Thought Leader

Mundane tech can be used for lethal ends

Israel is making use of artificial intelligence to further its genocidal agenda in Gaza

Amrita Pande & Anaïs Nony

When did it become ethical for machines, whose logic most humans can't even understand, to decide which parts of humanity to erase?

The role of artificial intelligence (AI) in the genocide unfolding in Gaza has revealed how AI-powered technology is causing unprecedented annihilation through killer drones, remote-controlled quadcopters, precision-guided smart bombs, programmed kill lists and targeting systems.

What is unfolding in Gaza today is a culmination of decades of civilian technologies that are being repurposed for genocidal acts.

The role of AI systems in unleashing this horror lies in widespread, mundane and everyday technologies developed during peacetime, such as biometric surveillance, predictive policing and algorithmic curation of social media to promote behavioural obedience.

Seemingly harmless AI biometric surveillance, such as the facial recognition systems on our phones, can easily evolve into a genocide agent.

From Facebook likes to video chat, no one can say with certainty if the technology we use every day is not compromised; if the data we produce is not being used to discriminate against activists or silence information.

In an Al Jazeera piece, Somdeep Sen argues that censorship has always been a necessary complement of genocide. Foreign journalists are not permitted to enter Gaza and Palestinian journalists in Gaza are silenced and killed. According to the New York-based Committee to Protect Journalists, as of 20 May, at least 105 journalists and media workers had been killed.

With AI and new communication technologies, this censorship has extended far beyond the borders of Israel-Palestine and has taken on new forms of algorithmic censorship.

Algorithmic censorship is based on automated operations for mediating communication on digital platforms.

Last year, half of the content circulating on the internet was automated traffic. This means that bots (short for robots) are running automated tasks which can either serve valuable functions (such as indexing websites) or have malicious intent and undertake criminal activities (such as fraud and mass manipulation).

According to the Imperva 2024 Bad Bot Report, the largest share of advanced bad bot traffic last year was found in the law and government industry.

In the context of geopolitical war, where citizens of the world have the right to make informed decisions, the impact of automated censorship is worrisome. Content considered problematic by a government can simply be suppressed on an ex-ante basis before users see it.

Understanding algorithmic censorship becomes even more crucial during conflicts, when one-sided, manipulated or sensationalised information is used to win the war for public sentiment.

Digital rights organisations and Human Rights Watch have criticised the Israeli cyber unit's surveillance and censorship of pro-Palestinian content; the targeting and slandering of journalists, scholars and activists as well as the surveillance of pro-Palestinian user content across the world.

In a report last year, Human Rights Watch documented over 1000 cases of suppression of pro-Palestinian content on Instagram and Facebook.

This censorship ranged from Meta putting a blanket ban on content related to the 7 October attack to Instagram suspending individual accounts, such as those of Leila Warah, Mondoweiss's West Bank correspondent, and Palestinian content designer Adnan Barq, to the "shadow banning" of pro-Palestinian media outlets by putting restrictions on their reach and visibility.

Shadow-banning is used as a tool to block users from social media platforms and online forums by making their posts or comments no longer visible to other users.

This kind of systematic censorship is legitimised by Meta's "dangerous organisations and individuals" policy which states that "to prevent and disrupt real-world harm, we do not allow organisations or individuals that proclaim a violent mission or are engaged in violence to have a presence on our platforms".

Although the full list of banned content remains a secret, a version of the list leaked by nonprofit media organisation The Intercept reveals that the majority are bodies that have been deemed violent by US foreign policy since 9/11 — those classified as "specially designated global terrorists".

But who defines terrorism or a violent mission? Unsurprisingly, terrorists are defined by using racial and religious proxies, predominantly black, South Asian and Middle Eastern groups.

On 29 May, the Israeli government passed a bill aimed at designating UNRWA, the UN Relief and Works Agency for Palestine Refugees in the Near East, as a terrorist organisation

Surveillance technologies developed during peacetime become lethal during conflicts, war and genocide

Manipulation: Crowds gather outside the California headquarters of Meta, which operates Facebook, to protest the censoring of posts about Palestine (above). Police raid the Al Jazeera offices in Jerusalem, Israel, on 5 May (left). Photos: Saeed Qaq/ Getty Images & Tayfun Coskun/ Getty Images

based on allegations made by Israel that some UNRWA staff members have ties to terrorist organisations, specifically Hamas and Islamic Jihad.

