THE CIPHER BRIEF

National Security is Everyone's Business
JULY 31, 2023 | 10:46 AM ET
RUSSIA › UKRAINE › TECH/CYBER ›

The way AI 'learns' poses risks so large, it almost supplants threats from China

JUNE 29TH, 2023 BY DAVID ARIOSTO | 0 COMMENTS

CIPHER BRIEF REPORTING — The Intelligence Community's 2023 Annual Threat Assessment released in March emphasized the Chinese Communist Party in what intelligence leaders later described as the "most consequential threat" to U.S. national security, particularly with regard to Beijing's aggressive pursuits in cyber and quantum technologies. But just a few months later, with a growing array of threats tied to artificial intelligence – that do not always originate from Beijing – some former U.S. leaders, now working in the private sector, see the aperture of threats posed by AI as widening.

"Yes, China is top of mind," said Chris Krebs, former U.S. Director of the Cybersecurity and Infrastructure Security Agency, speaking at the Cyber Initiatives Group Summit on Wednesday. "But it's almost being supplanted by AI risk."

"Just about every organization, either intentionally or unintentionally, [are] integrating AI workflows, processes, [and] business operations," he said, pointing specifically to software tools, such as AI-powered chatbots like *ChatGPT* and *Google Bard*.

The concern, however, is over how that data is being employed.

Trained on large language models (LLMs) that utilize neural networks – a collection of interconnected units or nodes – companies are now racing to embed those tools to help clients with everything from booking hotels to synthesizing meeting notes. But as security experts noted during Wednesday's summit, the nature of that symbiotic relationship between the user and the tech can pose increasing risks the more the two interact. Given how LLMs make use of increasing data to enhance those networks and improve search results, even seemingly innocuous queries can correlate with heightened risk.

"There are front-line workers … that are going out and using *ChatGPT* to help them be more efficient," noted Krebs. "But the unfortunate thing is that we're seeing a lot proprietary, sensitive, or otherwise confidential information getting plugged into public LLMs. And that's going to be a real long-term problem for some of these organizations."

The Cipher Brief hosts expert-level briefings on national security issues for Subscriber+Members that help provide context around today's national security issues and what they mean for business. Upgrade your status to Subscriber+ today.

In a recent report published by *Cyberhaven*, a California-based cybersecurity company, the authors determined that more than one in 10 employees evaluated had used *ChatGPT* in the workplace, while nearly 9% had pasted their company data into chat bots.

In one such case, an executive entered the company's 2023 strategy document, and then asked the chat bot to rewrite the information as a *PowerPoint* deck. In another, a doctor inputted a patient's name and medical information, using it to craft a letter to the patient's insurance company. An unauthorized third party, *Cyberhaven* explained, might then be able to ascertain that sensitive company strategy, or privileged medical history, simply by asking the chat bot.

In the broader scope, U.S. adversaries and criminal entities could also potentially use the tech to drum up information about critical infrastructure, for instance, that might improve the efficacy of a coming cyber strike.

"I don't even think we've really wrapped our arms around what a data breach from those sorts of interactions [could mean]," said Krebs.

Looking for a way to get ahead of the week in cyber and tech? Sign up for the Cyber Initiatives Group Sunday newsletter to quickly get up to speed on the biggest cyber and tech headlines and be ready for the week ahead. Sign up today.

Meanwhile, anecdotal reports of the phenomenon seem to be gaining momentum. So much so, that companies are issuing guidelines meant to prevent the mishandling of confidential information that can occur simply by using AI tools.

"The challenge is from a guard-rails perspective,"added Krebs. "There aren't a lot of options right now."

OpenAI retains data unless users select to 'opt-out'. But several major companies, including *J.P. Morgan Chase* and *Verizon*, have already blocked access to the technology, while others, such as Amazon, have issued warnings to employees, prohibiting them from inputting company data.

Meanwhile, the use of AI-powered searches have seen explosive growth.

ChatGPT, created by the research and deployment company *OpenAI*, is estimated to have reached more than 100 million monthly active users shortly after its launch, with more than 300 applications now using the tech, along with "tens of thousands of developers around the globe," the company said.

"We currently generate an average of 4.5 billion words per day, and continue to scale production traffic."

In the public sector, where chatbots have long been employed, especially across state and local governments as a public interface for questions about everything from health care claims to rental assistance to Covid-19 relief funds, cities like Los Angeles are seeking to further embrace AI-powered technology to improve bureaucratic functions, such as paying parking tickets and facilitating voter registration.

Officials often laud AI's potential as a means of efficiency, as does the tech itself.

In fact, when asked directly, "how might *ChatGPT* change how people interact with government?" it responded with a list: 1.) greater ease of communications, 2.) breaking-down language barriers, 3.) resolving issues without lengthy wait-times, 4.) automating routine functions, 5.) creating personalized guidance, and 6.) self-improving. But the chatbot also noted looming transparency, accuracy, and hacking vulnerabilities as potential pitfalls with its broader integration.

