ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

January 5, 2022

PROTECT YOUR ORGANIZATION FROM THE FOREIGN INTELLIGENCE THREAT

National Counterintelligence and Security Center | December 13, 2021

Today the global threat environment is more diverse and dynamic than ever. As spelled out in the latest Annual Threat Assessment of the U.S. Intelligence Community (IC), a growing number of state actors and non-state actors are targeting the United States. They are no longer just interested in obtaining classified U.S. secrets but also are collecting information from almost all U.S. Government agencies and virtually every sector of the U.S. economy. Personal data, trade secrets, intellectual property, technology, and research and development are all being targeted by adversaries who have the capabilities, patience, and resources to get them. To achieve their objectives, foreign adversaries are employing a range of illegal techniques, including insider threats, cyber penetrations, supply chain attacks, and blended operations that combine some or all these methods. They are also using a variety of legal and quasi-legal methods, including mergers and acquisitions, investments, joint ventures, partnerships, and talent recruitment programs to acquire U.S. technology and innovation. Ultimately, they seek to degrade our economic power and national security, compromise our critical infrastructure, and undermine our democratic institutions and ideals. This new form of conflict is not fought on a foreign battlefield, but in our power grids, our computer networks, our laboratories and research facilities, our financial institutions, our healthcare providers, and our federal, state, local, and tribal governments.

Read the full article here.

5 CYBERSECURITY TRENDS TO WATCH IN 2022

Becky Bracken | Threatpost | December 29, 2021

No one could have predicted the sheer chaos the cybersecurity industry would experience over the course of 2021. Record-annihilating numbers of ransomware attacks, SolarWinds' supply-chain havoc and most recently, the discovery of Log4j by…Minecraft gamers. All of it would have sounded too wild for real life a short year ago. Yet here we are. Predictions about the year ahead seem audacious considering the last 12 months, so instead, Threatpost talked to industry experts and developed this list of the five top trends to watch in 2022.

Read the full article here.

TOP 5 ESPIONAGE CASES OF 2021

Christopher Burgess | ClearanceJobs | December 27, 2021

This year's key espionage cases were once again dominated by the United States economic and geopolitical adversaries: Russia and China. The year also saw a number of insiders, with access to some of the nation's most sensitive secrets, attempt to sell those secrets to foreign nations. As 2021 comes to a close there is no sign of abatement in the nation's adversaries intent to conduct espionage activities, nor, sadly a reduction in the number of trusted insiders becoming untrustworthy. While 2020 had a clear highlight with Peter Debbins and his espionage on behalf of Russia coming to a close, 2021 still had quite a few cases and lessons to study. Here are the five top espionage topics/cases of 2021.

Read the full article here.

DOCUMENTS SHOW CHINESE GOVERNMENT COLLECTS DROVES OF DATA FROM WESTERN SOCIAL MEDIA: REPORT

Joseph Choi | The Hill | December 31, 2021

China is using part of its internal internet surveillance network to mine data from Western social media and provide its government agents with information on foreign targets, The Washington Post reported on Friday. Reviewing hundreds of Chinese bidding documents, contracts and company filings, the Post reported that China's public opinion analysis software — used to detect politically sensitive information online — was also being used to collect information on foreign targets through U.S. companies like Twitter and Facebook. Not only is China using its pre-existing software to gather data, it is also investing in more sophisticated programs to further its ambitions, the Post reported. One $320,000 Chinese state media software program reportedly mines through Twitter and Facebook to create a database of foreign journalists and academics. Other programs have reportedly been developed to observe Western and foreign language in Hong Kong and Xinjiang, two places where the international community has condemned China for its alleged human rights violations. The Post reported that these operations have been in the works since the beginning of 2020.

Read the full article here.

