Picture credit: US Dept Defense

BE PREPARED

Matt Medley *explains the four areas of the defence industry that will be impacted the most over the next 12 months*

Military supply chains have been impacted heavily due to the increase in conflicts in 2023, as a result inventories and resources of some military forces are becoming inadequate to combat enemy forces. Due to this, global defence budgets will increase in 2024—with the UK budget increasing by £5-billion and the US defence budget rising by 3.2 percent to $842-billion in 2024 from $816-billion in 2023. A lot of these budgets are expected to be spent on improving asset production to help military forces regain control of their supply chain, this will result in the global defence market growing significantly.

The manufacturing sector is part of the conundrum as to the increase in defence budgets as identified in a Deloitte report on supply chain risk management which highlights: "As most A&D suppliers are highly specialised with unique expertise and complex equipment, they struggle to make quick changes to production in response to varying demands. The challenge is accentuated as many suppliers serve both commercial aerospace and defence. Any spillover risk from commercial aerospace could leave defence OEMs vulnerable to sourcing critical parts for their programmes and platforms." The majority of the 2024 defence agenda will be dominated by rising budgets and increased procurement – with this in mind these are the four areas I see a large percentage of the budgets being spent on.

Prediction 1: Total Asset Readiness must improve to help military forces as the spectrum of conflict widens. The last 12 months have given rise to a wider spectrum of conflict. The combat between Ukraine and Russia shows symmetric features, as its between traditional air, military and naval forces on both sides trying to achieve dominance and territory. On the other end of the spectrum, a more modern asymmetric style of combat can be seen in the Israel and Hamas conflict which features combatants that are not typically a part of military forces of nation-state.

The difference in features of warfare has called for defence ministries and departments to better prepare for a broader spectrum of eventualities

The difference in features of warfare has called for defence ministries and departments to better prepare for a broader spectrum of eventualities – from natural disasters to full-scale theatre warfare. As well as a broad spectrum of military deployments ranging from high to low tech – tanks, boats and boots on the group versus parasailing and jet skis, remote locations versus heavily populated areas with schools and hospitals.

As highlighted in a recent Global Security Review essay, which paints a picture of the new challenges defence forces face and advocates for an agile approach to be taken towards The Changing Face of Conflict: "The agile approach to hybrid warfare offers a promising framework for responding to these complex and evolving threats. It emphasises flexibility, adaptability and rapid decision-making and incorporates the impact of technological developments on warfare."

This will even apply to the software infrastructure underpinning the military equipment supply chain, where disparate reporting mechanisms and software systems can be consolidated with an all-encompassing solution to track Total Asset Readiness – giving commanders a clear real-time view of the assets at their disposal, in the context of the mission they need to complete, wherever and whenever they are deployed. From this we expect to see an 16.3 percent increase in total defence spending in the US alone, with the IT spend in defence contractors rising from 3 percent of revenue up to around 5 percent of revenue as they invest heavily in AI and automation to help pursue optimised asset management and other technology-driven priorities.

Prediction 2: changes required to defence industrial bases as recent conflicts highlight lack of readily available assets and inventories. A radical re-think is required for Total Asset Readiness, as the conflict between Ukraine and Russia has highlighted the lack of assets, ammunition, vehicles, and inventories available to military forces in combat. This comes despite the mass investments made in ammunition and inventories by supporting countries. Current defence industrial bases (DIB) do not have the facilities to match the increase in recent demand as production rates were set up on non-large scale conflict replenishment. DIB expansion has never been so important!

This has been recognised by defence forces as for the first time ever the DoD is set to release a defence industrial base policy in late 2023. The policy outlines four key focus areas: building a resilient supply chain, improving workforce readiness, increasing flexible acquisitions, and economic deterrence. The US is not alone here. The UK military has also refreshed its defence strategy as it will reallocate £2.5-billion to bolster the ammunition stockpiles as it aims to increase military power and agility.

New manufacturing principles are likely to play a key role. The US Army is already looking at logistics and readiness as the service examines more opportunities to boost those operations by using advanced manufacturing technologies such as Additive Manufacturing and 3D printing technology to improve and sustain readiness as highlighted in a recent Janes report. As we move forward in response to the US DoD policy focusing on building a resilient supply chain, improving workforce readiness, increasing flexible acquisitions, and economic deterrence – I expect significant flow down requirements to begin quickly appearing in over 50 percent of all new defence contracts, as well as allied nations following suit with their own similar directives, requiring DIB organisations to transparently demonstrate supply chain resilience for not only themselves, but their suppliers as well. Due to the current munitions shortages with allies supporting ongoing global conflicts, that number will approach 100 percent for munitions suppliers.

