Civil Military Operations in the Age of Artificial Intelligence

Major Tony Smith

The introduction of artificial intelligence (AI) serves as the next major offset technology transforming the character of war. In 2018, the Department of Defense rolled out its AI strategy, largely ignoring risks and external factors that make AI's arrival a challenge for the United States. In competition, malicious AI use by geopolitical competitors is already contesting the psychological-cultural elements in the human domain where Civil Affairs operates. CA contributes to winning without fighting in the information domain by adopting counter-AI strategies that degrade a geopolitical competitor's ability to shape conditions during competition in preparation for armed conflict. In addition, CA can develop techniques that reduce AI's effectiveness during armed conflict to impact an adversary's decision-making calculus. As an information and maneuver force, CA is a capability the DoD should leverage to secure competitive advantages and win left of bang.

The use of AI in the Ukraine War illustrates challenges and highlights opportunities for future Civil Military operations (CMO). The malicious employment of AI by geopolitical competitors in the information domain increases the complexity and decreases the effectiveness of current CMO. This requires Civil Affairs to adopt measures that detect the scope of AI in the civil environment and contribute to the joint force's understanding of AI's use in the information domain. CA must also establish protective and defensive measures that counter malicious AI's impact on CMO and the civil environment.

The paper aims to examine the complexity AI imposes on Civil Affairs Operations (CAO) and propose novel solutions based on current trends. The latest CAO doctrine is cross-examined with events from the Ukraine war to highlight potential vulnerabilities and generate discussion on ways an adversary may use malicious AI to impact the civil environment. In addition, the paper utilizes other historical events to reinforce potential challenges to CMO. A way forward is proposed for CA forces that expands the focus of civil engagement and reconnaissance, integrates emerging capabilities into force structure, and postures CA and the joint force to operate in tandem with a digital landscape.

Three major themes are proposed as solutions by the author under the umbrellas of detection, protection, and defense. Detection measures include a preliminary understanding of an operating area's digital and data landscape and subsequently identifying AI technologies impacting the civil environment, particularly in the information domain. Protective measures involve reducing risk to Civil Affairs forces and the civil networks constructed within the civil environment. Finally, defensive measures include activities that challenge geopolitical competitors' attempts to delegitimize military operations, destabilize society through disinformation, and create instability in governmental institutions.

The author argues that the arrival of AI in competition and conflict challenges current CMO. Civil Affairs must be an active player in challenging geopolitical competitors' malicious use of AI during competition to serve as a force that wins without fighting.