Traditional Values, Modern Approach™
Issue#15 I July 2026

WARFARE HAS A NEW FACE, AND IT'S POWERED BY AI

HOW HYPER-FAST, LOW-COST AI SYSTEMS ARE COMPLETELY UPENDING TRADITIONAL MILITARY MATH, ECONOMIES AND LEGAL FRAMEWORKS

By Thulasy Suppiah, Managing Partner of Suppiah & Partners

The **world's first fully autonomous attack mission using Artificial Intelligence (AI), happened in the fall of 2023**. The Ukrainian Ministry of Défense officially approved the Saker Scout - an autonomous weapon system - **to complete the final strike phase of a mission, completely cut off from its human handlers**.

The system was developed in response to the intense electronic warfare (EW) landscape in Ukraine's eastern Donbas region. Russian forces deployed massive jamming networks, such as the Pole-21 and Zhitel systems, which blanked out the radio and GPS signals Ukrainian drone pilots used to navigate.

The Saker Scout is a First Person View (FPV) kamikaze quadcopter drone. If heavy jamming breaks the connection to its pilot, its onboard computer-vision software fully takes over to identify, track, and detonate on military targets without human intervention.

Militaries are constantly looking for flawless partners in war, and they may have found it.

The Spark of a New Revolution

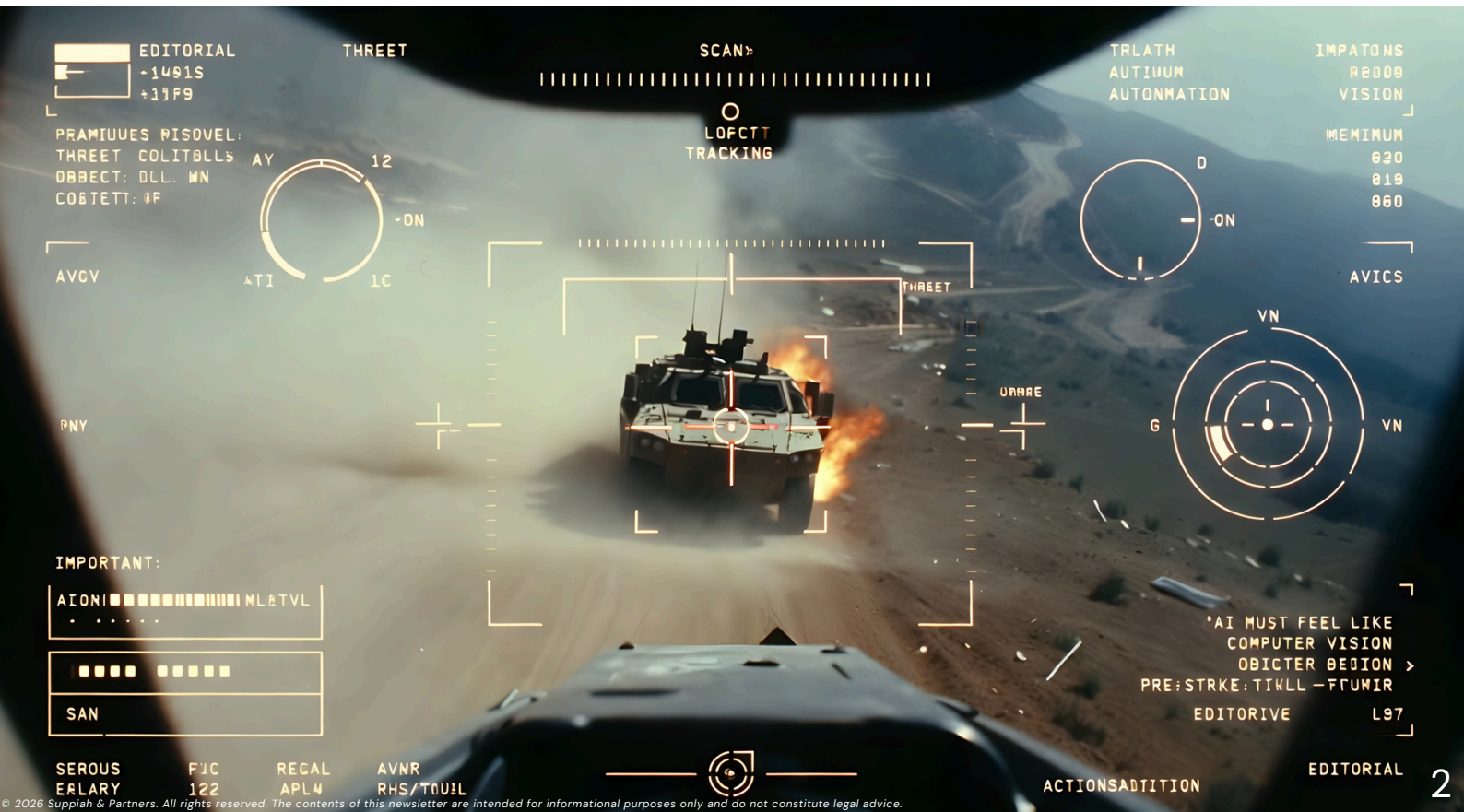
The integration of AI into military hardware has sparked a third revolution in warfare. Unlike the nuclear arms race, which relied on building expensive stockpiles, the AI arms race is defined by software, processing speed, and the mass production of cheap, autonomous systems.