"When we make these LLMs available to a large number of people, the data can be manipulated," noted Paul Lekas, Senior Vice President for Global Public Policy and Government Affairs at the Software and Information Industry Association. "The algorithm on top of the data can be adjusted to achieve certain means. And there's been an extensive amount of research over the past couple years, showing that LLMs can essentially propagate misinformation and common mistakes, and make it much easier to generate misinformation."

"I'm concerned about the landscape," he added during Wednesday's Cyber Initiatives Group Summit.

Others at the conference also chimed in with broader concerns.

"I might even be a little farther along the continuum than you," said Glenn Gerstell, former National Security Agency General Counsel and moderator of the session on cyber-propelled disinformation during which Lekas spoke. "I feel that the combination of the technical development … combined with the geopolitical and social situation means we're in for potentially a period of very, very destabilizing set of factors that could affect democracy."

Updated 6/29

Read more expert-driven national security insights, perspectives and analysis in The Cipher Brief because National Security is Everyone's Business

CATEGORIZED AS: ARTIFICIAL INTELLIGENCE CYBER CYBER INITIATIVES GROUP TECH/CYBER

TAGGED WITH: CHINA CYBERSECURITY INTELLIGENCE PRIVATE SECTOR

Leave a Reply

Logged in as David Ariosto. Log out »

SUBMIT COMMENT

Related Articles

EXCLUSIVE: Manila's Envoy to Beijing Weighs-In On Recent US-China Tensions

EXCLUSIVE SUBSCRIBER+ INTERVIEW — An old friend of Beijing returned to China this week in a move that harkens back to a time when Manila [...] More ›

CHINA PHILIPPINES UNITED STATES

JULY 20TH, 2023

Western Focus Sharpens on China Over Black Sea Grain Deal

EXCLUSIVE SUBSCRIBER+ INTERVIEW — In the wake of a Kremlin decision to halt a U.N.-brokered Black Sea agreement, which allowed Ukraine to export tens of millions [...] More ›

CHINA RUSSIA UKRAINE

JULY 17TH, 2023

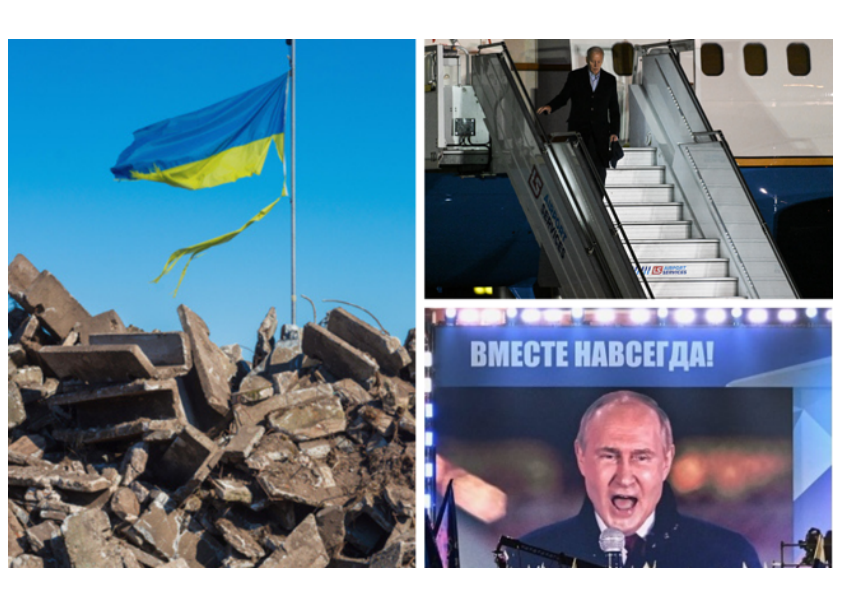
When It Comes to US-China Talks, Something "Vital" Is Still Missing

CIPHER BRIEF REPORTING — A rare series of diplomatic overtures in Beijing were absent at least one "absolutely vital" ingredient, U.S. Secretary of State Antony [...] More ›

