

Technologies like artificial intelligence are changing our understanding of war

December 11 2023, by Jordan Richard Schoenherr



Credit: Pixabay/CC0 Public Domain

Artificial intelligence (AI) is widely regarded as a disruptive technology because it has the potential to fundamentally alter social relationships. AI has affected [how people understand the world](#), [the jobs available in the](#)

[workforce](#) and judgments of [who merits employment](#) or [threatens society](#).

Nowhere is this more apparent than in warfare, which is defined by social and technological processes. Technologies such as [autonomous weapon systems \(AWS\)](#) and [cyberweapons](#) have the potential to change conflicts and combat forever.

Justifying warfare

[Acts of violence committed in war are often framed in virtuous terms](#), with [justice and other morality motivations](#) used to legitimate armed conflict.

Yet "[just wars](#)" require both clear definitions of who is a combatant and clear distinctions between war and peace. When such distinctions are eroded, this leads to [total wars](#)—all against all. Boundaries between civilians and soldiers and military and domestic infrastructure are blurred, making everyone and everything a legitimate target. We might believe that total wars are a thing of the past, involving [Mongolian hordes](#) or [trench warfare](#), but [recent discussions](#) of technology's impact on warfare have breathed new life into the concept.

New battlefields, old conflicts

Information has always been key to the successful development and implementation of military strategy and battlefield tactics, with [information warfare](#) predating the information age. Knowing the position and temperament of adversaries plays a decisive role in [predicting and manipulating their attitudes and behavior](#).

In our information age, we might assume that technological superiority

in collecting and aggregating data will translate into significant changes in the balance of power. This hasn't always been realized. [To be useful, data must be informative](#). Patterns might remain obscured in noisy data, might be too novel to be recognized or might be misidentified.

The ongoing Israel-Hamas war provides a clear example. [Palestinians are some of the most surveilled people in the world](#), with Israel pioneering and using [facial recognition technology](#) and [drone surveillance](#). This surveillance was justified on the grounds that more military intelligence would reduce the possibility of an attack.

Hamas's ability to inflict such a vicious, widespread co-ordinated attack on Oct. 7, 2023 cannot be attributed to superior technology. The Israeli army had more resources. Instead, [failures of human intelligence](#) and [successful concealment](#) provide the best explanation.

Hamas's use of drone technology also provided a decisive advantage. Despite Israel's earlier [destruction of the Hamas drone program](#), [the militant group's use of drones in the October attack](#) was a critical determinant of its success. This demonstrates the resiliency of armed forces that use relatively inexpensive technologies.

War without fighters

Cyberattacks are another emerging tool in the arsenal. As non-lethal weapons, [their threat and role in combat](#) continues to be a matter of debate: cyberattacks lead to disrupted or defaced websites, financial loss and compromised information. They rarely directly affect the physical world.

One notable exception is an attack [attributed to the U.S. and Israel](#) known as [the Stuxnet virus](#). It successfully damaged Iran's nuclear centrifuge equipment, setting the program back for years.

In contrast to traditional weapons, cyberweapons might best be seen as [force multipliers](#). Battlefields have always relied on communication between commanders and units. Disrupting communication during a critical military operation can reduce the offensive and defensive capabilities of an adversary. However, as more automated weapons systems are adopted, these weapons could be turned against their own armies using cyberattacks.

The most significant concern is that these weapons will be used to attack [critical infrastructure](#), the way [Russia disrupted the power grid in winter during its war on Ukraine](#).

Cyberspace itself is difficult for many to understand. The indirect relationship between action and consequences and the limited realism of data often results in organizations discounting the frequency and severity of these attacks. By [overestimating their ability to effectively cope with such attacks](#), they create vulnerabilities for themselves and the societies that they supply with their goods and services.

Like traditional weapons, [the precision of cyberweapons is key](#). In the case of Stuxnet, [the virus was not contained and it infected other computers](#). Other malware can similarly have a widespread effect.

The 2009 Conficker virus [nearly consumed the internet](#) with its ability to autonomously adapt and replicate within systems. If such an approach were weaponized, such a virus could disrupt commerce, power grids and transportation systems.

Wars of words

Alone, AI-based weapons will [not change the nature of warfare](#). They might nevertheless change how we [perceive and describe conflicts](#).

In the U.S., cyber operations have been described as "[persistent engagements](#)," framing attacks as an unrelenting conflict. In China, "[unrestricted warfare](#)" suggests that all methods and targets are permissible.

Both [North Korea's estimated 1.5 million cyberattacks on South Korea](#), as well as [attacks on Taiwan attributed to China](#), fit this pattern.

The limited capabilities of cyberattacks are less concerning than physical attacks. China's increased use of drones has [stoked tensions with neighbors, including Japan](#). Previous drone incursions have been referred to as "[acts of war](#)," with Taiwan [shooting one down last year](#). A rogue drone—or swarm—could unintentionally act as a catalyst for conflict in unstable geopolitical regions.

Yet, while state and non-state entities might act in a belligerent manner or even [take aggressive postures](#), these actions are often simply gambits. Despite the widely publicized [Chinese surveillance balloon that flew over Canada and the U.S.](#) last year, [the recent meeting between U.S. President Joe Biden and China's Xi Jinping](#) illustrates that words don't always translate into actions. And despite its threatening posturing, [China doesn't yet have the capacity to invade Taiwan](#).

Wars conducted solely or primarily with AI-enabled technologies will not likely happen in the near future. Humans will remain the primary combatants—and victims—of armed conflict.

While the rationales for wars will remain the same, we must consider how autonomous weapons and cyberweapons will change how conflicts will be perceived and fought. If they're fought beyond the abilities of meaningful human control, we are placing our fates in the hands of machines.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: Technologies like artificial intelligence are changing our understanding of war (2023, December 11) retrieved 30 April 2024 from <https://phys.org/news/2023-12-technologies-artificial-intelligence-war.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.