CHINESE APT HACKERS USED LOG4SHELL EXPLOIT TO TARGET ACADEMIC INSTITUTION

Ravie Lakshmanan | The Hacker News | December 30, 2021

A never-before-seen China-based targeted intrusion adversary dubbed Aquatic Panda has been observed leveraging critical flaws in the Apache Log4j logging library as an access vector to perform various post-exploitation operations, including reconnaissance and credential harvesting on targeted systems. Cybersecurity firm CrowdStrike said the infiltration, which was ultimately foiled, was aimed at an unnamed "large academic institution." The state-sponsored group is believed to have been operating since mid-2020 in pursuit of intelligence collection and industrial espionage, with its attacks primarily directed against companies in the telecommunications, technology, and government sectors. The attempted intrusion exploited the newly discovered Log4Shell flaw (CVE-2021-44228, CVSS score: 10.0) to gain access to a vulnerable instance of the VMware Horizon desktop and app virtualization product, followed by running a series of malicious commands orchestrated to fetch threat actor payloads hosted on a remote server. "A modified version of the Log4j exploit was likely used during the course of the threat actor's operations," the researchers noted, adding it involved the use of an exploit that was published in GitHub on December 13, 2021.

Read the full article here.

US COLLABORATION WITH CHINA CRITICAL DESPITE RIVALRY, FORMER TOP DEFENSE OFFICIAL ARGUES

Government Matters | January 4, 2022

While maintaining the United States' technological edge with China is essential, the balance of power will ultimately not be determined by technology but by diplomacy, alliances and strategic choices, according to Joseph Nye, former assistant secretary of defense for international security affairs, now distinguished service professor, emeritus at Harvard University. The U.S. is economically and ecologically interdependent with China and must work with the country to address global issues like climate change in order to advance U.S. interests, said Nye. He said the two nations are playing a "three-dimensional chess game" with military, economic and ecological boards, the third encompassing transnational concerns like pandemics and the environment. Nye suggested development of a special set of trade relations for telecommunications with democratic countries and recommended the U.S. take soft power – influence through attraction as opposed to coercion – seriously.

Read the full article here.

CHINA WILL 'EXHAUST ALL MEANS' TO LURE GLOBAL TALENT, DESPITE PUSH FOR TECH SELF-SUFFICIENCY, XI JINPING SAYS

Luna Sun | South China Morning Post | December 16, 2021

China is calling for more global talent to bolster technological innovation and national power, amid growing concern from foreign investors that Beijing's "dual-circulation" strategy might turn it further inward and hamper international collaboration. China will "exhaust all means" to recruit intelligent and innovative professionals from around the world, President Xi Jinping said in a speech to a key national talent work conference in September. The transcript, published on Thursday on Qiushi, a state journal covering the Chinese Communist Party's governing philosophy, laid out a specific timetable for China to become a world power in science and technology within two decades. "The emphasis on independent cultivation of talent must not mean self-isolation," Xi said. "China needs participation of global talent, while its development also provides opportunities for global talent." Xi said China must implement more proactive policies to lure top professionals, which are in short supply, and form a "talent system with global appeal and competitive advantage".

Read the full article here.

U.S.-CHINA TECHNOLOGY COMPETITION

Ryan Hass, Patricia M. Kim, and Emilie Kimball | Brookings | December 23, 2021

The scale and speed of China's technological advancements in recent years have raised concerns in Washington and elsewhere over the implications for the United States' overall economic competitiveness and its national security, as well as the impact on liberal values and good governance globally. There also has been growing concern about the fragmentation of the global technology sector, including the rise of divergent standards and norms, as the Chinese technology market increasingly decouples from those of the United States and the West more broadly. To evaluate the merits of these concerns and identify potential policy remedies to them, Ryan Hass, Patricia M. Kim, and Emilie Kimball, the co-leads of the Brookings Foreign Policy project "Global China: Assessing China's Growing Role in the World," convened 10 additional Brookings scholars for a written exchange on the role of technology in U.S.-China competition. These experts, drawn from a range of disciplines, were asked to offer their best judgments on the implications of China's growing technological capabilities and steps the United States could take.

Read the full article here.

