AI-ENHANCED COUNTER-OFFENSIVE DECISION-MAKING IN HYBRID WARFARE

Vladimir Babanov, Ph.D.

Chief-assistant professor, South-West University "Neofit Rilski"

Scopus Author ID: 60021493300; ORCiD: 0000-0001-8596-6493

E-mail: v.babanov@law.swu.bg

Summary: *In this article the use of artificial intelligence (AI) is being explored as a method for enhancing counter-offensive decision making within hybrid warfare environment. It is defined as an area where the intersection of conventional military tactics and other forms of warfare, such as cyber warfare, information warfare and psychological warfare, occur. Hybrid warfare creates conditions of uncertainty, urgency and high levels of asymmetry which necessitates effective and timely decision-making. The research demonstrates that the use of AI may provide enhanced support for counter-offensive planning by reducing decision cycle time, providing support for the integration of multiple domain data and by enhancing situational awareness using analytical tools and decision-support systems. The research identifies the benefits of AI enabled decision-making but also points out the existing limitations. It concludes that AI could be most effective when used as part of a balanced human-machine system whereby AI provides support for data driven decision-making processes and humans maintain strategic judgment and accountability.*

Keywords: *artificial intelligence, hybrid warfare, cyberwarfare, security policy, defense policy.*

Introduction

The concept of hybrid warfare has been used to explain a wide range of conflict strategies that include both conventional military action and unconventional tactics such as cyber-attacks, psychological or disinformation operations. These are described as having a number of characteristics including the synergies between different types of conflict. From these traits originate features that have been widely observed. They include difficulty of attributing responsibility for an attack, an asymmetric relationship between the belligerents, the disruption of norms and rules as well as a psychological influence over perceptions.

The nature of hybrid warfare creates challenging and complex environment for developing counter-offensive military plans in real time. In such uncertain circumstances, the technology of artificial intelligence (AI) seems as a promising option to improve the decision-making process of the nation-states under hybrid aggression. In terms of the potential improvement of the decision-making process for developing counter-offensive military plans, AI is particularly well-suited due to its ability to derive and rapidly analyze large volumes of data from a variety of sources and do it simultaneously. Once the data has been analyzed, AI could identify patterns, learn from past experiences, and generate actionable intelligence instantaneously. In theory, AI could provide military commanders with greater situational awareness and increase their options of stopping the adversary's advances and transition towards a counter-offensive actions.

The ongoing AI arms race between the nation-states is a confirmation of the technology's perceived value as a strategic advantage in the conduct of modern warfare (Sheikh, 2022). The advantage manifests mainly in several ways in which AI could be integrated for counter-offensive efforts. As hybrid warfare represents a multi-domain phenomenon, the duality of AI could be employed regarding the ambiguity and asymmetry, the fight against disruptive innovation or its acceleration and the psychological operations on both domestic and foreign population. For example, AI can facilitate levels of coordination and surprise unknown to warfare, and thus, represent a new paradigm for the conduct of hybrid warfare. At the same time, the integration of AI in the effort against hybrid attacks represents a significant risk even if used correctly. Specifically, a rogue AI could potentially lead to disruption of society's critical infrastructure, bringing loss of control of a state's economy and institutions. Thus, the duality of AI-enhanced decision-making in hybrid warfare requires a further study.

In this context, the article explores the effects of AI on the developing a counter-offensive in hybrid conflict, specifically addressing the strategic implications in the development stage. The study examines general principles that guide the development of an offense under a hybrid aggression. The Introduction establishes the context and stakes for using AI in multi-domain warfare. The Methodology section describes the analytical approach employed in the article. Further, in the Discussion is represented an analysis of the influence of AI on the development of an offense, and the consequences ranging from altered cognitive dynamics to the ethical and organizational implications. At the end, the article concludes with a summary of the main points discovered.

Methodology

By using a qualitative, multi-disciplinary methodology, the study investigated the possibility of AI-enhanced decision-making in hybrid warfare. The study relied on a systematic literature review of recent published academic research available in three major databases- Google Scholar, Scopus, Web of Science. During the selection phase, priority was assigned to literature that explicitly addressed the intersection of AI, military decision-making processes and hybrid conflicts. The majority of the literature selected was published in defense-related journals, proceedings from international security conferences, and policy-oriented research reports authored by defense research organizations.

Priority was placed on identifying literature related to the use of AI in enhancing strategic planning, operational tempo, human cognitive factors and organizational adaptation since all of these areas relate directly to the research question. By integrating findings from multiple disciplinary perspectives, the article develops a comprehensive understanding of how AI can potentially be used to enhance decision-making processes for counter-offensive operations in hybrid attacks. The use of this methodology enables the development of a conceptual framework for addressing the research problem, which acknowledges that the field of AI-enhanced military decision-making is rapidly developing. The next section of the paper uses this methodology to analyze the primary topic of interest, followed by an additional section of the paper that discusses the implications of the findings, and the potential future research directions.

Discussion

The possible impact of AI on counter-offensive decision making is demonstrated in the increased speed of the decision cycle. The speed of decision-making is often measured in terms of the DOODA loop (Dynamic Observe–Orient–Decide–Act). In hybrid war, which has elements of fast-paced cyber and information operations, an accelerated DOODA loop is required to take the initiative from the attacker. AI could decrease the time required for each of the four phases of the DOODA loop. On the Observe side, AI driven analytics could analyze and interpret data from a variety of sources, including satellites, intercepted communications, social media, and surveillance drones. It could filter out irrelevant information, and highlight new developments in the battlespace (Brehmer, 2010).

Once the Observe phase is complete, the Orientation phase can begin with machine learning algorithms integrating the available data and develop a cohesive operational picture. They can also apply predictive modeling techniques, including running what-if simulations and

micro-wargaming to predict how an adversary may respond to various courses of action (Schubert, J., Brynielsson, J., Nilsson, M., & Svenmarck, P., 2018). The Decide phase could utilize Decision Support Systems (DSS), which evaluate multiple options, identify the best course of action, and provide recommendations based on the generated data. This is possible because DSS consider many variables (i.e., terrain, enemy posture, timing, etc.) at a much faster rate than can be accomplished through human staff planning.

Once the Decide phase is completed, the Act phase initiates. AI could execute certain decisions (e.g. a cyber operation or signal to autonomous drones to engage a target) with little to no delay, or provide a list of vetted decisions to human commanders for approval (Schubert, J., Brynielsson, J., Nilsson, M., & Svenmarck, P., 2018). Taken together, these improvements offer the possibility of creating a hyper-accelerated offensive tempo. A command that utilizes AI to accelerate both the processing of information and decision making relative to an adversary might achieve decision superiority, and dictate the terms of the battle. For this purpose, speed of action in hybrid warfare conditions has gained even greater importance. With an ability to make and act on decisions before the adversary, an AI-enabled force could potentially disrupt their plans for the conflict and accomplish this objectives in the early stages.

This advantage is especially relevant in hybrid warfare, where surprise and psychological shock are valuable advantages. Well-coordinated attacks in multiple domains could produce disproportionate effects. However, like any other tool, speed is a two-edged sword. If the foundational data or algorithms used in decision support systems are either flawed or biased, negative consequences may follow. Therefore, to avoid failure, the use of AI to enhance the decision cycle, must be balanced by ensuring high-quality decisions.

Understanding the various elements of complex systems, including an enemy's military capabilities, their civil infrastructure and the bias and behavior of the civilian population, is essential to developing effective campaigns. AI's strengths in pattern identification and large data analysis significantly assist in finding high value targets as well as points of leverage. In kinetic warfare, AI enhanced reconnaissance, through computer vision for image intelligence or signal processing for electronic intelligence, could provide details regarding the location and logistics of an enemy that may be missed by human analysts (Moy, W. R., Gradon, K. T., 2023).

AI could compile data into a common operational picture (COP) so that decision makers would have a better understanding of the battlefield and its current status. Thus, AI could help offensive planners focus on pressing challenges rather than analyzing raw data. AI could also enhance the precision of offensive action. Through its ability to analyze sensor feeds, AI

algorithms could recognize legitimate targets from decoy or civilian objects with greater accuracy, thereby providing the basis for precise strikes. While precision refers to the accuracy of a strike, it also pertains to the timing and customization of non-kinetic attacks. Through predictive analytics, AI could identify the most impactful time to initiate a disinformation campaign to maximize psychological effect on the adversary's strategic commands and population (Kretysova, 2018).

AI also utilizes predictive analytics to allocate assets in electronic or cyber warfare. AI could also identify and determine which communication nodes to disrupt or which servers to clog in order to induce cascading failures in an adversary's command and control systems. This comes with the precondition of a strong cyber intelligence data provided to AI models. Therefore, AI-enabled counter-offensive decisions have better chances to select appropriate targets, methods, and timing to obtain strategic advantage.

Although the use of AI spills in the mechanical activities involved in decision-making, it has significant effects on the cognitive processes of human staff members too. While decision-making could be considered equally a technical process and a psychological one, the introduction of AI tools may alleviate some cognitive pressures associated with the process. However, it introduces additional cognitive issues to be considered. A beneficial cognitive aspect to the use of AI decision support is the possibility to reduce human error due to cognitive biases. This comes with the condition that AI models themselves have been spared from bias during training. Since automated systems are not susceptible to fatigue, tunnel vision, and emotions, they could provide an objective second opinion to assist decision-makers. AI can help planners avoid the potential pitfalls of confirmation bias, by identifying information that the planner may have missed when developing plans. Additionally, there is experimental evidence suggesting that AI monitors of human factors can help minimize mistakes during high-pressure decision-making situations (Meerveld, H.W. *et al.*, 2023).

In this way, AI acts as a cognitive tool to ensure that offensive strategies are developed using data and rational analysis as opposed to impulse or ingrained bias. However, over-reliance on AI increases the likelihood of the occurrence of automation bias, i.e., the propensity to place excessive faith in the accuracy of machine-generated outputs. Although planners may have confidence in the AI's suggestions if the AI system generates reliable suggestions, but they may become overconfident in the AI's infallibility. This can create problems, as even the most sophisticated AI systems could err, or be deceived.

Establishing such balance requires educating personnel in AI literacy and the outputs of explainable AI (XAI) to clearly justify recommendations. This allows human decision

makers to evaluate AI-based recommendations against their own knowledge and experience, and fosters a collaborative cognitive process. Another cognitive factor is the role of human decision-makers in the decision loop. At the tactical levels, time-sensitive offensive actions may require machine-only decision-making in order to maximize response times, which creates additional risks.

A key cognitive issue to be resolved is determining where AI should be allowed to automate decisions, and where human decision-making must take precedence (Feffer et al., 2024). Effective offensive decision-making in hybrid warfare will likely rely on a hybrid intelligence approach. In it, AI would manage routine and data-driven tasks so that human decision-makers could focus on strategic tasks. Conversely, human decision-makers would be responsible for authorizing large-scale offensive moves, considering the full scope of the operation and its implications.

Challenges and limitations

The implementation of AI in counter-offensive decision-making has both strategic and institutional challenges. Strategically, a concern is the potential destabilizing effect on international relations. The faster and more definitive is the nature of AI-supported attacks, the bigger is the possibility of unintended damage, that can diminish support from the international community. AI may create an "offense-dominant" environment which encourages pre-emptive attacks that international partners could consider inappropriate. Additionally, the speed at which AI supported attacks could be launched may limit the time available to diplomats and other decision-makers to resolve conflicts peacefully. Such situation introduces the risk of cascading escalation of attacks without safety mechanism (Yamin et al., 2021). There is still a lack of prevention of false positives that can lead to targeting benign participants in the conflict zone. Therefore, as AI becomes more prevalent in future combat environments, the inclusion of safety mechanisms and human verification processes becomes essential.

The issue of trust, or more correctly the lack thereof, is prevalent in almost all activities facing AI adoption. In the military, the development of new doctrine that formalizes the role of AI in decision-making is a hurdle itself. Similarly, within military organizations, clear rules of engagement for AI usage are also needed. In addition to policy and procedural development, there are several practical barriers to implementing AI in military organizations. They encompass the acquisition of high-quality data to train AI models, the modification of legacy systems to facilitate AI models, and the recruitment of personnel with technical skills sufficient to operate and maintain AI systems. The risk of compromised AI systems is significant and

could result in misleading recommendations to decision-makers with adverse outcomes. Therefore, as much attention should be placed in securing AI systems as is placed in securing critical infrastructure.

Between the most common challenges mentioned are the ethical and legal liabilities associated with AI-augmented decisions. Military operations often involve high stakes, and AI increases the degree of ambiguity surrounding the liability of various individuals involved in the decision process. Current laws of armed conflict place liability for actions taken during military operations on the human commanders. However, the opaque nature of many AI decisions creates a gray area, and therefore, requires additional consideration. The development of "human-in-the-loop" remains especially valid for military decision-making as well as thorough validation trials for AI-based decisions (Meerveld, H.W. *et al.*, 2023).

In this way, the liability for decisions made using AI can be transferred back to humans, thereby ensuring accountability for all decisions made utilizing AI. The strategic benefits of AI (speed and precision in offensive decision-making) are contingent upon the ability of organizations to adapt institutionally. Nation-states must transform their structures to facilitate the full utilization of AI capabilities. They must also train personnel to effectively work with AI, and implement adequate safeguards to ensure that AI does not have a negative impact on their security.

Conclusion

The successful integration of AI into decision making processes would depend on the balance between the benefits of using AI for enhanced decision-making processes and implementing sufficient controls to limit the potential for unintended consequences. Based on the preceding analysis, several primary themes emerge that represent the current state of the discussion.

