANCTIONING CHINA

Emily Kilcrease | Center for a New American Security | December 1, 2023

The relationship between the United States and the People's Republic of China (PRC) is marked by both geopolitical tensions and deep economic linkages. While policymakers may have once believed that economic integration would inject stability into the overall relationship and provide a deterrent to conflict, that idealistic vision has been shaken by Russia's brutal invasion of Ukraine. No longer can the United States and its partners assume that the PRC's economic interest in retaining ties to the global economy will override its nationalist impulses. The once unthinkable idea of imposing severe sanctions on China has become a strategic imperative to consider, as one of a range of measures that the United States and its partners may consider if relations with the PRC deteriorate further. Yet, sanctioning China represents a challenge more complex than any other in the modern era of sanctions.

Read the full article here.

CRITICAL TECHNOLOGY SUPPLY CHAINS IN THE ASIA-PACIFIC, OPTIONS FOR THE UNITED STATES TO DE-RISK AND DIVERSIFY

Taylore Roth, Samuel Naumann, Sarah Mortensen, Peter Heine, Amanda Sayre, John Ver Wey, and Adam Attarian | National Bureau of Asian Research | November 29, 2023

The People's Republic of China controls key nodes throughout U.S. critical technology supply chains, intensifying pressure for U.S. policymakers to diversify and establish alternatives. This analysis leverages an econometric approach to evaluating critical technology supply chains, as defined by the U.S. Department of Commerce's International Trade Administration, with the intention of identifying U.S. supply chain vulnerabilities and opportunities for trade diversification. As the Biden administration's Indo-Pacific Economic Framework looks to bolster investment and trade relationships with allies and partners in the region, trade analysis can help identify specific areas of mutual interest and opportunity. In particular, four critical technologies are key to future advances in computing and clean energy (fuel cells, nuclear power, neodymium magnets, and semiconductors), while specific supply chain nodes present strategic vulnerabilities.

Read the full article here.

CHINA-WATCHING COMMITTEE WARNS US CONGRESS ABOUT BEIJING'S 'MAGIC WEAPON'

Aadil Brar and John Feng | Newsweek | November 27, 2023

A bipartisan congressional committee is set to warn members of the U.S. Congress on Monday about threats posed to American politics and society by the "united front" system of China's ruling Communist Party, according to a memo shared with *Newsweek*. The document-the first on the subject produced by the House Select Committee on Strategic Competition between the United States and the Chinese Communist Party—will seek to inform Congress about what Beijing considers its "magic weapon."
The select committee on China, led by Reps. Mike Gallagher (R-WI) and Raja Krishnamoorthi (D-IL), was established earlier this year with the sole aim of highlighting issues of concern to both Republicans and Democrats. In particular, the group pledged to raise awareness on the CCP's political influence in the United States. The United Front Work Department, which answers to the Communist Party's Central Committee, oversees the broad spectrum of party's institutionalized influence operations and intelligence activities targeting groups inside and outside of China.

Read the full article here.

CONGRESS FEELING HEAT FROM GROUPS DEMANDING BAN ON CONTRACTS WITH CHINESE FIRM TAKING AMERICANS' DNA

Houston Keene | Fox News | November 29, 2023

Congress is feeling the heat from more than a dozen conservative groups that are calling for the passage of a National Defense Appropriations Act (NDAA) amendment to government contracts with a Chinese Communist Party (CCP)-linked biotech firm. Sixteen conservative groups sent a letter to senators and House lawmakers, calling on them to pass the NDAA provision to ban contracts with "adversarial biotech companies," specifically China's Beijing Genomics Institute (BGI). The amendments Gallagher, chairman of the House Select Committee on the CCP, told Fox News Digital that BGI "collects genetic data on people all over the world, to include that of pregnant women, and uses it for research with the Chinese military." "The CCP will undoubtedly use the genetic data collected by BGI to further its malign aggression, potentially even to develop a bioweapon used to target the American people," Gallagher warned.

Read the full article here.

THE EVOLUTION OF CHINA'S INTERFERENCE IN TAIWAN

Tim Niven | The Diplomat | December 1, 2023

On January 13, 2024, Taiwan will once again elect a president according to the country's own constitution. Once again, Taiwan's democracy will operate despite pressure from the People's Republic of China (PRC). For decades, China has engaged in foreign information manipulation and interference (FIMI) targeting Taiwan, and has optimized its tactics, techniques, and procedures, with the ultimate goal of annexing Taiwan. Beijing's sustained, long-term FIMI campaigns affect the context of every election in Taiwan, and particularly presidential elections, where cross-strait issues dominate voter concerns. FIMI efforts sustained over such a long timescale provide abundant opportunities for learning from trial and error. At Doublethink Lab, we have been observing and analyzing PRC FIMI targeting Taiwan for the last five years. Our observations to date suggest an evolution in tactics that appear to optimize the role of the different actors in China's FIMI apparatus, leading to reduced risks and costs associated with attribution, while increasing effectiveness and driving societal polarization.

Read the full article here.

CAN U.S.-CHINA STUDENT EXCHANGE SURVIVE GEOPOLITICS?

