

Picture credit: Livewire

SMALL SYSTEMS, BIG ADVANTAGE

Dan Gardner *explains why low SWaP will define modern warfare*

The ongoing conflicts that are still continuing in Ukraine and the Middle East have shown the world that modern warfare is undergoing a profound transformation. The era of relying on a handful of high-value platforms is giving way to one defined by distributed, networked systems operating at scale. At the centre of this shift are low SWaP (Size, Weight, and Power) technologies, which are increasingly becoming a critical enabler of true multi-domain operations (MDO).

As defence moves beyond siloed domains of air, land, sea and space, the ability to coordinate across all environments in real time has become essential, particularly under contested conditions. However, the widespread use of drones, sensors and satellites means that virtually anything generating a signal – from radar emissions and communications traffic to physical movement – can now be detected, tracked and targeted. The war in Ukraine has demonstrated this with brutal clarity; if you can be seen, you can be hit.

Low SWaP systems offer a fundamentally different model for operating in this environment. Their reduced size and power requirements allow forces to deploy large numbers of smaller nodes rather than depend on a few vulnerable platforms. This creates resilience through distribution. If one node is lost, the wider network continues to function. Capability degrades gracefully rather than catastrophically and systems can be replaced or reconstituted quickly.

Crucially, interoperability is no longer simply a software challenge. It has become a SWaP-driven capability. Smaller, distributed systems allow sensors, communications, and electronic warfare tools to be integrated in ways that were previously impractical. The result is a far more agile and survivable force structure.

CONTINUOUS CROSSCHECKING

At the heart of this transition lies a new understanding of resilience. A single sensor can be deceived but a distributed network is far harder to manipulate. Instead of spoofing one radar or jamming one communication link, adversaries must now contend with multiple interconnected nodes continuously cross-checking and validating what they observe. If one system detects a potential threat, others can confirm or challenge it in real time, preventing false signals from taking hold.

But in an ever-evolving modern warfare world, systems must go even further. They need not only to survive deception and jamming, but to exploit them. Electronic attacks themselves become valuable intelligence sources, revealing clues about an adversary's intent, capabilities, and potentially even position. Sophisticated techniques such as Digital Radio Frequency Memory (DRFM) deception, where radar signals are captured, modified and replayed to create false targets, highlight the complexity of the threat. But they also reinforce the need for systems capable of recognising, interpreting, and adapting to interference in real time due to adaptive signal processing and cognitive radar techniques.

This is no longer theoretical. In Ukraine, for example, both sides are already engaged in a constant battle of jamming, spoofing and electronic deception, with systems rapidly adapting frequencies, waveforms, and tactics in response to enemy interference. Electronic attack has become a daily feature of the battlefield, forcing operators to continuously evolve how sensors, drones and communications systems survive and function in contested environments.

ON THE EDGE

This evolution is being accelerated by advances at the edge. Processing and decision-making are no longer confined to centralised command systems; they are pushed out to individual nodes. That means local systems can react immediately to changing conditions without waiting for direction from higher headquarters. The network becomes not only more resilient, but crucially, more adaptive.

The defence sector has spent decades pursuing exquisite capability at the expense of scale. But the principle that 'good enough' Technology Readiness Levels matter more than technical perfection signals a correction: systems built on commercial hardware, designed to be lost and replaced, can deliver operational effects that a small number of high-end platforms cannot. Not because they are better individually, but because they can be fielded in numbers, updated rapidly and reconstituted when destroyed. In an era of attritional warfare, cost and replaceability are becoming operational advantages in their own right.

Overlaying all of this is the growing dominance of the electromagnetic spectrum. Jamming, spoofing, and electronic attack are no longer exceptional events; they are constant features of modern conflict. Communications and GNSS can no longer be assumed to be reliable or even trustworthy. Forces must therefore be designed to operate effectively in denied environments and, increasingly, to extract advantage from them by turning fragmented or contested signals into actionable understanding.

SUCCESS IN MODERN WARFARE NO LONGER DEPENDS SOLELY ON POSSESSING THE MOST ADVANCED PLATFORM. INSTEAD, ADVANTAGE BELONGS TO THOSE WHO CAN ADAPT FASTER THAN THEIR ADVERSARY

The implications are significant. Success in modern warfare no longer depends solely on possessing the most advanced platform. Instead, advantage belongs to those who can adapt faster than their adversary. Software updates, tactical adjustments and electronic warfare responses must evolve continuously and often in near real time. As a result, warfare has become a contest of learning speed as much as firepower.

FALSE SIGNALS

Deception therefore takes on even greater importance. A convincing false signal can force an opponent to reposition forces, expend scarce munitions or commit resources against a non-existent threat. Warfare becomes as much about shaping perception as destroying capability. In this environment, the margin for error is razor thin.

This is where low SWaP matters. Not as a technology category, but as an enabler of a different force design, one that treats distribution, adaptability, and speed of learning as primary measures of advantage. That means designing systems from the outset to be networked, attritable, and rapidly upgradeable, rather than retrofitting those qualities into platforms built for a different era.

Critically, low SWaP systems shift the economics of warfare. Their lower unit cost enables mass deployment and creates cost-imposition dilemmas for adversaries, where relatively inexpensive systems force disproportionately expensive responses.

The forces that get this right will not necessarily have the most sophisticated kit on the battlefield, but they will have the most difficult networks to break. ●

The advantage in modern warfare belongs to those who can adapt faster than their adversary

Dan Gardner is Technology Solutions Lead for Defence and Security at Plextek.