Policy **& Profit**

AMIR ISYAM ABDUL RAHIM
IM Possible Solutions Sdn Bhd managing director and Tunku scholar

AI as a weapon of war

- AI has entered the battlefield – and it's not on the sidelines
- Big Tech no longer just providers of infrastructure – they are targets
- AI-generated content now floods the digital front, influencing public opinion

UNLESS you have been living under a rock these past two months, you are aware of the rapidly deteriorating situation in the Middle East – now reverberating globally as energy prices surge.

Triggered by the United States' Operation Epic Fury and Israel's Operation Roaring Lion on Feb 28, 2026, what began as supposedly "targeted" strikes to eliminate Iran's nuclear capabilities – capabilities reportedly neutralised just months earlier – has escalated into a conflict spanning at least 10 countries, with spillover risks reaching Europe and Central Asia.

Its most profound global impact stems from Iran's blockade of the Strait of Hormuz, through which roughly a quarter of the world's oil and a fifth of its liquified natural gas (LNG) transit.

Although a fragile ceasefire was announced on April 8, 2026, early violations, stalled negotiations, and a US naval blockade point to continued instability.

While the geopolitical and military dimensions of this crisis continue to evolve, for policymakers, the conflict offers a series of lessons on the artificial intelligence (AI) digital front.

Big Tech as part of the modern kill chain

The conflict has signalled the effective collapse of "AI ethics" as a corporate priority, replaced by a clear national security pivot.

The post-2018 commitments to AI safety and the reluctance to deploy commercial technology for warfare or mass surveillance have largely given way to the active pursuit of defence applications by firms such as OpenAI, Palantir Technologies, Microsoft, and Google.

In doing so, Big Tech has shifted from passive service provider to a central component of the modern kill chain – effectively operating as defence contractors in all but name.

In the Gaza genocide, Israel reportedly leveraged Google and Amazon's US$1.2bil Project Nimbus infrastructure to support AI-driven targeting systems such as Lavender, The Gospel, and Where's Daddy.

These tools industrialised warfare – automating the identification of tens of thousands of targets at speed and scale, and, in tracking individuals to private residences for intentional strikes while with family.

This algorithmic warfare model reached new levels in the current conflict, with the United States using Palantir's Maven Smart System and Microsoft Azure's 'Secret' cloud to process real-time intelligence and run advanced combat simulations.

This depth of integration marked a turning point when Iran designated Big Tech infrastructure – including data centres – as legitimate military targets.

Subsequent strikes on data centre facilities in the United Arab Emirates and Bahrain underscored a new reality: the "cloud" is no longer abstract, but a physical frontline.

By hosting sensitive military workloads alongside civilian data, these firms have effectively blurred the line between commercial infrastructure and the battlefield – positioning digital infrastructure as instruments of war.

This raises a difficult but necessary question for Malaysia, particularly as it accelerates data centre development.

To what extent might partnerships with global tech firms indirectly contribute to the ongoing conflicts, including the genocide in Palestine?

The economic rationale is clear, but policymakers must now confront the ethical and geopolitical dimensions.

In an interconnected world, data and cloud infrastructure are not neutral – they can, directly or indirectly, enable conflict.

AI and the collapse of truth

The conflict has shown that the digital battlefield is now as critical as the physical one.

Modern warfare is no longer fought solely with missiles, but through the contest to shape public opinion.

Generative AI has enabled both state and non-state actors to create "hyper-reality" – a flood of high-quality fabricated content that outpaces traditional fact-checking.

Depending on one's perspective, Iran deployed this strategy effectively, exploiting anti-war sentiment in the United States and turning domestic politics into a strategic vulnerability.

Propaganda has evolved into "pop-culture subversion."

Iranian-linked actors produced AI-generated animations using Lego-style characters mocking Western leaders, paired with AI rap in American slang to bypass platform filters and reach younger audiences – reframing the war as a "rich man's war" to avoid the Epstein files scandal.

Chinese state-linked media, meanwhile, produced the AI-generated "Eagle versus Persian Cat" wuxia series, portraying the United States as predatory and Iran as a noble defender, simplifying the conflict for global audiences where Western involvement is framed as the driver of regional instability.

Beyond influence operations, AI has been deployed to erode trust and disrupt command environments.

In March 2026, AI-generated accounts amplified rumours of Benjamin Netanyahu's death following an alleged Iranian strike.

When Israel released proof-of-life footage, it was widely dismissed as a deepfake.

The episode illustrated a new reality: a leader need not be killed to be neutralised, sufficient to be rendered unverifiable.

Iran has also allegedly used AI-generated imagery to exaggerate military success, including fabricated visuals of damaged US carriers, attacks on major cities such as Tel Aviv, Dubai, and captured American soldiers.

Although later denied, these images felt credible enough to shape public perception and fuel anti-war sentiment, potentially contributing to pressure for the April 8 ceasefire on the Trump administration.

For Malaysia, this is a critical warning. As a highly Internet-connected society, it is particularly vulnerable to such "hyper-real" tactics.

In a future crisis – whether regional or domestic, including elections – national stability may depend less on military strength than on the ability to manage an information environment where truth can be manufactured by anyone with an AI prompt.

Malaysia must urgently build both institutional capacity and public awareness to navigate a world where seeing is no longer believing.

This conflict is not just another geopolitical flashpoint – it is a preview of how AI is fundamentally reshaping warfare.

From information operations to digital infrastructure, the line between civilian and military domains is rapidly eroding.

For Malaysia, a small country with growing digital ambitions, this presents both risk and responsibility.

We cannot remain passive. Instead, we must help lead global efforts to govern these technologies – shaping standards, norms, and accountability while contributing to a broader international consensus on their responsible use.

If left unchecked, we may not need to wait for AI to rise against us; we may have finished ourselves off long before that.