ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

April 5, 2023

HACKERS PROBING CONTRACTORS FOR PATH TO PENTAGON, DISA CHIEF SAYS

Colin Demarest | C4ISRNET | March 30, 2023

Foreign hackers are targeting contractors to the U.S. government not only for their intellectual property and non-public information, but also to find furtive avenues into Pentagon networks, according to the director of the Defense Information Systems Agency. Lt. Gen. Robert Skinner on March 29 told Congress that hackers backed by China, Russia and other adversaries are applying "very high" levels of effort to digitally infiltrate, surveil and make off with plans or intelligence closely held by suppliers to the Department of Defense. Also on their radar are means of going "upstream," he said at a Senate Armed Services subcommittee hearing. "Some of them see the defense industrial base as a soft underbelly," said Skinner, who also serves as the commander of the Joint Force Headquarters-Department of Defense Information Network. "That's why our work with [Cybersecurity Maturity Model Certification] 2.0 and our work day-to-day with our defense industrial base partners is critical moving forward, because that's where the adversary is really targeting." CMMC 2.0 is a framework launched in 2021 to protect the defense industrial base's sensitive unclassified information from frequent and increasingly complex cyberattacks.

Read the full article here.

AI IS GETTING POWERFUL. BUT CAN RESEARCHERS MAKE IT PRINCIPLED?

Mordechai Rorvig | Scientific American | April 4, 2023

Soon after Alan Turing initiated the study of computer science in 1936, he began wondering if humanity could one day build machines with intelligence comparable to that of humans. Artificial intelligence, the modern field concerned with this question, has come a long way since then. But truly intelligent machines that can independently accomplish many different tasks have yet to be invented. And though science fiction has long imagined AI one day taking malevolent forms such as amoral androids or murderous Terminators, today's AI researchers are often more worried about the everyday AI algorithms that already are enmeshed with our lives—and the problems that have already become associated with them. Even though today's AI is only capable of automating certain specific tasks, it is already raising significant concerns. In the past decade, engineers, scholars, whistleblowers and journalists have repeatedly documented cases in which AI systems, composed of software and algorithms, have caused or contributed to serious harms to humans.

Read the full article here.

PUBLIC-PRIVATE PARTNERSHIPS ARE ESSENTIAL TO STRENGTHEN CYBERSECURITY GLOBALLY

Derek Manky | CSO | March 27, 2023

Cyberattacks are on the rise, and so are the chances that your organization will fall victim to a breach. More than 84% of organizations experienced at least one cyberattack last year. While many widely recognized attack vectors like phishing emails are here to stay, we're observing enterprising cybercriminals evolving their methods and relying on increasingly sophisticated and complex attack tactics to infiltrate networks. From introducing threats with APT-like attributes to reimagining existing botnets and code, they're making what's old new again and enhancing their tactics. As bad actors take a "work smarter, not harder" approach, they can do more with less, which is concerning. At the same time, organizations are also wrestling with another challenge: An abundance of unfilled positions because of the cybersecurity talent shortage. A recent study shows that 3.4 million additional cybersecurity practitioners are needed to fill open roles. And nearly 70% of security leaders say their organizations face additional risks because of the ongoing skills shortage.

Read the full article here.

CHINA HAS BEEN WAGING A DECADES-LONG, ALL-OUT SPY WAR

Calder Walton | Foreign Policy | March 28, 2023

One week ago, TikTok CEO Shou Zi Chew was questioned by members of the U.S. Congress, before the world's media, about whether the Chinese government uses the wildly popular video-sharing app to spy on Americans. His testimony came several weeks after the appearance of a Chinese spy balloon floating across the United States. What are we to make of these two stories, which are at their core both about Chinese espionage? To borrow a phrase from Mission: Impossible: Relax, it's much worse than you think. We are now witnessing some of the effects of a decision made years ago by China to use every means and medium of intelligence-gathering at its disposal against the West. Its strategy can be summarized in three words: collect, collect, collect. Most Westerners do not yet appreciate just how sweeping China's intelligence onslaught directed at their countries is; for decades, their own governments likewise didn't understand because their attention was largely directed elsewhere.

Read the full article here.

