The Race to Write the World's First AI Rule Book

MAY 5TH, 2023 | BY DAVID ARIOSTO | 0 COMMENTS

CIPHER BRIEF REPORTING — Designed to drum up the world's first AI rulebook, the European Union's proposed Artificial Intelligence Act is a far-reaching legal framework aimed at strengthening Artificial Intelligence (AI) governance across a wide range of sectors, which has rivals watching as they consider their own versions.

Being first to write rules governing AI experts say, will likely afford competitive advantages – particularly in the security space – and will help devise global standards and align markets along common rules and priorities.

When confronted with the speed of AI innovation along with China competition, "there is no time to waste," Executive Vice President of the European Commission Margrethe Vestager said this week, ahead of a critical vote in the French city of Strasbourg, the official seat of the European Parliament.

"What I think is important is speed," Vestager added.

But the commission, which first unveiled regulatory proposals in 2021, has been slow to adopt such measures, thought to be critical in cementing the ethics, safety and reliability standards, as well as basic transparency of emergent AI systems.

Europe is focusing on more tailored legislation, based on "purposeful manipulation," "emotion recognition," and "predictive policing," while the U.S. approach focuses more on "highly distributed across federal agencies," with "many adapting to AI without new legal authorities," according to a recent Brookings Institution report.

"It's not going to be one size fits all," Lt. Gen Michael Groen, former Director of the U.S. Joint Artificial Intelligence Center, told The Cipher Brief regarding the U.S. approach. "It's not all going to be a strict regulatory agency model. There are some great opportunities here for industry and government to get together [and] set standards that are good for both."

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.

While officials say they hope the two systems remain interoperable, the "light touch" method, emblematic of the U.S. tact, presents a marked difference.

"The light touch is possible, but no lighter than what's needed," said Brian Scott, Deputy Assistant National Cyber Director for Cyber Policy and Programs, at a conference in San Francisco. "So that's a key piece. As we develop these regulations, we should be looking at ... risk-informed, performance-based, outcome-focused, and really ... in consultation with those that are regulated."

Be it legislatively-focused or agency directed, the adoption of a rules-based framework is thought to be a critical next phase of the technology that Bill Gates predicts will ultimately be more influential than the personal computer.

And Beijing, which articulated its early AI regulation efforts back in 2017, is taking note. In a bid to take an early lead as an AI global leader, the Chinese Communist Party set forth a plan, pegged to 2030, to develop China as "a principal world center for artificial intelligence innovation," which would launch it to "the forefront of innovative countries and an economic power." Since then, the AI sector in China has rapidly expanded into a multi-billion dollar industry, producing an estimated one-third of all AI journal papers and citations from 2021.

It's not just for the President anymore. Are you getting your daily national security briefing? Subscriber+Members have exclusive access to the Open Source Collection Daily Brief, keeping you up to date on global events impacting national security. It pays to be a Subscriber+Member.

Meanwhile, Chinese efforts to catch up on more recent AI-powered technologies, such as OpenAI's ChatGPT – the popular artificial intelligence chatbot that boasts more than 100 active million users – have been gaining steam. In April, Alibaba Cloud – a subsidiary of the Chinese multinational technology company Alibaba Group, announced the roll-out of its own AI-powered chatbot, Tongyi Qianwen, while the Beijing-headquartered Baidu offered up a similar rival. Simultaneously, Chinese telecommunications manufacturer Huawei and others, are thought to be pressing state-of-the-art AI products with fewer or less capable semiconductors; a move designed to end-run U.S. sanctions on the materials and machines needed for advanced AI development.

As China looks to answer questions surrounding supply chains and innovation, regulation – it would seem – is a logical next step. This week, Chinese authorities are set close a second round of AI regulation following last month's release of draft rules designed to oversee generative AI technologies. But devising universal standards is a complex feat, involving the inclusion of privacy and accountability concerns, as well as aspects of social media governance, management of cellular networks, and other technologies.

Last month, the Biden administration said it was seeking public comments on AI accountability procedures in the U.S., following calls from ethics groups, including the Center for Artificial Intelligence and Digital Policy, which petitioned the U.S. Federal Trade Commission to stop OpenAI from the continued commercial release of GPT-4, claiming it was "biased, deceptive, and a risk to privacy and public safety."