By using Decision Support Systems (DSS) such as the Pentagon's Maven Smart System integrated with advanced large language models, forces can process massive amounts of targeting data in minutes rather than days. This efficiency has triggered a global rush to develop AI-based targeting weapons, pushing global military spending to $2.88 trillion (RM 11.38 trillion) in 2025—a 41 per cent increase over the last decade.

The real-world impact of this technology was demonstrated during the recent United States war against Iran. Powered by AI-driven DSS, the US hit more targets in the first four days of the campaign than it did against ISIS over an entire six-month period. In total, the US struck 13,000 targets in just 38 days, including thousands of command centres and air defences. While these systems promise unprecedented tactical results, **their speed and automation raise troubling ethical questions**.

The Fundamental Problem

Today's arms race is uniquely destructive because cheap, asymmetric technology (like inexpensive drones) forces defenders to buy increasingly complex, multi-million-dollar countermeasures. This **locks nations into an unsustainable economic spiral where billions are spent defending against cheap threats**, completely freezing capital needed to solve existential global crises.



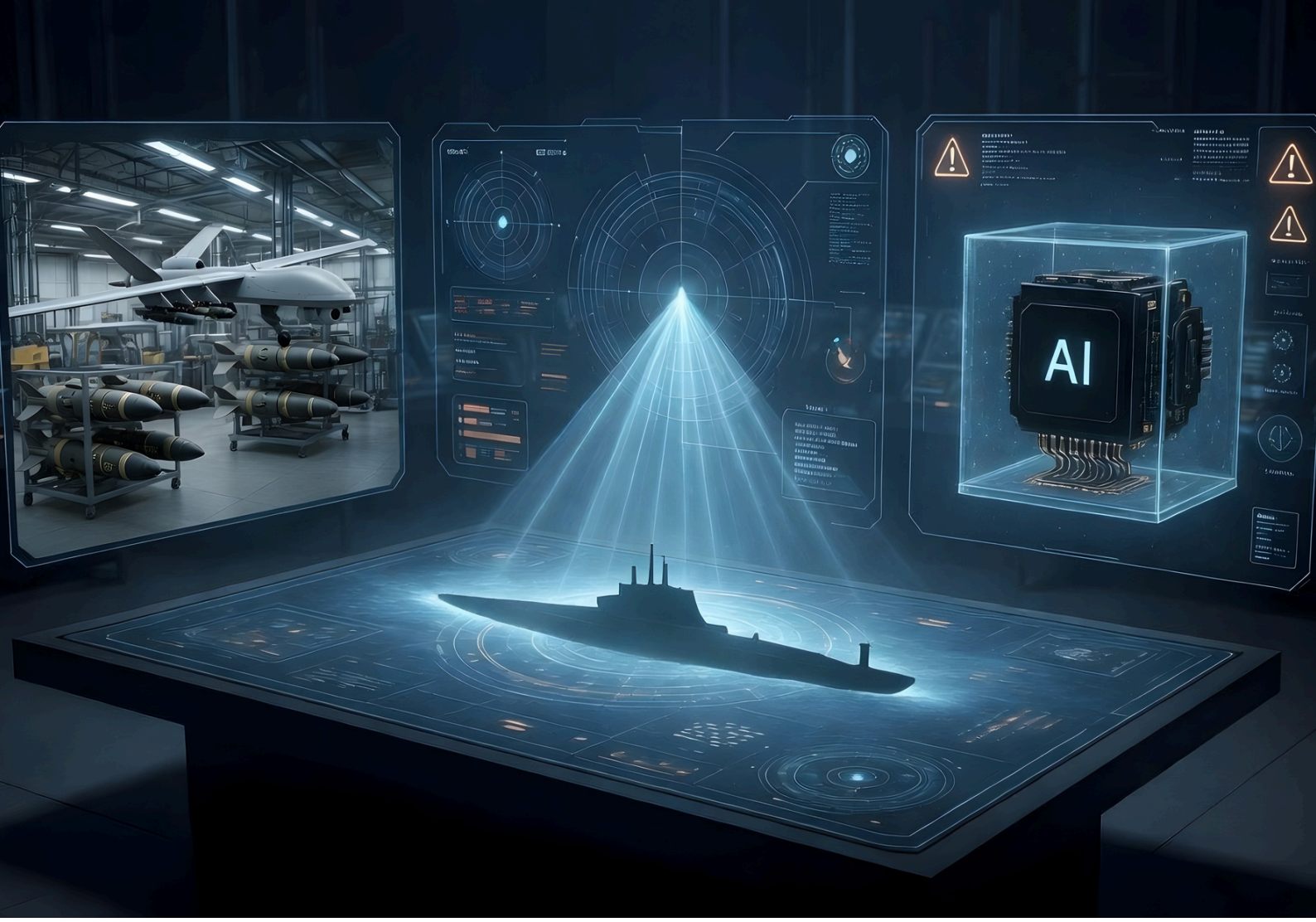
