ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

November 24, 2021

EXCLUSIVE: NO. 2 IN U.S. MILITARY REVEALS NEW DETAILS ABOUT CHINA'S HYPERSONIC WEAPONS TEST

David Martin | CBS News | November 16, 2021

In an exclusive interview with CBS News, General John Hyten, vice chairman of the Joint Chiefs of Staff and the No. 2 person in the U.S. military, revealed new details of last summer's Chinese hypersonic weapons test, which sent a missile around the world at more than five times the speed of sound. "They launched a long-range missile," Hyten told CBS News. "It went around the world, dropped off a hypersonic glide vehicle that glided all the way back to China, that impacted a target in China." Asked if it hit the target, Hyten replied, "Close enough." Unlike intercontinental ballistic missiles which travel in a predictable arc and can be tracked by long range radars, a hypersonic weapon maneuvers much closer to the earth, making it harder for radars to detect. Combined with hundreds of new missile silos China is building, Hyten believes the Chinese could one day have the capability to launch a surprise nuclear attack on the U.S. "They look like a first-use weapon," Hyten said. "That's what those weapons look like to me." For decades, the nuclear balance between the U.S. and Russia has depended on neither side having the capability to launch a successful first strike. If China is now trying to develop a first-strike capability, that balance would be in jeopardy.

Read the full article here.

CHINESE SPY BOSS' CONVICTION MARKS NEW CHAPTER IN WAR ON ESPIONAGE

Shannon Vavra | Daily Beast | November 15, 2021

After a federal jury convicted a Chinese spy boss of espionage earlier this month, counterintelligence officials told The Daily Beast that the case could be a seminal moment for the United States, as it works to combat a problem that has the FBI opening a new counterintelligence case into China every 12 hours. Yanjun Xu, a deputy director of a foreign intelligence branch of China's Ministry of State Security (MSS), became the first Chinese intelligence official to be extradited to the United States for trial and convicted. But, according to Bill Evanina, a former top official in the Office of the Director of National Intelligence, Xu almost certainly won't be the last. "It is a very big deal that we were able to extradite a known [Chinese] intelligence official from Europe," Evanina said. He left his role as chief of the National Counterintelligence and Security Center earlier this year and is now the CEO of The Evanina Group. "This [transcript] is going to be… used for decades as the proof that the Chinese Communist Party uses a whole of government approach to steal our technology."

Read the full article here.

RUSSIAN RANSOMWARE GANGS START COLLABORATING WITH CHINESE HACKERS

Bill Toulas | Bleeping Computer | November 17, 2021

There's some unusual activity brewing on Russian-speaking cybercrime forums, where hackers appear to be reaching out to Chinese counterparts for collaboration. These attempts to enlist Chinese threat actors are mainly seen on the RAMP hacking forum, which is encouraging Mandarin-speaking actors to participate in conversations, share tips, and collaborate on attacks. According to a new report by Flashpoint, high-ranking users and RAMP administrators are now actively attempting to communicate with new forum members in machine-translated Chinese. The forum has reportedly had at least thirty new user registrations that appear to come from China, so this could be the beginning of something notable. The researchers suggest that the most probable cause is that Russian ransomware gangs seek to build alliances with Chinese actors to launch cyber-attacks against U.S. targets, trade vulnerabilities, or even recruit new talent for their Ransomware-as-a-Service (RaaS) operations. A threat analyst told BleepingComputer earlier this month that this initiative was started by a RAMP admin known as Kajit, who claims to have recently spent some time in China and can speak the language.

Read the full article here.

5 MINUTES WITH STEPHANIE JAROS: IDENTIFYING AND ADDRESSING INSIDER THREATS

Layan Dahhan | Security | November 17, 2021

Stephanie Jaros, Director of Research for the U.S. Department of Defense's (DoD) counter-insider threat program, talks to Security about her journey through security and her work with insider threats. She talks about the integration of the human and behavioral sciences into DoD's program, the Threat Lab, as well as the importance of identifying and addressing insider threats — as well as the criticality of the timeline. Security magazine: Could you tell me a bit about your journey into security and what led you to your current position in the field? Jaros: The theme of my career I think is best summarized by, 'I don't know where I'm going, but I always seem to get there.' I had been studying sociology of sex and gender and I attended a career fair during graduate school for government employment. I was really interested in health and policy jobs, but we had all put our resumes into a resume bank so the people who attended the job fair could see them. One day, I got a call from a representative from U.S. Customs and Border Protection [CBP].

