ASCE
ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM
https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

April 21, 2021

ALLEGED PLA AIR FORCE OFFICER PLEADS NOT GUILTY DESPITE FBI'S CLEAR EVIDENCE

Christopher Burgess | Clearance Jobs | April 20, 2021

There are over 350,000 visiting scholars and students from China in the United States. Some of them are there at the direction of and under the control of the Chinese government. Some are also members of the Chinese People's Liberation Army, Air Force and Navy and for reasons known only to the Chinese government opt to obscure and hide their military affiliation using cover stories and non-military affiliation. Chen Song is alleged to be such an individual. Chen Song is a Chinese national doing neurological research at Stanford University. The U.S. government, via the Department of Justice (DoJ), alleges Song hid her status as Chinese PLA Air Force officer when applying for and receiving her J1 visa and charged her on July 17, 2020 with visa fraud. She was arrested the next day. In February 2021 additional charges were levied against Song. She pleads, not guilty. FBI Director Wray commented in November 2020 how "The Chinese Communist Party's theft of sensitive information and technology isn't a rumor or a baseless accusation. It's very real, and it's part of a coordinated campaign by the Chinese government, which the China Initiative is helping to disrupt.

Read the full article here.

RUSSIAN FOREIGN INTELLIGENCE SERVICE EXPLOITING FIVE PUBLICLY KNOWN VULNERABILITIES TO COMPROMISE U.S. AND ALLIED NETWORKS

U.S. Department of Justice Federal Bureau of Investigation | April 15, 2021

The National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) jointly released a Cybersecurity Advisory, "Russian SVR Targets U.S. and Allied Networks," today to expose ongoing Russian Foreign Intelligence Service (SVR) exploitation of five publicly known vulnerabilities. This advisory is being released alongside the U.S. government's formal attribution of the SolarWinds supply chain compromise and related cyber espionage campaign. We are publishing this product to highlight additional tactics, techniques, and procedures being used by SVR so that network defenders can take action to mitigate against them. Mitigation against these vulnerabilities is critically important as U.S. and allied networks are constantly scanned, targeted, and exploited by Russian state-sponsored cyber actors.

Read the full article here.

FBI OPENS A CASE ON CHINESE ACTIVITY 'EVERY 10 HOURS,' INTEL CHIEFS SAY

Patrick Tucker | Defense One | April 14, 2021

The threat from China, multi-faceted and severe, is foremost in a pack that includes Russian actions in Ukraine, Iranian nuclear efforts, and North Korea's existing nukes, U.S. intelligence leaders told the Senate Intelligence Committee on Wednesday. "We have now over 2,000 investigations that tie back to the Chinese government," FBI Director Chris Wray said at the hearing. "On the economic espionage side alone, it's a 1,300 percent increase over the last several years. We're opening a new investigation on China every ten hours and I assure the committee it's not because our folks don't have anything to do with their time." The threat goes well beyond issues like intellectual property theft, which intelligence leaders have been highlighting for years now. It includes the covert harassment of Chinese individuals living in the United States and elsewhere, an operation that the FBI dubbed "Fox Hunt" in a series of indictments last October. Most of Wednesday's conversation focused on Chinese technology. Avril Haines, who leads the Office of the Director of National Intelligence, told lawmakers that there exists "a whole series of technology sectors where China is…contesting our leadership in effect."

Read the full article here.

COLD WAR II—JUST HOW DANGEROUS IS CHINA?

H. R. McMaster and Matt Pottinger | Hoover Institution | April 13, 2021

China is a nation with 1.3 billion people, an economy projected to become bigger than the United States' in just a few years, and a rapidly growing military. Hong Kong has already fallen under its authority. Meanwhile, Taiwan looms in the distance—with a population of almost 24 million, it's a technology hub and the world's leading manufacturer of microchips and other items essential to high tech. What are China's ambitions toward Taiwan? And if they are ominous, what should the US response to Chinese aggression be? To answer these questions, we're joined by two experts: former national security advisor (and current Hoover Institution senior fellow) H. R. McMaster and former US deputy national security advisor (and current Hoover distinguished visiting fellow) Matthew Pottinger. They also discuss the Biden administration's recent diplomatic encounters with China, and which countries might be allies in a conflict with China—and which ones would not be.

Watch the full interview here.