The direct diversion of capital from human welfare to weapons is a primary ethical critique of military spending as just a fraction of this, roughly USD$150 billion to USD$200 billion (RM593 billion to RM791 billion) annually, could eradicate global hunger, provide clean water, and fund universal primary education.

Additionally, traditional military targeting involved rooms full of human intelligence analysts manually comparing satellite photos with radio log. It's a process that takes hours, days, or weeks. The AI **compresses this OODA (Observe, Orient, Decide, Act) Loop into seconds**.

When systems process data instantly, the quantity of targets skyrockets. The resulting dilemma? The logic shifts from human-driven intuition to machine-driven pattern recognition. If a human analyst is handed 500 machine-generated targets a day rather than 5, they no longer have the time to deeply question the data. This creates a severe risk of automation bias where human operators simply trust what the algorithm tells them, treating a highly complex probability estimate as an absolute fact.

Finally, the concept of **faster escalation cycles due to machine-speed reactions** describes a dangerous military feedback loop. When opposing militaries both deploy AI to make decisions, the speed of conflict shifts from human speed (minutes, hours, or days) to algorithmic speed (milliseconds).

What happens if one AI system misinterprets an action and reacts instantly? The opposing AI will react to that reaction just as quickly. Before human commanders can even figure out what is happening, a minor misunderstanding can spiral into a major conflict.



