ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

September 28, 2022

TRANSITIONING TO A QUANTUM-SECURE ECONOMY

White Paper | World Economic Forum | In collaboration with Deloitte | September 2022

Quantum computing promises transformative simulation and modelling capabilities across a diverse range of industries. However, these advances in computational power will also introduce significant risks via the potential threat of disruption to some widely used encryption standards. While definitive timelines for both quantum computing applications and the associated quantum cybersecurity threats have not yet fully materialized, organizations must act now to evaluate their readiness to adapt to the quantum threat. The quantum threat is expected to have a large and disruptive impact on the current digitally dependent economy. An orderly response is highly desirable over a reactive one. It is a business imperative that organizations start to think about what a secure quantum transition could look like and understand their cryptographic and data exposure to avoid disruption of business operations. The unknown timeline of this quantum risk – which could lead to a "not me, not now" response – may impose a more significant impact than is necessary. This white paper arises from in-depth discussions between senior leaders and quantum experts from the quantum security working group, part of the quantum computing network of the World Economic Forum.

Read the full article here.

CONTROL SYSTEM DEFENSE: KNOW THE OPPONENT

U.S. Joint Cybersecurity Advisory | September 2022

Operational technology/industrial control system (OT/ICS) assets that operate, control, and monitor day-to-day critical infrastructure and industrial processes continue to be an attractive target for malicious cyber actors. These cyber actors, including advanced persistent threat (APT) groups, target OT/ICS assets to achieve political gains, economic advantages, or destructive effects. Because OT/ICS systems manage physical operational processes, cyber actors' operations could result in physical consequences, including loss of life, property damage, and disruption of National Critical Functions. OT/ICS devices and designs are publicly available, often incorporate vulnerable information technology (IT) components, and include external connections and remote access that increase their attack surfaces. In addition, a multitude of tools are readily available to exploit IT and OT systems. As a result of these factors, malicious cyber actors present an increasing risk to ICS networks. Traditional approaches to securing OT/ICS do not adequately address current threats to those systems. However, owners and operators who understand cyber actors' tactics, techniques, and procedures (TTPs) can use that knowledge when prioritizing hardening actions for OT/ICS.

Read the full article here.

SCIENTISTS AT AMERICA'S TOP NUCLEAR LAB WERE RECRUITED BY CHINA TO DESIGN MISSILES AND DRONES, REPORT SAYS

Ken Dilanian | NBC News | September 21, 2022

At least 154 Chinese scientists who worked on government-sponsored research at the U.S.'s foremost national security laboratory over the last two decades have been recruited to do scientific work in China — some of which helped advance military technology that threatens American national security — according to a new private intelligence report obtained by NBC News. The report, by Strider Technologies, describes what it calls a systemic effort by the government of China to place Chinese scientists at Los Alamos National Laboratory, where nuclear weapons were first developed. Many of the scientists were later lured back to China to help make advances in such technologies as deep-earth-penetrating warheads, hypersonic missiles, quiet submarines and drones, according to the report. Scientists were paid as much as $1 million through participation in Chinese government "talent programs," which are designed to recruit Chinese scientists to return to China.

Read the full article here.

IRANIAN HACKERS TARGET HIGH-VALUE TARGETS IN NUCLEAR SECURITY AND GENOMIC RESEARCH

Ravie Lakshmanan | The Hacker News | September 13, 2022

Hackers tied to the Iranian government have been targeting individuals specializing in Middle Eastern affairs, nuclear security and genome research as part of a new social engineering campaign designed to hunt for sensitive information. Enterprise security firm attributed the targeted attacks to a threat actor named TA453, which broadly overlaps with cyber activities monitored under the monikers APT42, Charming Kitten, and Phosphorus. It all starts with a phishing email impersonating legitimate individuals at Western foreign policy research organizations that's ultimately designed to gather intelligence on behalf of Iran's Islamic Revolutionary Guard Corps (IRGC). Spoofed personas include people from Pew Research Center, the Foreign Policy Research Institute (FRPI), the U.K.'s Chatham House, and the scientific journal Nature. The technique is said to have been deployed in mid-June 2022. What's different from other phishing attacks is the use of a tactic Proofpoint calls Multi-Persona Impersonation (MPI), wherein the threat actor employs not one but several actor-controlled personas in the same email conversation to bolster the chances of success.