GLOBAL TRENDS 2040: A MORE CONTESTED WORLD

The National Intelligence Council | March 2021

Welcome to the 7th edition of the National Intelligence Council's Global Trends report. Published every four years since 1997, Global Trends assesses the key trends and uncertainties that will shape the strategic environment for the United States during the next two decades. Global Trends is designed to provide an analytic framework for policymakers early in each administration as they craft national security strategy and navigate an uncertain future. The goal is not to offer a specific prediction of the world in 2040; instead, our intent is to help policymakers and citizens see what may lie beyond the horizon and prepare for an array of possible futures. Each edition of Global Trends is a unique undertaking, as its authors on the National Intelligence Council develop a methodology and formulate the analysis. This process involved numerous steps: examining and evaluating previous editions of Global Trends for lessons learned; research and discovery involving widespread consultations, data collection, and commissioned research; synthesizing, outlining, and drafting; and soliciting internal and external feedback to revise and sharpen the analysis.

Read the full report here.

NATIONAL SUPPLY CHAIN INTEGRITY MONTH – CALL TO ACTION FRAMEWORK FOR ASSESSING RISKS

National Counterintelligence and Security Center

Increased risk to supply chains are due to evolving dependence on globally sourced commercial Information and Communication Technologies (ICT) for mission critical systems and services. Resulting residual risks are passed to end-user enterprises in the form of products and services that may contain defective, counterfeit or otherwise tainted components with malware, exploitable weaknesses and vulnerabilities from sources with unknown trust. This SCRM Framework addresses risk topics relevant to the reliance on others who make risk decisions about matters in which they are not the risk owners. The SCRM Framework also addresses means to identify and counter supply chain attacks that can exploit products and processes throughout the supply chain lifecycle.

Read the full article here.

CHINESE INTELLIGENCE RECRUITING PRIVATE RESEARCHERS, SCIENTISTS

Abhinandan Mishra | Sunday Guardian Live | April 17, 2021

The Chinese intelligence, or the Intelligence Bureau of the Joint Staff Department of the Central Military Commission of the People's Republic of China, is now recruiting private researchers, professors and scientists across European countries to gather strategic information for the Chinese. Among those who have been targeted are researchers with private and government universities who specialize in defence studies and scientists who are working with government and inter-governmental bodies. Such recruitment activity has taken place in prominent European countries like Germany, Poland and Estonia, an annual report released by the Estonia Internal Security Service (ISS) or KaPo, recently, has revealed. According to the report, Beijing's interference in the internal affairs of Estonia by recruiting private individuals is not limited to a theoretical prospect anymore. "For some time now, Beijing's actions have caused concerns for counterintelligence. The danger is no longer theoretical; it has been confirmed by the first court decision. Chinese intelligence recruited an Estonian citizen," the report reads.

Read the full article here.

FASTTAKE: WHAT'S MISSING FROM US INTEL'S 2021 THREAT ASSESSMENT

Barry Pavel and Ronald Marks | Atlantic Council | April 16, 2021

The Director of National Intelligence's Threat Assessment for 2021, released this week, outlines the US intelligence community's projection of the most dangerous threats to the United States over the next year—beginning with China as the primary threat facing the United States and proceeding "down the list" to Russia, Iran, and North Korea; then moving to transnational issues such as COVID-19, climate change, and terrorism; and then outlining ongoing instability in key regions of the world. In so doing, the report nicely parallels both the Biden administration's Interim National Security Strategic Guidance, released last month, as well as the preliminary outline of the administration's fiscal year 2022 budget, which was just presented to Capitol Hill. The report's assessment of disruptive technologies as major geopolitical tools is a relatively novel and long overdue element of this annual report, and one that we should expect to grow in prominence and importance throughout this new, turbulent decade.

Read the full article here.

CONGRESSMEN ASK BIDEN ADMIN TO KEEP CHIP DESIGN SOFTWARE AWAY FROM CHINA

Tim De Chant | ARS Technica | April 16, 2021

Don’t let American companies sell semiconductor design software to Chinese firms, two members of Congress are asking the Department of Commerce. Sen. Tom Cotton (R- Ark.) and Rep. Michael McCaul (R-Tex.) yesterday requested that electronic design automation (EDA) tools be designated as “foundational technologies” by the Department of Commerce. The label would require companies to obtain export licenses if they want to sell EDA tools to Chinese companies. The congressmen also requested in their letter to Secretary of Commerce Gina Raimondo that any fab worldwide that uses American tools be prevented from selling 14 nm or better chips to Chinese companies. The current leading edge in semiconductors is the 5 nm node, and currently, only Samsung and Taiwanese semiconductor company TSMC are producing chips commercially at that node. Restricting Chinese companies to 16 nm or larger could possibly keep them four generations off the leading edge.

Read the full article here.