ETHICAL AND STRATEGIC RISKS

The new global AI arms race is making the world much more dangerous in three simple ways. First, it creates a **stockpile problem**: because AI can find thousands of targets in seconds, armies are rapidly running out of real-world missiles and drones to actually hit them. This forces factories into a frantic race to build more weapons. Second, it **destabilises hidden defences**: because AI can instantly map out an enemy's hidden bases or submarines, countries feel completely exposed, forcing them to build thousands of fake decoys and extra weapons just to survive a surprise attack. Finally, it **breaks peace treaties**: traditional peace deals only work when you can count an enemy's tanks or ships on a satellite map, but you cannot count or see a hidden AI computer code, making it almost impossible for nations to agree on safety rules.

Today, global stability no longer rests on how many weapons a country possesses but on **who has the fastest data networks and the most aggressive code**. In the current environment, every military power feels deeply exposed, creating intense, unremitting pressure to strike first before the enemy's algorithm beats them to the punch.

As the Australian Institute of Internation Affairs noted, “A world where no one feels safe cannot be stable. It is not in the national interest of any state to create an environment of continuous arms racing and nuclear buildup.”

IMPACT ON SMALLER OR LESS POWERFUL NATIONS

AI tools (especially open-source models and commercial drones) make it easier for smaller states - or even non-state actors, to develop meaningful military capabilities. This has caused a **cost asymmetry advantage**. Across the region, inexpensive drones and missiles are forcing the US and its Gulf partners to expend their most sophisticated, high-cost air defences.

While an Iranian Shahed-136 one-way attack drone costs a mere USD$20,000 to USD$50,000 (RM79,092 to RM197,730), intercepting it frequently requires multi-million-dollar munitions. A single Patriot interceptor costs roughly USD$4 million (RM15.82 million), while a THAAD missile ranges from USD$12 million to USD$15 million (RM47.46 million to RM59.32 million). That over 200 Ukrainian specialists are now advising the US military on how to intercept Iran's Shahed drones without firing Patriot missiles that cost 200 times more, proves that the era of modern drone warfare has arrived - and the US is lagging behind.

Iran does not just use these weapons directly; it exports the low-tech blueprints, commercial components, and localised manufacturing capabilities to non-state proxies like the Houthis in poverty-stricken Yemen and militias in Iraq. Using Iranian-supplied, low-cost drone and anti-ship missile kits, the Houthis successfully disrupted global shipping lanes for years.

Iran is also able to frequently bypass sanctions because the components they require are entirely civilian. Recent intelligence disclosures showed the Islamic Revolutionary Guard Corps (IRGC) using front companies in global trade hubs to procure commercial Chinese satellite communication gear and antenna accessories.

By integrating commercial guidance systems with open-source machine learning models, Iran can upgrade unguided rockets into precision-guided weapons without needing a multi-billion-dollar military-industrial complex.

AI in warfare reshapes the global balance in ways that sometimes place smaller or developing countries at an advantage. However, top-tier AI systems still require infrastructure, talent, and data - areas dominated by countries like the US, Russia and China.

INCREASED VULNERABILITY THROUGH AUTOMATED THREATS

Automated cyberattacks have eliminated human fatigue by operating continuously at scale, requiring only a single success to breach networks at zero cost to attackers. This dynamic severely disadvantages smaller economies. They lack the budget and expertise to counter autonomous algorithms that scan public infrastructure and exploit flaws faster than human defenders can patch them. A striking precedent occurred between December 2025 and February 2026, when a lone hacker bypassed the safety filters of commercial models like Claude Code and GPT-4 to deploy over 5,000 automated commands against Mexico. This single AI-driven campaign rapidly exfiltrated 150 gigabytes of data, compromised the identities of 195 million citizens, and breached the federal tax authority, to prove that outdated state networks are utterly unable to cope with the velocity of modern AI intrusions.