Read the full article here.

PROFESSOR, NASA RESEARCHER PLEADS GUILTY IN CHINA TIES CASE

Associated Press | Voice of America (VOA) | September 23, 2022

A NASA researcher and Texas A&M University professor pleaded guilty to charges related to hiding his ties to a university created by the Chinese government while accepting federal grant money. Zhengdong Cheng pleaded guilty to two counts — violation of NASA regulations and falsifying official documents — during a hearing in Houston federal court Thursday. Cheng's conviction was part of a program called the China Initiative, which was first started under the Trump administration. But in February, the Justice Department abandoned the program after complaints it chilled academic collaboration and contributed to anti-Asian bias. The department had also endured high-profile setbacks in individual prosecutions, resulting in the dismissal of multiple criminal cases against academic researchers in the last year. The Justice Department said it planned to impose a higher bar for such prosecutions. Cheng had originally been charged with wire fraud, conspiracy and false statements when he was arrested in August 2020. But he pleaded guilty to the new charges as part of an agreement with federal prosecutors.

Read the full article here.

A SINISTER WAY TO BEAT MULTIFACTOR AUTHENTICATION IS ON THE RISE

Dan Goodin | Wired | March 30, 2022

Multifactor authentication (MFA) is a core defense that is among the most effective at preventing account takeovers. In addition to requiring that users provide a username and password, MFA ensures they must also use an additional factor—be it a fingerprint, physical security key, or one-time password—before they can access an account. Nothing in this article should be construed as saying MFA isn't anything other than essential. That said, some forms of MFA are stronger than others, and recent events show that these weaker forms aren't much of a hurdle for some hackers to clear. In the past few months, suspected script kiddies like the Lapsus$ data extortion gang and elite Russian-state threat actors (like Cozy Bear, the group behind the SolarWinds hack) have both successfully defeated the protection. The strongest forms of MFA are based on a framework called FIDO2, which was developed by a consortium of companies to balance security and simplicity of use.

Read the full article here.

USA ADDS TWO MORE CHINESE CARRIERS TO 'PROBABLY A NATIONAL SECURITY THREAT' LIST

Laura Dobberstein | The Register | September 21, 2022

The US Federal Communications Commission (FCC) has added two Chinese companies to its list of communications equipment suppliers rated a threat to national security: Pacific Network Corp, its wholly owned subsidiary ComNet (USA) LLC, and China Unicom (Americas). "Earlier this year the FCC revoked China Unicom America's and PacNet/ComNet's authorities to provide service in the United States because of the national security risks they posed to communications in the United States. Now, working with our national security partners, we are taking additional action to close the door to these companies by adding them to the FCC's Covered List," said Chairwoman Jessica Rosenworcel. The latest additions join Huawei, ZTE Corporation, radio-comms vendor Hytera, video surveillance systems Hikvision and Dahua, as well as Russia-based cybersecurity firm Kaspersky, plus telecom companies China Mobile and China Telecom, who are already on the list. The new companies earned a spot on the now ten-strong list as they are believed to be "subject to the exploitation, influence and control of the Chinese government, and the national security risks associated with such exploitation, influence, and control." Therefore, they pose "an unacceptable risk to the national security of the United States."

Read the full article here.

US NEEDS TO REFORM EFFORTS TO STOP ENEMY SPIES, REPORT SAYS

Nomaan Merchant | Associated Press | September 20, 2022

A new Senate study warns that U.S. spy agencies' efforts to stop China and other adversaries from stealing secrets are hampered by miscommunication and a lack of money and staff at the office intended to coordinate those efforts. The report comes amid warnings that Chinese and Russian attempts to obtain sensitive data and meddle in elections are on the rise. The Senate Intelligence Committee report released Tuesday says the National Counterintelligence and Security Center, which is supposed to coordinate efforts by the U.S. government, doesn't have a clear mission and is limited in its authority. NCSC cannot fund or mandate programs for many government agencies or private companies that hold secrets prized by foreign spy services. There's also disagreement among intelligence officials about who should lead responses to cyberattacks and campaigns trying to influence Americans — and whether those efforts should be categorized as counterintelligence, the report says.

Read the full article here.