A 'WORST NIGHTMARE' CYBERATTACK: THE UNTOLD STORY OF THE SOLARWINDS HACK

Dina Temple-Raston | NPR | April 16, 2021

"This release includes bug fixes, increased stability and performance improvements." The routine software update may be one of the most familiar and least understood parts of our digital lives. A pop-up window announces its arrival and all that is required of us is to plug everything in before bed. The next morning, rather like the shoemaker and the elves, our software is magically transformed. Last spring, a Texas-based company called SolarWinds made one such software update available to its customers. It was supposed to provide the regular fare — bug fixes, performance enhancements — to the company's popular network management system, a software program called Orion that keeps a watchful eye on all the various components in a company's network. Customers simply had to log into the company's software development website, type a password and then wait for the update to land seamlessly onto their servers. The routine update, it turns out, is no longer so routine.

Read the full article here.

ADELAIDE UNIVERSITY REFUSES MILLIONS IN RESEARCH PROJECTS DUE TO FOREIGN INTERFERENCE CONCERNS

Sara Tomevska | ABC News | April 14, 2021

The University of Adelaide has revealed it turned down seven collaborative research projects with overseas institutions due to concerns over foreign interference. The projects rejected include a research proposal from a Chinese multinational technology company based in Shenzhen, which the university said came at "significant financial cost" and "put the renewal of staff employment contracts in jeopardy". The university also turned down a research proposal in "advanced materials" from an Australian company, valued at $3 million, after a due diligence investigation revealed commercialisation funding was to come from a Hong Kong company linked to the "Panama Papers" scandal. Those projects were rejected before the federal government introduced new legislation in 2018 to clamp down on foreign interference in publicly-funded universities. Since that time, the university has rejected a further five research proposals. The revelations come from a submission the university made to a federal parliamentary joint committee on Intelligence and Security.

Read the full article here.

AUSTRALIAN UNIVERSITY REJECTS CHINESE-FUNDED RESEARCH WORTH MILLIONS FOR NATIONAL INTEREST

Rebecca Zhu | The Epoch Times | April 14, 2021

Several research projects and joint collaborations worth millions of dollars have been rejected by Adelaide University because of high-risk links to Beijing. In its submission to a national inquiry into security risks affecting higher education last month, the university revealed it rejected projects on the basis of national interest or university reputation. "As a leading Australian university in the fields of defence and cybersecurity, the University of Adelaide takes seriously its responsibilities towards foreign interference," a spokesman told The Epoch Times. "Examples provided to the Parliamentary committee help to illustrate the quality of the University's due diligence and are the direct result of improved practices and oversight in relation to these issues." One example was the rejection of a AU$3 million (US$2.3 million) project on advanced materials, which on the surface appeared to pose no risk as an Australian company was proposing it.

Read the full article here.

ANTI-CHINESE RACISM HINDERS EFFORTS TO COUNTER FOREIGN INTERFERENCE: PATERSON

Anthony Galloway | The Sydney Morning Herald | April 13, 2021

Liberal senator James Paterson says he is concerned about the rise in anti-Chinese racism in the wake of COVID-19, warning it is hampering efforts to counter foreign interference within Australia. The chairman of Parliament's powerful security and intelligence committee, an outspoken critic of Chinese Communist Party influence, said politicians needed to be careful not to stoke anti-Chinese or anti-Asian sentiment, adding it was something he thinks "deeply about". Chinese Australians have reported a significant rise in racist attacks over the past 12 months, with research showing one in five has been physically threatened or attacked because of their Chinese heritage. Senator Paterson said "anti-Chinese racism" and "anti-Asian racism" had increased during the global pandemic, "and that's the last thing I want to see".

Read the full article here.

CYBERATTACKS ARE SPIKING. COLLEGES ARE FIGHTING BACK.

Katherine Mangan | The Chronicle of Higher Education | April 14, 2021

The message, emailed to thousands of students and employees at the University of Colorado's Boulder campus last week, was alarming. Their personal information, including addresses, phone numbers, Social Security numbers, academic progress reports, and financial documents, had been stolen, and their university was refusing to cooperate with extortion demands. As a result, the data was starting to be posted on the dark web, the shadowy back channel of the internet where cybercriminals lurk. Elsewhere around the country, students and employees at at least nine other universities were receiving similar warnings. The campuses are part of an escalating number of extortion and ransomware attacks the FBI has been tracking since March 2020, when the Covid-19 pandemic took hold in the U.S. Cybercriminals have taken advantage of the unique circumstances of the pandemic to double down on their demands.

Read the full article here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Academic Security and Counter Exploitation Program is coordinated by The Texas A&M University System Research Security Office as a service to the academic community.

https://rso.tamus.edu

Academic Security and Counter Exploitation Program | *The Open Source Media Summary* | April 21, 2021 | Page 5 of 5

ASCE
ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM