THE CURRENT

AI AND GLOBAL SECURITY: IMPLICATIONS FOR MILITARY OPERATIONS

ARWIN DATUMAYA WAHYUDI SUMARI

The dual-use nature of AI technology has triggered concerns regarding its use for unfavorable acts in military operations. International humanitarian law must adapt to the rapid changes in AI-enabled military operations to ensure global security and peace.

INTRODUCTION

The ubiquitous reach and application of artificial intelligence AI across most echelons of society and goverment has triggered a new generation of warfare as its functionality is applied to formulating warfare strategies, tactics, and operations. Accompanying the potential improvements in the nature of warfare are fears AI could be maliciously employed by state or nonstate actors worldwide.

AI technology is beneficial to numerous industries and vocations; at the same time, when used in high-risk tasks, AI can unintentionally lead to the loss of human life. Certainly, AI technology positively impacts military operations, especially in the case of highly dynamic, complex, data-rich, time-constrained operations. At the same time, the dual-use nature of AI technology can lead to security vulnerabilities and expose loopholes in

international humanitarian law (IHL) that could pave the way for its misuse and malicious use. In an era of emerging and disruptive technologies, therefore, AI technology employment in defense and military operations must be governed by international norms of responsible use to maintain global security stability.

Great-power nations have competed to make the most of AI's capabilities to improve their economies and strengthen their respective armed forces. The United States, China, and Russia have allocated considerable budgets to building armed forces strengthened with AI-based combat equipment. Using AI technology in military weaponry or weaponizing AI changes the landscape of global security, including geopolitical and geoeconomic aspects that impact military geostrategy.

In Russia's ongoing war against Ukraine, both nations have utilized drones equipped with AI technology. This has many battlefield advantages such as carrying out reconnaissance and surveillance deep behind enemy lines, increasing the reach of military operations, reducing casualties of soldiers and civilians, and saving money and time on military operations. The use of AI technology in drones can increase targeting accuracy by up to 80 percent. The advantages of AI have led the United States to invest significantly in such technology to advance its strategic interests.

Despite its advantages, the results of a survey on the use of AI in military operations revealed that 68 percent of the public harbors concerns about the use of autonomous weapons systems (AWS). These systems can be deployed in ways that lead to violations of IHL. For example, some allege Israel's use of AI technology in Palestinian territories has resulted in some civilian deaths. This type of AI technology can result in collateral damage (unintended civilian casualties). With the weaponization of AI for military operations, the world must enact new norms that require any country using these technologies to adhere to international legal and ethical frameworks.

AI technology in combat equipment shows excellent prospects for increasing the visibility of targets, reducing the risk of casualties to soldiers and civilians, and penetrating battlespaces risky to humans. On the other hand, AI technology has the potential to be misused for purposes that can significantly and negatively impact security and humanity and disrupt the current world order. Some misuses of AI include creating new techniques for cyberattacks, creating fake information for deception, and, more severely, creating lethal weapons of mass destruction. Indeed, the threat resulting from the use of AI in AWS becomes more significant when applied to weapons of mass destruction.

The world's great powers have been competing to master AI technology. They have allocated large budgets for research, development, application, and implementation of various AI technologies in their weapons systems. Yet, AI does not stand alone; it is the work of humans. Its creation and use depend heavily on the original intent when it was created. The use of AI technology can thus be considered from two perspectives: internal and external. Internal factors are related to humans as creators, and external factors are related to humans as users. For example, the United States develops AI-based weapons systems for lethal attacks, while China focuses on AI-based systems for paralyzing its adversaries' forces.

AI TECHNOLOGY AND REGIONAL AND GLOBAL SECURITY

Across history, militaries have initiated the development of various advanced technologies globally. Karl von Clausewitz famously observed, "war is a mere continuation of policy by other means." As such, the use of AI for military purposes directly impacts the world's political maps. Additionally, some technologies are made available for public use, while others fall under intellectual property rights protections, and no specific prohibition exists for any country to control it. In other words, there is no geographical limit to the development and application of these technologies.

Considering AI from the perspective of strategic competition, great-power countries have allocated considerable budgets to build, develop, and implement AI technology into their weap-

ons systems. AI technology is now a prime focus of the research and development of multiple types of modern combat equipment, including the next-generation air dominance (NGAD) fighter F-47, which can control many autonomous drones. In fiscal year 2025, the United States allocated $1.8 billion for AI, while the Defense Advanced Research Project Agency (DARPA) has requested funding to develop AI and human-machine symbiosis to enable better decisions in complex battlefield environments. In March 2025, China announced it would budget approximately $246 billion for defense with a focus on surveillance. Russia is allocating defense funds that are projected to reach $132 billion to build AI for military robotics and to integrate AI into military systems. The AI mastery competition between the United States and China, as well as some countries in the EU and the UK, is represented in the form of granted patents, where China leads with 60 percent.

As is the nature of dual-use technology, AI can degrade global security. AI technology applied to civilian interests can be redirected for military purposes by inserting certain codes into computer programs that quickly change the way an algorithm works. Accordingly, from the perspective of security challenges, using AI technology in weapons systems can pose both direct, military threats and indirect, nonmilitary threats. The race to build lethal autonomous weapons systems (LAWS) may trigger countries in the region that feel intimidated to take steps to create national defense strategies in anticipation of AI-based warfare. In such an AI arms race, countries with strong technological and economic foundations will further build and develop LAWS, and countries with limited capabilities will seek alliances or form new alliances with great-power nations. Such escalation could lead to direct military conflict. These same countries—nations with limited capabilities but rich in resources needed to support the development of LAWS—can also be vulnerable to political, economic, and/or social pressure at the hands of great-power nations seeking to acquire these resources, especially energy, to develop capabilities.

THE MILITARY AND AI

Data and facts show that militaries of great-power nations have built and used AI technology in exercises and actual military operations. Some countries have declared their use of AI technology in war equipment, some have built and developed this capability in secret, and some have plans to develop this AI capability. A growing number of military tasks can be handed over to AI. Currently, AI is being used to gather intelligence for domestic interests and develop strategies for controlling available resources in regional and global countries. AI-augmented intelligence enables a country to strategize to secure domestic resources and explore resources beyond its borders. AI is also being used in prediction models to accelerate the decision-making cycle with more accurate recommendations. Finally, AI is being employed in personnel and weapon safety and security to reduce errors in decision-making.

The goal of incorporating AI technology into AWS is to enable these weapons systems to conduct multipurpose warfare. This technology can "reduce the direct involvement of personnel while simultaneously increasing the lethal impact on the enemy." Additionally, AI can accelerate the detection, analysis, and repair of weapons thus improving the maintenance process. AI can also leverage cyberspace security and computer network protection capabilities in cyberspace.

MALICIOUS USE

There is always the potential for AI technology to be used in nefarious ways. AI technology can be misused in the operations of weapons systems, for example, transforming hypersonic missiles into LAWS WMDs. State and nonstate actors can utilize drones with independent decision-making capabilities to commit unfavorable acts. Cyberattacks can be executed with new AI-engineered techniques. Disinformation, misinformation, theft, and propaganda have occurred through various means, in person and online (i.e., social media). These techniques represent cognitive warfare and can be combined with other methods to evolve into a hybrid attack on a nation.

CONCLUSION AND RECOMMENDATIONS

The global competition between great-power countries to master AI technology for military purposes has significantly impacted international security. These militaries are generally the leading initiators of advanced technologies. Accordingly, the actual and potential application of AI in dual-use capacities by these militaries has made the pursuit of AI a security dilemma and represents a new threat to world security. Moreover, the abuse of AI in military operations by several countries is evident today. Although a country's use of advanced technology to attack an adversary has been regulated in international law, IHL has not explicitly dealt with WMD LAWS. For this reason, a balance is needed. Responsible nations must work together to form new, responsive global norms for the weaponization and militarization of AI to prevent it from being used in violation of IHL. In particular, concerned nations must

- Strengthen the language of IHL to emphasize that AI technology in military operations is intended for use only in war situations and only against combatants as well as to reduce collateral damage to civilians. Some suggestions include convening special meetings in countries with IHL mandates, producing joint resolutions incorporating articles on AWS's ethical and moral use of AWS, and prohibiting the use of LAWS.
- Build trust that any party using military AI technology will not abuse it, including both great-power and regional-power countries. Promulgate a joint UN resolution, or resolutions by other multinational bodies to prevent misuse and malicious use of AI for military operations.
- Encourage great-power and regional-power countries to formally agree to restrict military AI technology applications to defensive rather than offensive purposes.
- Advocate that globally, AI technology be used solely to improve human welfare and security. Formulate an international joint resolution that AI technology is intended for human welfare and the maintenance of global security interests and not for offensive war or other destructive acts. ~ **Σ**

ABOUT THE AUTHOR

AFM Asst. Prof. Dr. Ir. Arwin Datumaya Wahyudi Sumari, S.T., M.T., IPU, ASEAN Eng., ACPE, EPEC Eng. is a member of the Indonesian Air Force. He is a former rector of the Adisutjipto Institute of Aerospace Technology and holds national and international certifications and several patents and copyrights on artificial intelligence and its applications. He is currently special staff to the chief of staff of the Indonesian Air Force and an adjunct professor at the State Polytechnic of Malang, Indonesia.

The Current | © George C. Marshall European Center for Security Studies | ISSN: 3053-0342