CASCADING INFRASTRUCTURE RISK

Critical infrastructure like banks, power grids, and satellite communications increasingly relies on interconnected third-party software. This leaves less-protected nations with systemic exposure. While a fully autonomous, purely AI-generated supply-chain attack has not yet been publicly documented, a landmark precedent exists: the 2017 NotPetya cyberattack. State-sponsored hackers hijacked a mandatory Ukrainian accounting software update (M.E.Doc), and unleashed a destructive data-wiping worm. Within hours, the infection spread globally via interconnected corporate networks. It crippled shipping giant Maersk, froze multinational logistics and pharmaceutical systems, and disabled radiation monitoring at Chernobyl. It resulted in USD$10 billion (approximately RM39.7 billion) in global damages.

NotPetya remains the most destructive cyberattack in history and offers a terrifying blueprint if augmented by AI.

DEPENDENCE ON EXTERNAL TECHNOLOGY

Many nations lack the domestic infrastructure to build sovereign artificial intelligence models, forcing them to rely on AI ecosystems developed by foreign tech giants. This creates dependency, transforming commercial software agreements into national security risks. As AI models function as black boxes hosted on external cloud servers, client states have zero visibility into the underlying source code. This exposes them to structural vulnerabilities, such as digital backdoors, intentional data exfiltration, or sudden supply-chain termination. If geopolitical tensions flare, a foreign provider can

simply cut off access to the cloud infrastructure, instantly blinding a nation's automated logistical, banking, or administrative networks.

Following international sanctions stemming from the war in Ukraine, major Western tech giants such as **Microsoft, Amazon Web Services (AWS), Google Cloud, and enterprise software giant SAP,** systematically cut off access to their cloud platforms in Russia. Tens of thousands of businesses and organisations were given strict deadlines before their data access was permanently terminated. Amidst the chaos, businesses were forced to migrate to inferior domestic software alternatives.

Another stark example of strategic supply-chain termination, is the US using export controls to cripple its adversaries' AI capabilities. Washington forced Dutch firm Advanced Semiconductor Materials Lithography (which monopolises advanced chip-lithography machines) and the Taiwan Semiconductor Manufacturing Company (the world's largest advanced contract chipmaker) to instantly halt sales and servicing to Chinese tech companies and data centres. Consequently, nations dependent on Western-licensed hardware were frozen out of the computing power required to build or maintain cutting-edge AI models. It exposed the extreme risk of relying on a supply chain controlled by a foreign superpower.

ECONOMIC TRADE-OFFS

Governments with constrained budgets must balance the exorbitant cost of investing in AI defence capabilities against immediate domestic needs like healthcare, education, and economic development. AI infrastructure requires massive capital investments in high-performance data centres, microchips, and specialised tech talent. Funding such systems starves essential public services. But to focus resources entirely on social infrastructure creates compounding military risks.

This leaves developing countries trapped in a brutal financial tug-of-war. For example, Kenya recently had to choose between spending its limited cash to fight a massive wave of cyberattacks, or funding schools, hospitals, and food amidst public protests over the

high cost of living. If a government picks cyber-defence, its citizens may riot over the lack of public services. But if it ignores the cyber threats, hackers can instantly freeze the country's banks and power grids. This leaves poorer nations in a dangerous loop: they cannot afford to buy modern AI defences, but they cannot afford to ignore them either. Truly, modern AI-driven rearmament forces developing economies into a destabilising financial paradox.

EXPOSURE TO INFORMATION WARFARE

According to the World Economic Forum's Global Risks reports, **mis- and disinformation** are now ranked among the highest short-term global threats precisely because they allow cash-strapped or isolated regimes to strike at the societal core of democratic nations for pennies on the dollar.

Imagine if a bully didn't have to fight you physically, but could instead instantly whisper a different, perfectly tailored lie into the ear of every kid in school to make them turn on each other. That is exactly what AI-driven information warfare does on a global scale.