Read the full article here.

AS U.S. SPIES LOOK TO THE FUTURE, ONE TARGET STANDS OUT: CHINA

Greg Myre | NPR | November 16, 2021

It's pretty rare for U.S. spies to gather at a conference and talk openly about the most pressing national security threats. "I've got to tell you all, it's so odd after 27 years of being in the clandestine service, to see your picture and your bio pop up," said Cynthia Saddy, a retired CIA officer. As she spoke to a ballroom filled with current and former intelligence officials at a resort in Sea Island, Ga., a huge screen displayed her photo and the high-powered positions she held at the agency, including chief of staff in the Directorate of Operations. One former CIA director, Michael Hayden, joined the Cipher Brief Threat Conference virtually and helped set the tone as he shared the advice he gave to the current CIA director, William Burns. "First of all, you've got to go to China. And then second of all, you've got to go go to China. And the third one is, you've got to go to China. And he said, 'OK, I got it,'" Hayden recounted.

Read the full article here.

FBI: AN APT ABUSED A ZERO-DAY IN FATPIPE VPNS FOR SIX MONTHS

Catalin Cimpanu | The Record | November 17, 2021

The US Federal Bureau of Investigation said it discovered an advanced persistent threat (APT) abusing a zero-day vulnerability in FatPipe networking devices as a way to breach companies and gain access to their internal networks. "As of November 2021, FBI forensic analysis indicated exploitation of a 0-day vulnerability in the FatPipe MPVPN device software going back to at least May 2021," the agency said in a flash security alert sent out on Tuesday. The FBI said the vulnerability allowed the hacking group to exploit a file upload function in the device's firmware and install a webshell with root access. The FBI said it spotted the hackers abusing the zero-day only against FatPipe MPVPN devices, but the vulnerability also impacted other products, such as IPVPN and WARP. All are different types of virtual private network (VPN) servers that companies install at the perimeter of their corporate networks and use to allow employees remote access to internal applications via the internet, acting as mash-up between network gateways and firewalls.

Read the full article here.

PROTECTING CRITICAL AND EMERGING U.S. TECHNOLOGIES FROM FOREIGN THREATS

The National Counterintelligence and Security Center | October 2021

Given the unique opportunities and challenges posed by emerging technologies, the National Counterintelligence and Security Center (NCSC) today announced it is prioritizing its industry outreach efforts in a select few U.S. technology sectors where the stakes are potentially greatest for U.S. economic and national security. These sectors produce technologies that may determine whether America remains the world's leading superpower or is eclipsed by strategic competitors in the next few years. These sectors include, but are not limited to: artificial intelligence, bioeconomy, autonomous systems, quantum, and semiconductors. As mandated by Congress, a core NCSC mission is to conduct counterintelligence (CI) outreach to the U.S. private sector, academic and research communities, as well as other external stakeholders to arm them with information about foreign intelligence threats to their organizations and ways to mitigate risk.

Read the full article here.

IS U.S. COUNTERINTELLIGENCE UP TO THE TASK OF PROTECTING AMERICA'S SECRETS?

James Bruno | Washington Monthly | November 12, 2021

One weekday a decade ago, Chinese security officers entered a government office, pulled one of its employees out into the building's courtyard, and shot him dead, The New York Times reported in 2017, citing three former U.S. officials. The chilling execution, the article said, was meant as a warning to others who might think of betraying their country. Beijing dismissed the report as a "purely fabricated story." The alleged incident was part of a roll-up of the CIA's spy networks in China in which at least 30 CIA assets were executed, according to Foreign Policy. It will take years to rebuild the networks—unless the Chinese security services keep taking them apart. In October, Russian intelligence launched a massive cyberassault on thousands of the U.S. government's IT systems, American businesses, and research institutions, four months after President Joe Biden warned Vladimir Putin to deescalate tensions. The episode comes on the heels of Russia's SolarWinds hacking late last year, which included the computer networks of the Departments of Homeland Security, Defense, State, Commerce, and Treasury.

