RSIS COMMENTARY

28 July 2025

ChatBIT and the Militarisation of Open-Source AI: Security Implications for Asia

Annemarie Mugisa Acen

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS | S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg

No. 164 – 28 July 2025

RSIS Commentary is a platform to provide timely and, where appropriate, policy-relevant commentary and analysis of topical and contemporary issues. The authors' views are their own and do not represent the official position of the S. Rajaratnam School of International Studies (RSIS), NTU. These commentaries may be reproduced with prior permission from RSIS and due credit to the author(s) and RSIS. Please email to Editor RSIS Commentary at RSISPublications@ntu.edu.sg.

ChatBIT and the Militarisation of Open-Source AI: Security Implications for Asia

By Annemarie Mugisa Acen

SYNOPSIS

The rapid advancement of open-source AI has outpaced regulatory oversight, raising critical concerns about its potential exploitation for military applications. There is a lack of attention within global AI governance platforms on regulating the use of open-source AI in military applications and the risks to security and stability, especially in Asia.

COMMENTARY

In June 2024, a team of Chinese researchers affiliated with the People's Liberation Army unveiled ChatBIT, an AI model developed specifically for military applications. Built on Meta's open-source Llama-2-13b large language model, ChatBIT is designed to support military operations, including battlefield intelligence, situational awareness, and operational decision-making.

This development raises concerns about the lack of regulatory measures regarding the use of open-source AI for military purposes. While the United States expressed concern over ChatBIT, it has not received enough scrutiny in ongoing global AI governance discussions. Given ChatBIT's potential impact on global and regional security, countries need to pay closer attention to the possible use of open-source AI for military applications.

Open-Source AI vs. Closed-Source AI

Unlike closed-source AI models such as OpenAI's GPT-4 or Google's Gemini, which operate under strict access controls, open-source models can be freely modified and their source codes used to create AI chatbots and models. While this openness fosters innovation, it also poses a significant security risk. Meta's Llama-3 Acceptable Use Policy prohibits military applications, but enforcement remains a challenge. Once released, these models can be modified for use beyond their original purpose, including in the military domain.

China is not alone in leveraging open-source AI for strategic advantage; the US Department of Defense has also explored similar applications through partnerships with American tech companies. This poses a challenge to existing governance mechanisms that aim to regulate these technologies and oversee their effective implementation.

While many Western companies and governments claim to be guided by ethical principles, there have been cases where these principles appear to have been ignored. In November 2024, Meta adjusted its policy to allow US government agencies and defence contractors to use Llama models for cybersecurity and intelligence purposes. This underscores the difficulty of holding the private sector accountable for the governance of AI in the military domain.

Regional Military AI Governance Efforts

Many Asian countries are still in the early stages of integrating AI into their defence systems. Instead of responding directly to developments like ChatBIT, several countries remain focused on foundational steps, such as updating defence strategies, investing in dual-use technologies, and experimenting with AI applications in controlled environments. For example, Japan's Defence Ministry launched its first basic policy on the use of AI in July 2024, while South Korea launched a research centre on defence AI earlier in the same year. These efforts are part of broader military modernisation and transformation efforts and do not focus on open-source AI governance per se.

In Southeast Asia, there has been comparatively less attention on the governance of military AI. Until recently, discussions about AI within ASEAN largely focused on civilian capabilities. It was only in early 2025 that the ASEAN Defence Ministers' Meeting (ADMM) made its first joint statement on military AI, highlighting the topic's newness in the region. There remains no regional white paper or coordinated policy framework specifically tackling the risks of open-source AI in military operations.c

This muted response may be due partly to capacity limitations, differing threat perceptions, and political sensitivities surrounding military innovation. However, some countries in the region have reacted cautiously to ChatBIT's emergence, with security analysts warning about the potential for asymmetric military capabilities and exploitation by non-state actors. Still, these concerns have not yet resulted in significant policy responses.

These circumstances highlight the importance for Southeast Asia to accelerate regional dialogue and cooperation on military AI governance, particularly regarding open-source tools, which, due to their accessibility, increase the risk of misuse. Given the dual-use nature of AI technologies, frameworks developed for civilian use could be expanded or adapted, but they will require recalibration to address the specific risks posed by militarised open-source AI.

Regulating the Military Use of Open-Source AI

Strengthening international governance frameworks will be crucial in addressing the growing risks associated with open-source military AI. At the same time, binding global agreements may prove difficult to fully enforce because of domestic political constraints. Existing multilateral conferences, such as the Responsible AI in the Military Domain (REAIM) Summit, offer a good starting point for multistakeholder dialogue.

Platforms like the REAIM Summit and other similar initiatives need to focus on creating shared regulatory frameworks that can help manage and reduce the militarisation of open-source AI models. This might involve practical steps such as setting up early warning systems to detect any suspicious military uses of open-source tools, along with encouraging voluntary transparency for state-led AI projects. By tackling these risks head-on, these platforms can significantly help bridge the current governance gaps and promote greater accountability in the development of military AI.

There is also a need to work with private sector developers of open-source AI to implement technical and policy safeguards to prevent their misuse for military applications. For example, Meta's Llama Guard is an open-source classifier designed to detect potentially harmful outputs. Llama Guard demonstrates one way of implementing technical safeguards that are embedded within open-source models.

Additionally, the BigScience Workshop's development of the BLOOM model showcases how the open-source community can play a proactive role in AI governance. BLOOM was released with usage restrictions and detailed documentation, emphasising the importance of collaboration, sharing ideas and the role of community-oriented standards. Together, these examples show that building guardrails for open-source AI is entirely possible; the challenge lies in scaling these efforts through enforceable policies and widely adopted industry standards.

Conclusion

As the militarisation of open-source AI models intensifies, the ability of existing governance efforts to manage the associated risks will depend on a concerted partnership between states, the private sector, and the open-source community. While transparency and accessibility are crucial to the advancement of AI, safeguards and accountability are equally important.

Asia finds itself in an exciting yet precarious situation. There is a need for stronger regional coordination and proactive engagement in global and Asia-specific governance frameworks for military AI; otherwise, the region risks becoming vulnerable to the strategic exploitation of open-source AI for military purposes.

The region does not need to start from scratch when developing regulation. Taking stock of existing efforts by states and other players is an important first step towards developing regional technical safeguards and enhancing international cooperation. The expertise and tools already exist to address some of the critical challenges posed by the militarisation of open-source AI.

What is needed is multilateral coordination and enforcement based on shared principles, although this will pose another significant challenge, given the fractious nature of the regional and global order.

Annemarie Mugisa Acen recently graduated with an MSc in International Relations from the S. Rajaratnam School of International Studies (RSIS) at Nanyang Technological University. She interned with RSIS' Military Transformations Programme from December 2024 to May 2025.

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.