Algorithmic censorship, surveillance and control of user content regulates information flows around Israel-Palestine.

Studies have demonstrated the impact of filter bubbles, a term coined by internet activist Eli Pariser to describe the effects of algorithmically mediated, personalised content curation on intellectual isolation and polarisation of debates and, hence, on democratic thinking.

During conflicts and in conflict zones, such as in Israel, there is a concern about state-manipulated narratives and fake news accentuating such polarisation. The rapid and convenient uptake of the misinformation about "beheaded babies" is a case in point. These filter bubbles, where we only read a limited range of ideas, cause us to exist in echo chambers with selectively served information. We believe what we believe and neither read about, nor feel the need to engage with, different opinions.

While the industry of deep-fake videos and troll factories, run by misinformation contractors on the dark web and by government agencies, are instances of extreme propaganda, algorithm-driven polarisation of debates can be far more mundane.

Algorithms often categorise content based on patterns and user behaviour and are designed to suppress or promote certain content before streaming and dissemination through social media, news articles, posts etc.

This algorithmic curation of content essentially means all the news updates we scroll through on our tablets and phones are personalised to match our interests and worldviews.

Surveillance technologies developed during peacetime become lethal during conflicts, war and genocide. As reported by *The New York Times*, Israel's invasion of Gaza was an opportunity for the Israeli government to intensify existing biometric mass surveillance of Palestinians.

Cloud computing and machine learning services provided as "civilian technologies" by Big Tech companies such as Amazon, Google and Meta from Whatsapp to Israel and the Israel Defence Forces are repurposed for genocidal acts.

Much like law-enforcement agencies use predictive policing algorithms (PPA) to predict which children from which neighbourhood are most likely to join gangs and become criminals, the Israel Defence Forces uses PPA to predict who could become a Hamas operative.

Predicting is one thing, but taking action based on this prediction has graver consequences. Targeting systems such as Gospel and Lavender are graphic examples of how unchecked and unregulated use of these PPAs desensitise us to their use as technology of genocide.

Scholars and activists, such as Joy Buolamwini, founding director of The Algorithmic Justice League, and Timnit Gebru, founder of the Distributed Artificial Intelligence Research Institute, have demonstrated that PPA exacerbates long-standing biases based on categories such as gender and race.

This use of PPA increases the chances of racial profiling by feeding into and reinforcing historical biases. Biases become fatal for Palestinians in Israel. A case in point is the November amendment of Israel's counter-terrorism law by the Knesset allowing the military to monitor social media accounts, identify potential opposition and make preemptive arrests.

The amendment allows the military to imprison people based on their consumption of social media and even for "thinking" in ways that might be construed as pro-Palestinian and hence "potential acts of terror".

When considering the use of AI in times of war, the power of the machine reveals a paradoxical use — as a weapon to facilitate abuse. We are using tools (Google Docs, Whatsapp groups, Zoom meetings, Instagram profiles) to organise, spread information and resist power. Yet, the very tools we use to work against the hegemonic powers are produced by those powers.

In other words, the tools that we use to testify against horror are the same tools used to manipulate opinions, shape information and censor dissident voices. How did we end up using the master's tools to defeat the system of power in place?

This ambivalent power resides in the fact that the machine has no body, no emotions, such as empathy, and no duties, such as responsibility.

Yet, in every machine resides a human reality that speaks to the intent of the inventor and the moral value of the team of engineers who imagined, programmed and developed the machine, as well as whoever implemented it.

The technology of genocide deployed against the Palestinian people requires us to think differently of, not just violence and horror, but also humanity and human responsibility.

Amrita Pande is professor of sociology at the University of Cape Town and Anaïs Nony is an associate researcher at the Centre for the Study of Race, Gender & Class at the University of Johannesburg.