By using advanced AI tools, bad actors or rival countries can create incredibly realistic fake videos, audio clips, and social media posts for almost zero cost. Instead of trying to convince everyone of one big lie, they create a **digital fog** of thousands of small lies designed to target specific arguments people are already having. This makes it impossible for citizens to agree on what is actually real.

While big, wealthy countries have the money and technology to build digital shields to spot and flag these fakes, smaller or less-developed nations often do not. They might not have strong local news stations to double-check the facts, or the right laws to police social media networks. As a result, an attacker can cheaply throw an entire country's elections or government into total chaos without ever using a real weapon.

REGULATORY AND GOVERNANCE CHALLENGES

Smaller nations face severe regulatory and governance challenges in the age of AI, primarily operating as rule-takers rather than rule-makers. As global frameworks and compliance standards are dictated almost entirely by major powers and supranational bodies like the European Union or NATO, smaller states are forced to adopt external regulations that may not align with their domestic interests. Further, politically fragile states frequently lack the internal institutional capacity and legal frameworks required to regulate and secure AI within their own national defence sectors, leaving them structurally dependent on foreign superpowers.

CONCLUSION

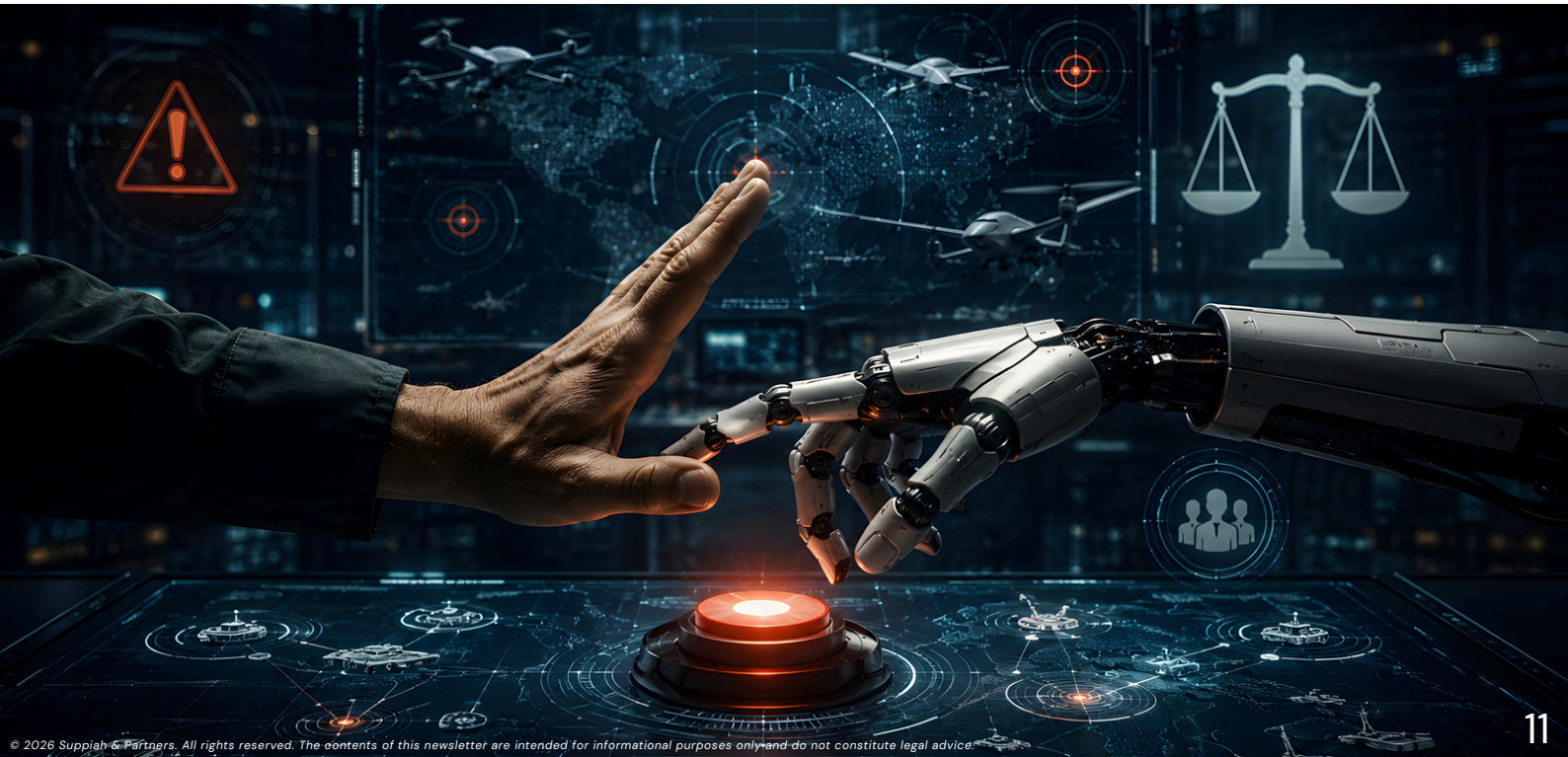
The idea of introducing thinking machines into war is not new, and attempts have been made by militaries since World War II with little result. Then, innovations in microchips made it possible to introduce microprocesses into military weaponry. This resulted in precision guided munitions that could hit targets on their own once fired but also in systems that could fire automatically. Many US-built legacy systems, such as the Navy's Close-In Weapon System (CIWS), smart anti-ship mines, and the Army's Patriot Air Defence System, can engage targets autonomously once activated. Yet, none contain AI, and no one would accuse them of "thinking". Their logic is entirely predictable, and they operated for decades without triggering global alarm.