CHINA CYBER CYBER INITIATIVES GROUP

JUNE 19TH, 2023 BY DAVID ARIOSTO

Featured Piece



Warning Signs of a More Dangerous Global Conflict

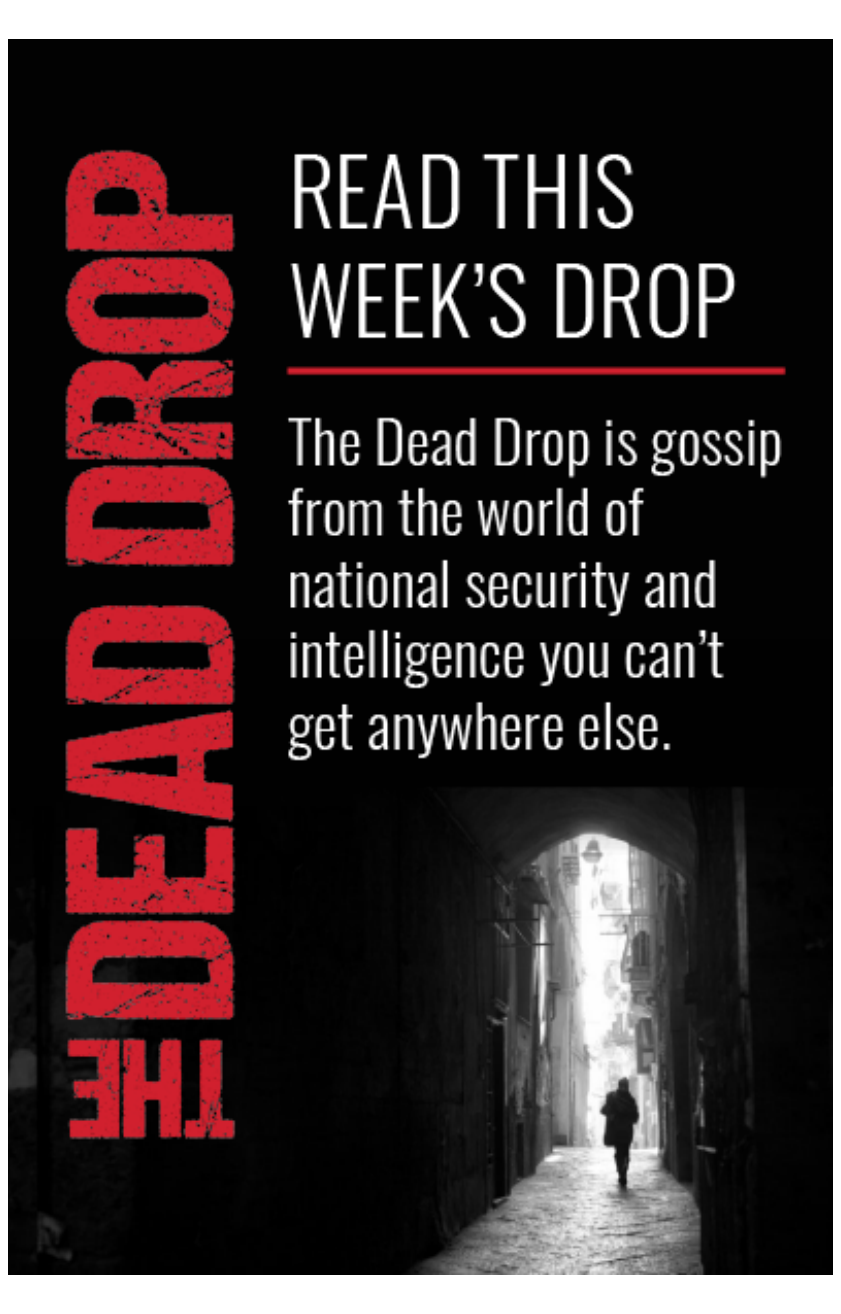
BOTTOM LINE UP FRONT — If President Joe Biden's recent remarks in Poland and President Vladimir Putin's in Moscow just a day later are any indication of the path forward, the February 24 anniversary of the Russian invasion of Ukraine may represent the beginning of a new and potentially much more dangerous phase of the conflict, which is increasingly looking like a conflict between NATO and the Russian Federation.

FEB 22, 2023, BY ROB DANNENBERG

About the Cipher Brief

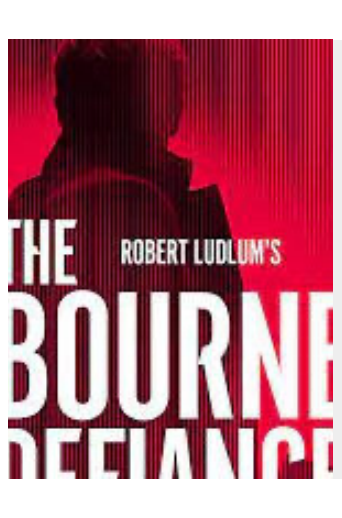
National security is everyone's business. The Cipher Brief is committed to publishing trusted, non-partisan information that brings together the expertise of the public and private sectors.

READ MORE



Book Reviews

View all ›



Defiance: The Latest in The Bourne Series

BOOK REVIEW: Robert Ludlum's The Bourne Defiance By Brian Freeman / G.P. Putnam's Sons Reviewed by Elizabeth C. MacKenzie Biedell The Reviewer: Elizabeth MacKenzie Biedell [...] More ›

JULY 25TH, 2023 BY THE BOURNE DEFIANCE

What the Experts Say

> The Cipher Brief's Open Source Report is an extraordinary product and an important daily read for situational awareness on national security issues.

General John R. Allen (Ret.)
Former Commander of the NATO International Security Assistance Force in Afghanistan

The Cipher Daily Brief

Sign up for the Free Newsletter

Get a daily rundown of the top security stories delivered to your inbox Monday through Friday with exclusive briefs and columns on what matters most to you and your organization.

SIGN UP

For general inquiries please email
info@thecipherbrief.com