IN SUDDEN ALARM, TECH DOYENS CALL FOR A PAUSE ON CHATGPT

Will Knight and Paresh Dave | Wired | March 29, 2023

An open letter signed by hundreds of prominent artificial intelligence experts, tech entrepreneurs, and scientists calls for a pause on the development and testing of AI technologies more powerful than OpenAI's language model GPT-4 so that the risks it may pose can be properly studied. It warns that language models like GPT-4 can already compete with humans at a growing range of tasks and could be used to automate jobs and spread misinformation. The letter also raises the distant prospect of AI systems that could replace humans and remake civilization. "We call on all AI labs to immediately pause for at least 6 months the training of AI systems more powerful than GPT-4 (including the currently-being-trained GPT-5)," states the letter, whose signatories include Yoshua Bengio, a professor at the University of Montreal considered a pioneer of modern AI, historian Yuval Noah Harari, Skype cofounder Jaan Tallinn, and Twitter CEO Elon Musk. The letter, which was written by the Future of Life Institute, an organization focused on technological risks to humanity, adds that the pause should be "public and verifiable," and should involve all those working on advanced AI models like GPT-4.

Read the full article here.

RUSSIA ARRESTS US JOURNALIST EVAN GERSHKOVICH ON SPYING CHARGE

Paul Kirby | BBC News | March 30, 2023

US journalist Evan Gershkovich has been arrested in Russia and accused of spying while working for the Wall Street Journal. An experienced Russia reporter, he was working in the city of Yekaterinburg at the time of his detention. The White House has condemned his detention "in the strongest terms". The Kremlin claimed he had been caught "red-handed" but the Wall Street Journal vehemently denied the allegations against him. Mr Gershkovich, 31, is well known among foreign correspondents in Moscow and BBC Russia Editor Steve Rosenberg describes him as an excellent reporter and a highly principled journalist. US Secretary of State Antony Blinken echoed the Wall Street Journal in saying he was "deeply concerned" by the arrest. US officials said they had immediately sought access to Mr Gershkovich but had not had any response. The WSJ said its reporter had dropped out of contact with his editors while working in Yekaterinburg, about 1,600km (1,000 miles) east of Moscow, on Wednesday afternoon. US officials said Mr Gershkovich's driver had dropped him off at a restaurant and two hours later his phone had been turned off.

Read the full article here.

THE CALL TO HALT 'DANGEROUS' AI RESEARCH IGNORES A SIMPLE TRUTH

Sasha Luccioni | Wired | April 4, 2023

Last week, the Future of Life Institute published an open letter proposing a six-month moratorium on the "dangerous" AI race. It has since been signed by over 3,000 people, including some influential members of the AI community. But while it is good that the risks of AI systems are gathering visibility within the community and across society, both the issues described and the actions proposed in the letter are unrealistic and unnecessary. The call for a pause on AI work is not only vague, but also unfeasible. While the training of large language models by for-profit companies gets most of the attention, it is far from the only type of AI work taking place. In fact, AI research and practice are happening in companies, in academia, and in Kaggle competitions all over the world on a multitude of topics ranging from efficiency to safety.

Read the full article here.

CHATGPT FOR BUSINESS: FACT VS. FICTION, WHAT YOU NEED TO KNOW

David Rand | The Future of Commerce | March 27, 2023

You've undoubtedly heard about OpenAI's ChatGPT, a powerful chatbot built on natural language processing and artificial intelligence technologies. In its first two months of release, the free tool attracted more than 100 million monthly active users, making it the fastest-growing consumer application of all time, according to UBS. By comparison, it took TikTok nine months and Instagram 2-1/2 years to reach that milestone. According to ChatGPT, "ChatGPT is an AI language model developed by OpenAI, which is capable of generating human-like text based on the input it is given. The model is trained on a large corpus of text data and can generate responses to questions, summarize long texts, write stories and much more. It is often used in conversational AI applications to simulate a human-like conversation with users." Breaking that down, ChatGPT is a natural-language AI processing tool that allows for engagement with a chatbot, much like you'd converse with a human.

Read the full article here.