AI POWERS AUTONOMOUS MATERIALS DISCOVERY

Tom Fleischman | Cornell Chronicle | December 17, 2021

When a master chef develops a new cake recipe, she doesn't try every conceivable combination of ingredients to see which one works best. The chef uses prior baking knowledge and basic principles to more efficiently search for that winning formula. Materials scientists use a similar method in searching for novel materials with unique properties in fields such as renewable energy and microelectronics. And a new artificial intelligence tool developed by Cornell researchers promises to rapidly explore and identify what it takes to "whip up" new materials. SARA (the Scientific Autonomous Reasoning Agent) integrates robotic materials synthesis and characterization, along with a hierarchy of artificial intelligence and active learning methods, to efficiently reveal the structure of complex processing phase diagrams, making materials discovery vastly quicker. Sebastian Ament, doctoral student in the field of computer science, and Maximilian Amsler, former postdoctoral researcher and now a visiting scientist at Cornell, are co-lead authors of "Autonomous Synthesis Via Hierarchical Active Learning of Nonequilibrium Phase Diagrams," which published Dec. 17 in Science Advances.

Read the full article here.

CHARLES LIEBER: HARVARD PROFESSOR GUILTY OF HIDING TIES TO CHINESE PROGRAMME

BBC News | December 22, 2021

Charles Lieber was found guilty of making false statements to authorities, filing false tax returns and failing to report a Chinese bank account. His sentencing date is yet to be decided. The 62-year-old was charged in 2020 as part of a US campaign to counter economic espionage from China. However, some critics say this campaign harms academic research. Prosecutors in Boston said Lieber knowingly hid his involvement in China's "Thousand Talents Plan", which aims to attract foreign research specialists. It has been flagged by the US as a security concern in the past. Lieber, a former head of Harvard's department of chemistry and chemical biology, had in 2011 joined China's Wuhan University of Technology as a scientist. He was given a monthly salary of $50,000 (£37,000), in addition to living expenses of up to $158,000 for this role. The filings say he was also given more than $1.5m to establish a research lab at the university and, in return, was expected to work for the university, applying for patents and publishing articles in its name.

Read the full article here.

IS INSIDER RISK THREATENING YOUR GROWTH AND INNOVATION?

Ananth Appathurai | Fast Company | December 21, 2021

A lot has changed in a short amount of time. With the rush to remote work at the onset of the pandemic, digital transformation shifted from a growth and productivity strategy to a business imperative necessary to keep organizations running. Even those organizations that were already hybrid had to suddenly support an entire remote staff—effectively overnight. As we transition, with stops and starts, into the new world of hybrid remote work, it's apparent that there's no going back. Digital transformation timelines jumped ahead by seven years in a matter of weeks in early 2020 and things aren't slowing down anytime soon. We are now riding the crest of a second wave of digital transformation that is sweeping every company and every industry as companies aggressively target growth. This second wave is great for innovation, but it brings with it an inherent risk that can have unexpected ramifications across any business: Insider risk is growing and it threatens to limit the speed, agility, and innovation that organizations are counting on to power their growth.

Read the full article here.

A RECENT SPY CASE SHOWS HOW CHINA HAS BEEN ABLE TO PULL OFF ITS WHIRLWIND MILITARY MODERNIZATION

Stavros Atlamazoglou | Insider | December 13, 2021

A historic court decision sheds light on how China has used espionage to gain a military and economic advantage over the US and the rest of the world. US counterintelligence officials managed to lure Yanjun Xu, a senior Chinese intelligence officer, out of China in 2018 and then get him extradited to the US to stand trial for attempting to steal advanced aircraft-engine technology, which China's military has struggled to develop. This case is only the latest in a series of espionage operations by Beijing meant to steal industrial and military secrets from the US and its allies and partners and even from Russia — theft that has allowed China's military to rapidly build its arsenals of sophisticated weapons. On November 5, a federal jury convicted Xu — deputy division director of the Sixth Bureau of the Jiangsu Province Ministry of State Security (MSS), the primary intelligence agency of the Chinese Communist Party — of "conspiring to and attempting to commit economic espionage and theft of trade secrets." The Chinese intelligence officer was coordinating an operation to get access to a General Electric Aviation composite aircraft engine fan, a piece of technology no other firm has been able to reproduce.

Read the full article here.