Now, something has changed. The inclusion of AI into military systems has shifted the paradigm from mere automation to true machine autonomy, enabling weapons to select, track, and engage targets using algorithms that operate beyond direct human oversight and predictability. This is immoral and a grave threat to national and global security. As algorithms are incapable of comprehending the value of human life they should never be empowered to decide who lives or dies.

The United Nations Secretary General António Guterres agrees that "machines with the power and discretion to take lives without human involvement are politically unacceptable, morally repugnant and should be prohibited by international law."

Allowing algorithms to decide when to use lethal force also raises significant questions about who is ultimately responsible and accountable.

What's scary is **experts - including the heads of OpenAI and Google DeepMind - have warned that Artificial intelligence could lead to the extinction of humanity. Dozens have supported a statement published on the webpage of the Centre for AI Safety**.



Top AI-driven systems currently in use for military operations:

- **Intelligence, surveillance, and reconnaissance (ISR)**: When the US and Israel struck Iran in February 28 this year, it marked the first time in history, the entire architecture of a major interstate conflict, from intelligence fusion and target generation to post-strike battle damage assessment, was fundamentally governed by AI. It used a special military method called ISR. Instead of humans doing all the spying, an AI system was used to scan through thousands of satellite pictures, radio signals, and internet posts every single second. The AI combines all this massive information into one live, unified digital twin, which is like a giant 3D computer video game map that mirrors everything happening at that exact moment. By constantly watching this digital map, the AI can automatically spot strange patterns or dangers that humans might miss, giving commanders a superpower called situational awareness so they always know what the enemy is doing. The computer doesn't just watch; it also uses predictive analysis to guess what the enemy will do next, and picks out the best targets for military strikes. Once the mission is over, the AI looks at new pictures to check if the job was done right. Computers are now helping to plan and guide almost every single step of a modern war.

- **Cyber Warfare**: Automated threats or cyberattacks executed independently by software scripts, bots, or AI algorithms rather than human operators. As they operate continuously and at scale, they strip away human fatigue, allowing attackers to fail 99.9% of the time at zero cost. Only a single success is required to breach a network.