THE RISING RISK OF CHINA'S INTELLECTUAL-PROPERTY THEFT

Derek Scissors | National Review | July 15, 2021

In the economic competition, the main American challenge is not, as is sometimes implied, inadequate innovation. The U.S. is the world's wealthiest country by tens of trillions of dollars. The number of U.S. patents granted to Ameri-cans set a record in 2019 and nearly matched it in 2020. That more than tripled the number of patents granted to second-place Japanese filers in our market. The main challenge is not even Chi-nese innovation. Beijing's preference for large firms and state funding at the expense of genuine competition ensures it will struggle in key areas, from aircraft development to shale. The main challenge is China's acquisition of intellectual property (IP) and use of regulatory and financial subsidies to develop products from that IP to drive the U.S. out of global markets. Pending legislation may, if passed, increase these risks. The United States Innovation and Competition Act (USICA) has passed the Senate, while the National Science Foundation for the Future Act has passed the House. Each spends at least $100 billion over five years on U.S. research and development, but the Senate included many more provisions attempting to limit Chinese access than the House has to date. Without stronger safeguards than even the Senate currently includes, China will be able to capture the technology developed by additional U.S. re-search, subsidize its deployment, and actually bring harm to American companies and workers rather than the benefits Congress imagines. That the People's Republic of China (PRC) will continue seeking to acquire American research is not seriously debatable.

Read the full article here.

THE LOS ALAMOS CLUB: COWARDICE HAS CONSEQUENCES

David Acevedo | National Association of Scholars | September 23, 2022

The People's Republic of China (PRC) has engaged in research theft and academic espionage in American higher education for some time. Whether it be on the institutional level through Confucius Institutes or on the individual level through the Thousand Talents Plan and other "talent programs," the last five years have made abundantly clear that China intends to steal as much intellectual property as possible, and that the U.S. intends to do little, if anything, about it. This problem, however, seems to be much worse than we thought. A new bombshell report by Strider Technologies, titled The Los Alamos Club: How the People's Republic of China Recruited Leading Scientists from Los Alamos National Laboratory to Advance Its Military Programs, provides crucial insight into the extent to which China has infiltrated American research—in this case, sensitive government research. The findings of this study should deeply concern all who care about research integrity and U.S. national security. Strider is a research and intelligence firm that helps companies "proactively identify, manage, and respond to nation-state directed IP [intellectual property] theft and supply chain vulnerabilities." It conducts research on a wide range of intelligence-related issues, which, these days, includes a significant amount of work on China.

Read the full article here.

U.S.-CHINA TENSIONS FUEL OUTFLOW OF CHINESE SCIENTISTS FROM U.S. UNIVERSITIES

Sha Hua and Karen Hao | The Wall Street Journal | September 22, 2022

An increasing number of scientists and engineers of Chinese descent are giving up tenured positions at top-tier American universities to leave for China or elsewhere, in a sign of the U.S.'s fading appeal for a group that has been a driver of innovation. The trend, driven in part by what many of the scholars describe as an increasingly hostile political and racial environment, has caused the Biden administration to work with scholars of Chinese descent to address concerns.

Read the full article here.

CHINESE FIRMS ARE NOT ALL SERIAL INTELLECTUAL-PROPERTY THIEVES

The Economist | February 9, 2019

Wars sometimes have moments of cultural levity—even trade wars. Last summer, as America and China were bombarding each other with tariffs, a quaint exhibition opened at the National Museum of China on Tiananmen Square paying tribute to, of all things, American intellectual-property (IP) protection. It was a surprise hit. More than 1m visitors filed past 60 beautifully crafted models of inventions, such as an ice-cream maker, submitted to the United States Patent Office between 1836 and 1890 (all property of the Hagley Museum in Delaware). No doubt some visitors were arm-twisted to go, because it coincided with the start of an innovation drive by President Xi Jinping. But many were simply in thrall to American inventiveness. One remarkable visitor, says David Cole, the Hagley Museum's boss, was an elderly man, Hu Guohua, who was granted the first-ever patent in Communist China, in 1985. It was a reminder of how young IP protection is in China; in America the first patent dates back to 1790 and was signed by George Washington. IP is one of the main fronts in President Donald Trump's trade war against China. It is also the crux of an indictment in America against Huawei, a Chinese tech giant. In both cases, the government seeks to give the impression that stealing from the West is part of the modus operandi of Chinese firms, something a *Wall Street Journal* columnist described last week as a practice they regard as a "patriotic duty".

Read the full article here.