DOCUMENTS LINK HUAWEI TO CHINA'S SURVEILLANCE PROGRAMS

Eva Dou | The Washington Post | December 14, 2021

The Chinese tech giant Huawei Technologies has long brushed off questions about its role in China's state surveillance, saying it just sells general-purpose networking gear. A review by The Washington Post of more than 100 Huawei PowerPoint presentations, many marked "confidential," suggests that the company has had a broader role in tracking China's populace than it has acknowledged. These marketing presentations, posted to a public-facing Huawei website before the company removed them late last year, show Huawei pitching how its technologies can help government authorities identify individuals by voice, monitor political individuals of interest, manage ideological reeducation and labor schedules for prisoners, and help retailers track shoppers using facial recognition. "Huawei has no knowledge of the projects mentioned in the Washington Post report," the company said in a statement, after The Post shared some of the slides with Huawei representatives to seek comment.

Read the full article here.

TECH ADVANTAGE CRITICAL TO PREVAIL IN STRATEGIC COMPETITION WITH CHINA, DOD OFFICIAL SAYS

Terri Moon Cronk | U.S. Department of Defense | November 5, 2021

Technological capability on an ongoing basis is critical to the United States maintaining its edge against other nations, such as China, Michael Brown, director of the Defense Innovation Unit, said yesterday. At the 2021 Aspen Security Forum in Washington, D.C., Brown discussed preserving the United States' technological edge and quickly getting new technology into the hands of U.S. warfighters. "We need technological advantage to prevail in this strategic competition with China," the DIU director said. "For the military, that means that we've got to modernize faster. We [have] got to use more commercial technology." Brown added that requirements in acquisition and budgeting must again work for the Pentagon. "I've been leading DIU for three years now, and what I see is [that] we're not going fast enough. We're not transforming at the scale that we need to make changes to address the threat with China."

Read the full article here.

PROTECTING YOUR ORGANIZATION'S SECRETS

National Counterintelligence and Security Center | January 3, 2019

Foreign adversaries and competitors are actively seeking information that is vital to our national and economic security, U.S. global competitiveness, and your organization's mission. This includes: Sensitive or proprietary financial, trade, or economic policy information, pioneering research and development, emerging technologies, sector-specific information, including commerce, transportation, agriculture, health, homeland security, energy, and communications. You have access to facilities and computer networks, as well as sensitive information, resources, technologies, research and other data that our foreign adversaries and competitors desperately want. Our adversaries and competitors are interested in you because you have connections and access. You also have social media accounts. A work and/or personal smartphone. Social and professional networks include others in sensitive positions. You may travel, both domestically and abroad. These are all potential vulnerabilities.

Read the full article here.

HOW TO REBOOT A BROKEN OR OUTDATED SECURITY STRATEGY

John Edwards | CSO | January 18, 2021

An enterprise security strategy should be like a weather report: subject to frequent updates. Allowing a security plan to fall out of sync with current and emerging threats, as well as evolving enterprise technologies and interests, can open the door to financial and reputational catastrophes. Many elements contribute to a comprehensive security strategy and just as many factors can break or outdate a once-formidable security blueprint. "People, process, and technology are the key areas," says Greg Carrico, senior cybersecurity manager at business and technology consulting firm Capgemini North America. "Companies that don't maintain a pulse on current events, process automation, review cycles and current technical skillsets may continue to struggle with the protection of their most critical items without even realizing that threat actors have set their proverbial sights on them." The best security plans are crisp, relevant, and easily understood by everyone across the entire enterprise.

Read the full article here.

HOW BIG TECH FACTORS INTO THE US-CHINA GEOPOLITICAL COMPETITION

Emily De La Bruyère and Nathan Picarsic | The Hill | October 22, 2020

On Oct. 6, the House Judiciary Committee issued a report calling for new antitrust regulations to rein in Big Tech. This report comes after a 15-month antitrust probe into technology firms Google, Apple, Amazon, Twitter and Facebook - and with it, findings that the tech giants all hold monopoly power. Congress is making the wrong call - not because of what was in the House report, but because of what was not: These 450 pages, the antitrust probe, and the national conversation about Big Tech writ large ignore the strategic context. They assume that the U.S. system sits in a vacuum; that the alternative to Big Tech is small, or smaller, tech. It is not. The alternative to U.S. Big Tech is China's Big Tech.

Read the full article here.