Read the full article here.

REPORT: 70% OF IT PROS SAY SECURITY HYGIENE HAS GOTTEN HARDER OVER PAST TWO YEARS

Venture Beat | November 19, 2021

A new report from Enterprise Strategy Group (ESG) and JupiterOne warns of inadequate security hygiene and posture management practices at many organizations. The research found that 86% of organizations believe they follow best practices for security hygiene and posture management. However, 70% of organizations said they use more than ten security tools to manage security hygiene and posture management, which raises concerns about data management and operations overhead. In addition, 73% of security professionals admitted that they still depend on spreadsheets to manage security hygiene and posture at their organizations. As a result, 70% of respondents said that security hygiene and posture management had become more difficult over the past two years as their attack surfaces have grown. Overall, the report suggests that security asset management programs are too often informal, disorganized, and immature. It proposes that organizations would benefit from adopting greater integration technologies, advanced analytics, and process automation.

Read the full article here.

AMERICA NEEDS MORE THAN 'GUARDRAILS' WITH CHINA

Michael R. Auslin | The Spectator | November 16, 2021

As recently as a week ago, there was talk that Monday night's virtual summit between President Joe Biden and Chinese Communist Party general secretary Xi Jinping was an opportunity to "reset" the US-China relationship. By the time the two leaders sat down in front of their video screens, the summit had been downgraded to a "meeting" and the White House made clear that little concrete agreement, and no breakthrough, was to be expected. The meeting lived down to expectations, uneasily combining a more sober and realistic US assessment of the parlous state of bilateral ties with what seems a return to a pre-2017 model of surface bonhomie and references to the "the long-term work that we need to do together," according to a senior US official. Despite the assurances that Biden wants meaningful and substantive discussions, from Taiwan to AI to hypersonic missiles, the flashpoints between Beijing and Washington continue to grow with little indication that the conflictual trajectory can be altered.

Read the full article here.

EU SETS CONDITIONS FOR JOINT HIGH-END RESEARCH WITH CHINA

Yojana Sharma | University World News | November 19, 2021

The European Commission in Brussels is currently involved in negotiations with China to draw up a joint roadmap for science and technology cooperation, but with stricter terms of cooperation than in the past. However, European Union officials have said the European Commission is willing to step away from any final agreement on certain aspects of research and innovation if China does not agree to certain principles of openness and reciprocity. Vojko Bratina, science attaché at the EU delegation in Beijing, said the EU is looking to 'rebalance' research relations between Europe and China. "The world is changing and evolving and so also changing the conditions for research and innovation," he told a conference on 'International Higher Education and Global Science: EU-China Relations in a Changing World Order' at Utrecht University in the Netherlands on 4-5 November, referring to the rise of China as well as geopolitical competition. The joint EU-China roadmap currently being negotiated with China's Ministry of Science and Technology and other ministries will establish the conditions to guide future research and innovation cooperation and also identify particular research fields where the EU wants more cooperation with China, he said.

Read the full article here.

TOP LESSON FROM SOLARWINDS ATTACK: RETHINK IDENTITY SECURITY

Kyle Aspach | Venture Beat | November 18, 2021

Among the many lessons from the unprecedented SolarWinds cyberattack, there's one that most companies still haven't quite grasped: Identity infrastructure itself is a prime target for hackers. That's according to Gartner's Peter Firstbrook, who shared his view on the biggest lessons learned about the SolarWinds Orion breach at the research firm's Security & Risk Management Summit — America's virtual conference this week. The SolarWinds attack — which is nearing the one-year anniversary of its disclosure — has served as a wake-up call for the industry due to its scope, sophistication, and method of delivery. The attackers compromised the software supply chain by inserting malicious code into the SolarWinds Orion network monitoring application, which was then distributed as an update to an estimated 18,000 customers. The breach went long undetected.

Read the full article here.