Vivian Wang | New York Times | November 28, 2023

On a cool Saturday morning, in a hotel basement in Beijing, throngs of young Chinese gathered to do what millions had done before them: dream of an American education. At a college fair organized by the U.S. Embassy, the students and their parents hovered over rows of booths advertising American universities. As a mascot of a bald eagle worked the crowd, they posed eagerly for photos. But beneath the festive atmosphere thrummed a note of anxiety. Did the United States still want Chinese students? And were Chinese students sure they wanted to go to the United States? "We see the negative news, so it's better to be careful," said Zhuang Tao, the father of a college senior considering graduate school in the United States, Australia and Britain. He had read the frequent headlines about gun violence, anti-Asian discrimination and, of course, tensions between the United States and China, at one of their highest levels in decades. "After all, the entire situation is a bit complicated." Students have been traveling between China and the United States for generations, propelled by ambition, curiosity and a belief that their time abroad could help them better their and their countries' futures.

Read the full article here.

BRITISH DOCUMENTARY ALLEGES CHINA INFLUENCES UNIVERSITIES, SPIES ON HONG KONGERS IN UK

Lyndon Lee | VOA | December 1, 2023

A BBC Channel 4 documentary, "Secrets and Power: China in the UK," claims the Chinese government is interfering with academic freedom and spying on Hong Kong activists in the United Kingdom. The 49-minute film released Wednesday alleges that the University of Nottingham used a Beijing-approved curriculum in classes taught on a satellite campus in Ningbo and closed its School of Contemporary Chinese Studies under pressure from Beijing. The program also claims a professor at the Imperial College London collaborated with researchers at a Chinese university on the use of artificial intelligence weaponry that could be used to benefit the Chinese military. Both institutions deny the allegations. The film also alleges that Chinese government agents pretending to be journalists used fake profiles and avatars to target Hong Kong activists now living in the U.K. VOA Mandarin sent an email to the Chinese Embassy in the United Kingdom seeking comments on the claims in the documentary but has not received a response.

Read the full article here.

DESPITE RISK, AI RESEARCH IS 'ENTANGLED' WITH CHINA-STUDY

Yojana Sharma | University World News | November 28, 2023

European Union Commission President Ursula von der Leyen and other European leaders have referred to 'derisking' relations with China, including research collaboration in the key field of artificial intelligence, but Europe is still 'entangled with China' when it comes to AI research, according to a new report. AI research collaboration between China and Europe has grown significantly in the five years from 2017 to 2022, despite temporary disruption from the COVID-19 pandemic, according to the report from the Mercator Institute for China Studies (MERICS) in Berlin. "AI research collaboration is valuable for China and for Europe. China's growing importance in the field makes it a critical partner," it states. Yet some of these collaborations are clearly benefitting China's military and the Chinese government's authoritarian aims. And there are also concerns that the deployment of ever more capable AI systems, like generative AI GPT-4, could "pose serious social and even existential risks", unless effort is devoted to safety, alignment and other risk research, states the MERICS report.

Read the full article here.

CHOKEPOINT CONSORTIUM: CHINESE EXPERTS ON CONFRONTING AMERICAN PRESSURE

Michael Laha | The Jamestown Foundation Global Research and Analysis | December 1, 2023

News broke this September that Huawei released a new 5G-capable phone produced with domestic chip technology reportedly in contravention of US export controls. While experts disagree to what extent this new product represents a true domestic breakthrough, it serves as an important symbolic win for a nation-wide effort by the People's Republic of China (PRC) to overcome restrictions imposed by the United States (SCMP, September 6; SCMP, September 30). Concerns about becoming technologically independent have by now become an enduring thrust of PRC leadership's strategic thinking. Just this week, President Xi Jinping visited the Shanghai Science and Technology Innovation Exhibition in order to promote the city's importance to this mission (*People's Daily*, November 29). The seeds of China's self-reliance strategy were planted many years ago and gained real momentum when the United States began scrutinizing Huawei.

Read the full article here.

USEFUL RESOURCES

SAFEGUARDING THE PUBLIC-RUSSIAN INTELLIGENCE POSES A PERSISTENT THREAT TO THE UNITED STATES

Federal Bureau of Investigation and National Counterintelligence and Security Center

Despite Russia's substantial military losses since its February 2022 invasion of Ukraine, Russia's intelligence services (RIS) remain a formidable threat to the United States. In recent months, the U.S. government has sanctioned several Russian intelligence operatives and their associates for activities targeting the United States, and authorities across Europe have arrested and charged a number of suspected Russian spies in their nations. Even so, in public remarks in September 2023, FBI Director Christopher Wray warned the number of Russian intelligence officers operating in the United States is "still way too big."

View the full resource here.

EMPOWERING THE FRONTLINE, WHERE SECURITY AND INDUSTRY INTERSECT

Bureau of Industry and Security

View the full resource here.

HOLIDAY ONLINE SHOPPING TIPS

Cybersecurity and Infrastructure Security Agency | November 21, 2023

The holiday season is a prime time for hackers, scammers, and online thieves. While millions of Americans will be online looking for the best gifts and Cyber Monday deals, hackers will be looking to take advantage of unsuspecting shoppers by searching for weaknesses in their devices or internet connections or attempting to extract personal and financial information through fake websites or charities. The best defense against these threats is awareness. There are a few simple steps we all can take to be more secure before and after we shop.

View the full resource here.