- **Unmanned Ground Vehicles (UGVs)**: Platforms like the THeMIS (Estonia) or Uran-9 (Russia) patrol hostile terrain, clear mines, and engage targets with mounted weapons.

- **Unmanned Aerial Vehicles (UAVs)**: Remote-piloted drones like the MQ-9 Reaper (US) are built for long-endurance global surveillance and precision strikes.

- **Unmanned Underwater Vehicles (UUVs)**: Iran has introduced UUVs such as the Azdhar autonomous torpedo. Fuelled by quiet lithium-ion electric propulsion, these low-cost submersibles can patrol underwater for days, waiting to lock onto the hull pixels or acoustic signatures of passing tankers. Because they are incredibly cheap to manufacture compared to traditional submarines, Iran can deploy them in large numbers, making detection and clearance a costly nightmare for foreign minesweepers and anti-submarine units.

- **Lethal Autonomous Weapons Systems (LAWS)**: In seeking a battlefield advantage, Ukraine's weapons developers deployed the world's first operational LAWS to execute mission-critical strikes independently. Instead of managing every tactical step manually, a human commander simply issues a high-level directive, such as "destroy the target". The AI then automatically generates and executes a complex checklist of tasks, controlling multiple military assets simultaneously at blistering speed.

- **Humanoid Military Robots**: Bipedal, AI-driven machines are designed to mimic human soldiers. Whilst still in development by firms like Ghost Robotics (US) and Unitree (China), they represent the next frontier in combat tech.

- **Military robots**: Machines designed to support or replace soldiers in combat, reconnaissance, logistics, and other defence roles. These robots range from simple bomb-disposal bots to advanced AI-powered systems capable of decision-making on the battlefield. They reduce risk, extend operational range, and take on tasks too dangerous for humans.

- **Decision Support Systems (DSS)**: Most notably platforms like the Pentagon's Maven Smart System integrated with advanced large language models (like Anthropic's Claude or specialized tools from Microsoft, Amazon, and Google). These systems act as hyper-advanced data fusion engines. They ingest a chaotic, overwhelming torrent of raw battlefield intelligence simultaneously, including: Live drone video feeds, satellite radar and imagery, intercepted electronic communications and radio signals and local geography and historical troop movements. The AI sifts through this massive mountain of data in seconds. It automatically flags anomalies, identifies hidden structures, translates languages, classifies vehicles, and links separate puzzle pieces together.

REFERENCES

- Mutually Automated Destruction: The Escalating Global A.I. Arms Race
- Robot Soldiers Could Make Wars Deadlier—And China Is Already Building an Army
- What are military robots? Types, examples & the future of warfare
- New Frontiers and Innovations in the FPV Drone Wars - Inside Unmanned Systems
- How AI-enabled Targeting Could Intensify Global Arms Competition
- Homepage - Autonomous Weapons Systems
- Slaughterbots are here.
- Global military spending hit record high in 2025 | NHK WORLD-JAPAN News
- Record military spending threatens global peace and development, new UN report warns
- How AI protects critical infrastructure from emerging global threats
- The Mexican Government Breach Reveals What Attackers Can Do With AI Tools
- NotPetya: The Most Expensive Cyberattack in History
- Microsoft says Russian companies will be forced off its cloud services within days
- Education, health lose as defence wins in 2025/26 budget
- Cognitive manipulation and AI will shape disinformation in 2026. Here's how to build resilience
- Electoral Commission launches deepfake detection pilot to counter AI misinformation Posted
- The New Battlespace: How Geospatial AI Is Reshaping Military Intelligence

SUPPIAH & PARTNERS
since 2007

Traditional Values, Modern Approach ™

Issue#15 I July 2026

+603-4142 3766

https://suppiahlaw.com/

thulasy@suppiahlaw.com

UG-13, LEXA Galleria,
No. 45, Jln 34/26, Wangsa Maju,
53300 Kuala Lumpur

PREVIOUS NEWSLETTERS