THE FLIP SIDE OF THE AI BOOM HAS BROUGHT ITS OWN CYBER THREATS WITH AI-ENABLED HACKERS

Prediction 3: 2024 will see the rise of autonomous low-cost 'swarm' drones take to land, sea and air. As evidenced by recent conflicts, drones will continue to step up to the military plate and they are not alone, but in swarms. Drones can be produced quickly, cheaply and have a range of features ranging from carrying out surveillance missions in previously dangerous areas to even carrying out light attack missions without putting warfighters at risk. As a result, they are becoming more prominent in military fleets and adoption rates are rising.

Drones are also hugely desirable for defence forces as they can be deployed on air, land and sea making them very versatile. Enter the drone carriers, such as the Royal Navy's HMS Prince of Wales, which they aim to house drones on to be able to transfer assets and supplies to and from vessels without requiring any manned vehicles. As an even cheaper alternative some nations such as Turkey with their TCG Anodolu vessel and Iran with two old merchant container ships are converting previously manned vessels into drone carrying vessels.

The US DoD is also seeing the benefit of swarm drones, as seen when the Deputy Secretary of Defence Kathleen Hicks announced the 'Replicator' initiative at the 2023 Defence News Conference. The initiative aims to quickly build and field swarms of low-cost air, land, and sea drones or All-Domain Attributable autonomy (ADA2) that are able to swarm hostile forces. The DoD aims to have these ready for deployment in the next 18-24 months. These ADA2 assets will help military forces overcome and overwhelm threats that are posed by large assets hosted by enemy forces, the drones will use Artificial Intelligence to autonomously 'swarm' enemy forces.

Effective equipment alternatives such as a drones will be the way forward in 2024 as military powers seek to keep costs low and maximise budgets – while reimagining the concept of mass in the sea/air/land battlespace.

> THE UKRAINE CONFLICT HAS HIGHLIGHTED THE LACK OF ASSETS AVAILABLE TO MILITARY FORCES

Prediction 4: cyber security forces to fight AI with AI. The increase in use of autonomous vehicles and digital technologies comes with heightened vulnerabilities to cyber attacks across the military supply chain. As seen in a Deloitte report: “National security concerns elevate the importance of data security for defence manufacturers. They share and exchange covered defence information (CDI) and controlled unclassified information (CUI) on program specifications, technology and equipment performance as they collaborate across research, design, development and deployment of defence products.”

The flip side of the AI boom has brought its own cyber threats, with AI-enabled hackers. AI has allowed for hackers to carry out cyber attacks at much larger scales, quicker with increased anonymity. AI accelerates malware and changing codes making it harder for threats to be detected.

We must fight AI with AI. An AI-enabled defence can enable cyber security to stay one step ahead of hackers. Machine Learning technologies can be implemented by defence forces to boost threat detection accuracy and quickly automate responses to cyber attacks.

It is more important than ever for all organisations connected to the military supply chain to have penetration tested underlying cyber security software, which can react quickly to prevent data breaches. Many forces have already been deploying cyber defence tools as seen in a recent European Defence Matters report, which reported that some autonomous cyber defence tools using intelligent agents already exist today, monitoring network activities and ready to trigger immediate action when anomalous behaviour is detected. Early malware detection, crucial for cyber risk mitigation, is considered a high-potential activity in which autonomous systems could excel in the future.

In the year ahead I expect to see defence forces exponentially increasing their use of autonomous agents and specialised digital artefacts to enhance cyber defence, as seen with the Defence Information Systems Agency looking to immediately expand its use of AI-driven tools to automate penetration testing on defence networks.

The year ahead will bring growth opportunities for the defence industry, powered by an increase globally in military spending as forces aim to revolutionise their capabilities and assets. A plethora of factors are expected to drive this growth, involving a wider spectrum of conflict, asset and inventory readiness will be tested, and a surge in innovative equipment such as low-cost ‘swarm’ drones. The increased use of digital technologies will put pressure on cyber security to improve – but overall 2024 is shaping up to be a growth year for the defence industry and military forces ●

Matt Medley is Global Industry Director, A&D at IFS.

The UK military will reallocate £2.5-billion to bolster the ammunition stockpiles as it aims to increase military power and agility

Picture credit: US Dept Defense