ADVERSARIAL MACHINE LEARNING AND CYBERSECURITY

Micah Musser, Andrew Lohn, James X. Dempsey, Jonathan Spring, Ram Shankar Siva Kumar, Brenda Leong, Christina Liaghati, Cindy Martinez, Crystal D. Grant, Daniel Rohrer, Heather Frase, John Bansemer, Jonathan Elliott, Mikel Rodriguez, Mitt Regan, Rumman Chowdhury, and Stefan Hermanek | Center for Security and Emerging Technology | April 2023

Artificial intelligence systems are rapidly being deployed in all sectors of the economy, yet significant research has demonstrated that these systems can be vulnerable to a wide array of attacks. How different are these problems from more common cybersecurity vulnerabilities? What legal ambiguities do they create, and how can organizations ameliorate them? This report, produced in collaboration with the Program on Geopolitics, Technology, and Governance at the Stanford Cyber Policy Center, presents the recommendations of a July 2022 workshop of experts to help answer these questions. In July 2022, the Center for Security and Emerging Technology (CSET) at Georgetown University and the Program on Geopolitics, Technology, and Governance at the Stanford Cyber Policy Center convened a workshop of experts to examine the relationship between vulnerabilities in artificial intelligence systems and more traditional types of software vulnerabilities.

Read the full article here.

SPEECH BY PRESIDENT VON DER LEYEN ON EU-CHINA RELATIONS TO THE MERCATOR INSTITUTE FOR CHINA STUDIES AND THE EUROPEAN POLICY CENTRE

European Commission | March 30, 2023

Ladies and Gentlemen, it is a real pleasure to be here at this very special event co-hosted by two of Europe's most knowledgeable and independent-minded think tanks. In a time when global affairs are becoming harder to decrypt – and in an era where facts are routinely challenged – the work that you do at these think tanks has never been more important for Europe. Because it is only by having a deeper understanding of the world as it really is – not as we may wish it to be – that we can develop better informed policies. This is why I believe think tanks are an essential part of our democracy. In just ten years, MERICS has developed a unique expertise in analysing the political, economic and social trends in China and how these impact Europe and the world. And we must preserve and uphold your right – and that of all think tanks –– to be analytical and to be critical.

Read the full article here.

CHINA'S FAKE SCIENCE INDUSTRY: HOW 'PAPER MILLS' THREATEN PROGRESS

Financial Times | Communications of the ACM | March 29, 2023

Chinese researchers have become some of the world's most prolific publishers of scientific papers. But experts say that China's impressive output masks systemic inefficiencies and an underbelly of low-quality and fraudulent research. The world's scientific publishers are becoming increasingly alarmed by the scale of fraud. An investigation last year concluded: "The submission of suspected fake research papers . . . is growing and threatens to overwhelm the editorial processes of a significant number of journals." Bernhard Sabel at Otto-von-Guericke University of Magdeburg is one of many journal editors calling for "swift global action to restore the health of the scientific record and to prevent the erosion of trust in science." Estimates of the extent of fake scientific output vary from 2 percent to 20 percent or more of published papers.

Read the full article here.

RUSSIAN SPY POSED AS A BRAZILIAN STUDENT TO GET INTO ELITE JOHN HOPKINS INTERNATIONAL RELATIONS MASTER'S PROGRAM TO POSITION HIM CLOSE TO THE AMERICAN SECURITY ESTABLISHMENT, COURT PAPERS SAY

Hope Sloop | Daily Mail | March 30, 2023

A Russian spy posed as a Brazilian student in order to enter the U.S. and attend Johns Hopkins University's international relations graduate program, according to a federal indictment. GRU operative Sergey Vladimirovich Cherkasov, 37, masqueraded as a South American student named Victor Ferreira and even applied for a job at the International Criminal Court, in order to position himself inside the American security establishment. The Justice Department claims Cherkasov entered the U.S. in 2018 in hopes of gathering intel on Americans and made connections with a State Department employee, a Capitol Hill worker, and other security officials. Cherkasov allegedly created the 'Ferreira' alias while in Brazil where he pretended to be the son of a deceased Brazilian national. In 2022, the Russian spy tried to access the International Criminal Court in the Hague, reportedly to obtain information on the investigation into Russia's invasion of Ukraine. After Cherkasov got into Johns Hopkins' prestigious international relations program in 2018, he sent an email to several people who had helped him gain entry. 'Today we made the future — we managed to get in one of the top schools in the world,' he wrote in the email that was cited in federal court Friday by the DOJ.

Read the full article here.