The first one is that AI has the potential to grant a competitive advantage in terms of speed and the ability to conduct complex coordinated offensive operations (Collier, 2025). As such, the side that uses AI most effectively to accelerate the cognitive process for decision making and execute multi-domain operations can potentially “establish a dominant position” in conflict. Although the speed-based competitive advantage can be a significant factor in achieving a favorable outcome, it also presents risks to strategic stability. Specifically, the speed at which military operations can now occur reduces the time available for possible de-escalation.

The second one is that the nature of the relationship between humans and AI would determine how decisions are made. The goal is to develop a hybrid intelligence that combines the analytical abilities of machines with the judgment and creativity of humans. In this context, humans provide the intent and ethical guidance in combination with creativity. AI ensures precision and recalls of datasets with logical reasoning. This is key in the effort to mitigate each other's shortcomings.

Third, the utilization of AI for decision-making brings a paradigm shift on how organizations prepare. Military organizations must create a culture of AI-readiness. This would require updates to doctrine that clearly outline the authority and roles of AI in planning and executing military operations. Moreover, military organizations need to invest in education to ensure that all members of the organization, regardless of rank or function, understand the strengths and limitations of AI.

Fourth, a consistent framework for the use of AI in warfare is extremely necessary. Such frameworks could include constraints on autonomous offensive actions, requirements for explanations of AI used in identifying targets, and the establishment of rules of engagement specific to AI-driven operations.

In the discussions about the use of AI-enhanced counter-offensive decision-making must be recognized that AI is a tool for the objectives of human politics. While the introduction of AI will not change the fundamental causes of hybrid conflicts or the necessity of a clear strategy, AI will change the means and tempo of implementation of those strategies. There will be an increased emphasis on the ability of humans to learn and adapt to changing circumstances as they increasingly interact with AI in decision loops. Strategically, a reevaluation of the concepts of surprise and deception in warfare is becoming more likely, due to the utilization of AI by the involved parties, potentially resulting in rapid exchange of attacks and counterattacks.

Bibliography:

1. Shiekh, H. (2022). AI as a Tool of Hybrid Warfare: Challenges and Responses. *Journal of Information Warfare*, *21*(2), 36-49.

2. Brehmer, B. (2010). Command and control as design. In Proceedings of the 15th International Command and Control Research and Technology Symposium. Washington, DC: US Department of Defense CCRP, paper 182, https://www.dodccrp.org/events/15th_iccrts_2010/papers/182.pdf

3. Schubert, J., Brynielsson, J., Nilsson, M., & Svenmarck, P. (2018, November). Artificial intelligence for decision support in command and control systems. In *23rd International Command and Control Research & Technology Symposium "Multi-Domain C* (Vol. 2, pp. 18-33) https://www.researchgate.net/publication/330638139_Artificial_Intelligence_for_Decision_Support_in_Command_and_Control_Systems

4. Moy, W. R., & Gradon, K. T. (2023). Artificial intelligence in hybrid and information warfare: A double-edged sword. In *Artificial intelligence and international conflict in cyberspace* (pp. 47-74). Routledge. https://www.researchgate.net/publication/378013172_Disinformation_and_Artificial_Intelligence_Techniques_-_a_Double-Edged_Sword

5. Meerveld, H.W., Lindelauf, R.H.A., Postma, E.O. *et al.* The irresponsibility of not using AI in the military. *Ethics Inf Technol* **25**, 14 (2023). https://doi.org/10.1007/s10676-023-09683-0

6. Collier, H. (2025, June). AI in Social Engineering: The Next Generation of Offensive Cyber Operations. In *European Conference on Cyber Warfare and Security* (pp. 80-83A). Academic Conferences International Limited. DOI:10.34190/eccws.24.1.3385

7. Feffer, M., Sinha, A., Deng, W. H., Lipton, Z. C., & Heidari, H. (2024, October). Red-teaming for generative AI: Silver bullet or security theater?. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* (Vol. 7, pp. 421-437).

8. Yamin, M. M., Ullah, M., Ullah, H., & Katt, B. (2021). Weaponized AI for cyber attacks. *Journal of Information Security and Applications*, *57*, 102722. https://doi.org/10.1016/j.jisa.2020.102722

9. Kertysova, K. (2018). Artificial intelligence and disinformation: How AI changes the way disinformation is produced, disseminated, and can be countered. Security and Human Rights, 29(1-4), 55-81. https://brill.com/view/journals/shrs/29/1-4/article-p55_55.pdf