LINKEDIN FAKES: A WOLF IN BUSINESS CASUAL CLOTHING

Hatlesslder Blog | November 23, 2021

Nobody wants to believe they'll fall for a scam. Especially not any of you, my intelligent, savvy, and OPSEC-conscious friends! Your radar is always on and carefully protecting your personal information, so you'd never click the link in that fortune-promising email, you'd never open an unexpected file attachment, and you'd certainly never send some stranger a document with your personal details on it, that's inconceivable!! Or is it? What if there was a site where doing those types of things wouldn't actually seem all that out of the ordinary? One where interacting with strangers and sharing personal information about yourself could lead to long-term gainful employment? What if the profile on the other end of that message looks polished, with a long work history of instantly recognizable company logos, a top-tier college, and a mountain of mutual connections and groups? One with a real, human, smiling face that syncs up perfectly with the nice, tidy appearance of the rest of the profile.

Read the full article here.

NSA DIRECTOR: EVOLVING CYBER THREATS REQUIRE DEEPER PUBLIC-PRIVATE PARTNERSHIPS

Brandi Vincent | Nextgov | November 17, 2021

The government has long leaned on partnerships with companies and academia to advance technology, but according to one top cybersecurity leader, the complexities of the modern conflict landscape warrant cross-sector collaboration that goes deeper than any before. "I do think that there is a realization that we can't do this alone," Gen. Paul Nakasone said Tuesday night at an Intelligence and National Security Alliance-hosted dinner in Virginia. "So, this partnership has to exist—and it's got to get even more powerful." Nakasone, the commander of U.S. Cyber Command and director of the National Security Agency, outlined areas of investment his team is pursuing in the face of new strategic challenges. They include talent, technology and partnerships. He also shed light on a new partnership NSA is embarking on with the National Cryptologic Foundation to advance future-facing research and build pipelines for cybersecurity jobs. "Let me talk a little bit about the strategic environment we see today. It does begin with China—that presents our greatest political challenge of our time," Nakasone explained. "This is not Cold War 2.0 and China is not the Soviet Union."

Read the full article here.

INTERNATIONAL STUDENT ENROLMENT FELL BY 15% LAST YEAR

Mary Beth Marklein | University World News | November 18, 2021

International student enrolment in universities in the United States fell by 15% last year, a not-unexpected decline that was attributed primarily to the COVID-19 pandemic, according to a report released this week. A companion survey suggests a rebound may already be in the making. Enrolments in the 2020-21 academic year topped out at 914,095, erasing five years above the one million mark, said the report, released on Monday by the Institute of International Education (IIE), a non-profit organisation that tracks annual enrolment trends for the US State Department. More than 710,000 students were enrolled as undergraduate, graduate and non-degree students.

Read the full article here.

DHS CHIEF INFORMATION SECURITY OFFICER WARY OF PENTAGON'S CHANGES TO CMMC

Justin Doubleday | Federal News Network | November 16, 2021

The Department of Homeland Security is testing out its own way of evaluating contractor cybersecurity measures, amid concerns about the efficacy of the Defense Department's Cybersecurity Maturity Model Certification program. DHS launched a pathfinder this summer to begin evaluating existing contractors with cyber hygiene clauses in their contracts, according to Ken Bible, chief information security officer at DHS. He said DHS has had those clauses in place since 2015, but has never held companies accountable for meeting the standards. He said DHS has assessed one contractor so far on whether it is meeting the cybersecurity standards. "We're going to continue to expand upon that Pathfinder," Bible said during a conference today hosted by SC Media. "I don't know that we found from that one Pathfinder everything that we needed to really build out our DHS program in that area."

Read the full article here.

FCC KICKS CHINA TELECOM AMERICAS OUT OF US, CITES CHINESE GOVERNMENT CONTROL

Jon Brodkin | ARS Technica | October 26, 2021

The Federal Communications Commission today voted to block China Telecom Americas from the US market, saying that the "US subsidiary of a Chinese state-owned enterprise" is "subject to exploitation, influence, and control by the Chinese government." The telco "is highly likely to be forced to comply with Chinese government requests without sufficient legal procedures subject to independent judicial oversight," the FCC said. The vote was 4-0 with both Democrats and both Republicans approving the order to revoke and terminate China Telecom's Section 214 authority to operate in the US. The FCC said its order "directs China Telecom Americas to discontinue any domestic or international services that it provides pursuant to its Section 214 authority within sixty days following the release of the order."

Read the full article here.