"Responsible AI systems could bring enormous benefits, but only if we address their potential consequences and harms," said NTIA Administrator Alan Davidson in a statement. "For these systems to reach their full potential, companies and consumers need to be able to trust them."

It pays to be a Subscriber+Member with exclusive access to virtual briefings with leading experts and top officials in the national security and intelligence space.

Overall, however, a growing realization among security experts suggests that "there is no putting this genie back in the bottle," according to Susan M. Gordon, former Principal Deputy Director of National Intelligence.

"Ideas about slowing it, stopping it, impeding it, that just isn't going to happen."

And yet, she added, worries that "the free world is going to end because of this technology" should also be put aside, given America's track record of finding a way to manage. "With respect to AI, it's a great time to have a discussion from a national security perspective... with those who are "developing [this technology] at an incredible rate of speed."

Cipher Brief Cyber Editor Ken Hughes contributed to this report.

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

Updated 5/9 9:00am

CATEGORIZED AS: ARTIFICIAL INTELLIGENCE   CHINA   EUROPE

Leave a Reply

Logged in as David Ariosto. Log out »

SUBMIT COMMENT

Related Articles

The way AI 'learns' poses risks so large, it might supplant threats from China

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 [...] More ›

ARTIFICIAL INTELLIGENCE   CYBER   CYBER INITIATIVES GROUP   TECH/CYBER

JUNE 29TH, 2023, BY DAVID ARIOSTO

The Great Tech Race of our Time

SUBSCRIBER+MEMBER EXCLUSIVE – The battle for semiconductors, a core ingredient of both basic and advanced technologies – such as Artificial Intelligence (AI) – has long [...] More ›

ARTIFICIAL INTELLIGENCE   BUSINESS   NATIONAL SECURITY
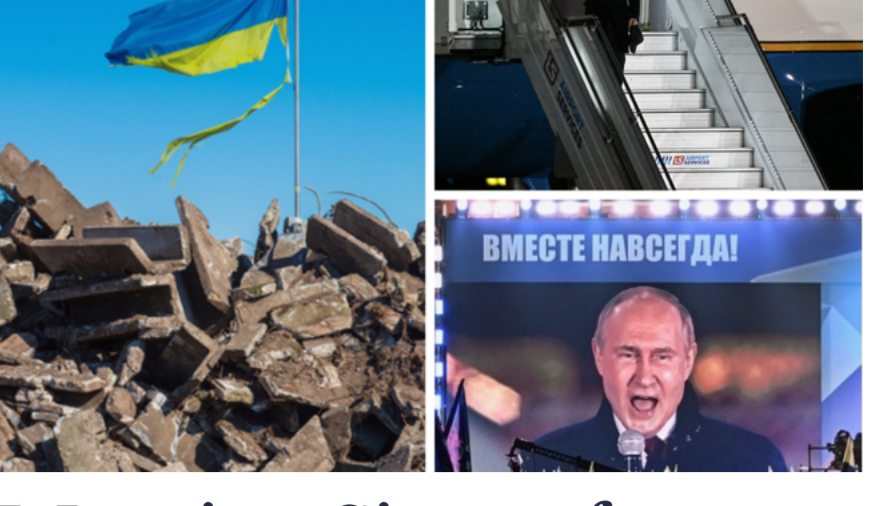
APRIL 28TH, 2023, BY THE CIPHER BRIEF

The Drone Series: What's Over the Horizon?

EXPERT PERSPECTIVE – Russian authorities say they shot down a Ukrainian drone over the area that serves as headquarters for the Russian Black Sea Fleet [...] More ›

CHINA   BRYAN CLARK   DRONES   TECH/CYBER

AUGUST 22ND, 2022, BY THE CIPHER BRIEF

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 what 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 [...]

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

---

HOMEPAGE
ABOUT US
ADVERTISE
CAREERS
CONTACT
GET OUR NEWSLETTER

COLUMNS
THE DEAD DROP
PODCASTS

THE CIPHER BRIEF

For general inquiries please email info@thecipherbrief.com

© 2023 Copyright | The Cipher Brief All rights reserved.   Privacy Policy   Terms of Service & Pricing Policy   Glass Mountains / Powered by