GLOBSEC
IDEAS SHAPING THE WORLD

Helsing

Deterrence on the Eastern Flank

The role of software and AI.

Facing the unthinkable

'We must take bold decisions and demonstrate our commitment to the transatlantic bond.'

Jens Stoltenberg, May 2023.

NATO's Eastern Flank now faces the unthinkable – the very real threat from a Russia deter-mined to re-assert itself and seek new ways to achieve its ambitions in Ukraine. This threat is simultaneously both acute and chronic as Russia will remain a significant military force for some time. The growth of the Alliance has increased the length of the border area which must be resourced to deter and, if necessary, defend. Current force numbers mean this will be impossible through mass alone, munition shortages across Europe means any major defence would be measured in hours rather than weeks or months. Technology must be employed as a force multiplier. Whilst people, effectors and munitions are in short supply, sensors are plentiful. The Eastern Flank can gain a deterrence advantage by leveraging the digital nature of the new equipment covered elsewhere in this paper and generating soft-ware-defined, AI-enabled sensor fusion and targeting cycles that deliver effects faster than is conventionally possible.

Platforms will continue to play a key role. However, most are reaching the limits of what is physically possible whilst their costs spiral upwards. Furthermore, many programmes will face delays, France's Jaguar will not enter service until 2030, five years behind schedule. The UK's Ajax is approaching ten years behind schedule – it is unfortunately common for modern platforms to take a long time to mature. That, and manufacturing capacity for new platforms in Europe has declined since the end of the Cold War, which will further constrain the ability to introduce new hardware and force the Eastern Flank to rely on what equipment it already has.[1] Software-defined capability transformation can be achieved at the pace of relevance by introducing AI-enabled edge processing capabilities onto existing platforms. This type of solution can be scaled with ease because it is platform agnostic. It can also evolve with the threat in ways that physical platforms cannot.

Land

AI enabled integration of sensor-decider-effector kill chains will revolutionise conventional capabilities. In Ukraine, software enablement, through battle management systems like Kro-pyva, has reduced the time taken to conduct an artillery fire mission against unplanned tar-gets by 60% and resulted in an 80% reduction in artillery deployment time.[2] However key parts of the tactical targeting cycle such as detection and localisation are conducted at hu-man rather than machine speeds. Introducing AI into this chain (with a human remaining in the loop) will offer order-of-magnitude gains by amplifying and simplifying ISR feeds and targeting cycles through edge processing. It can, for example, improve the accuracy of initial target coordinates.

Equally, the static nature of the Eastern Flank coupled with the challenge of its size means that it is ideally suited to networked and uncrewed electro-optical sensors deployed around likely avenues of Russian incursion. AI-enabled sensor fusion allows large numbers of sen-sors to contribute to a real-time common operational picture that is free of duplication and can be quickly understood by operators. Furthermore, given the variance of equipment across NATO, software can act as an integrator allowing for interoperability, a crucial factor in successful deterrence. Interoperability is only one of the significant capability benefits that can be measured:

1 Sehphard News team, Christopher Foss, Decisive Edge Newsletter | Land | April 2023. **Decisive Edge Newsletter | Land | April 2023 | Shephard (shephardmedia.com)**

2 **Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022 (rusi.org)**

- Software and AI can accelerate indirect-fire kill chains by automating the detection and geolocation of targets in GNSS-denied environments; prioritising targets and recommending the best effectors to decision makers; and instantly disseminating target information from sensor to decider to effector.

- Munitions savings as artillery fires become far more efficient. Evidence from Ukraine shows that savings of up to 30% of all artillery shells can be made by using AI ena-bled indirect fire using automatic detection, localisation, and fire correction.[3]

- Force multiplication. Force multiplication is achieved by separating the formerly one-to-one relationship between sensor and operator, and effector and operator. In this way, unprecedented scaling is made possible: tasks that were previously conducted at company level can now be carried out at platoon level.

As well as the land domain examples above, significant opportunities present themselves for cognitive electronic warfare in the air, and AI-led improvements to NATO's anti-submarine warfare capabilities.

Air and sea

Russian air defences in Ukraine have proven their efficacy and the VKS its professionalism.[4] It follows that Eastern Flank nations will face a formidable air defence challenge in any con-flict with Russia. Cognitive electronic warfare (C-EW) is one area where AI can be applied to enhance situational awareness, long-term understanding of an opponent's emitters, and generate advanced cognitive jamming solutions against enemy radars. C-EW can be applied as part of a routine upgrade to Eastern Flank combat aircraft, or as an off-board processing capability for strategic analysis of electronic intelligence.[5] It would improve the deterrence posture of Eastern Flank nations by increasing the survivability of their fixed wing strike packages against Russian air defence systems.

Finally, anti-submarine warfare (ASW) is critical to deterring Russia as it protects against the sub-surface element of the country's nuclear forces, as well as Russia's own attempts to intercept and degrade shipping and military vessels in the North Sea, Baltic Sea, and the Atlantic.[6] AI-enabled software upgrades applied to passive sonar can dramatically improve the ability of a sonar operator to understand the sub-surface environment, localise tracks of potential targets, and navigate it safely by significantly reducing the operator load. Similar upgrades applied to ASW sensors across domains would provide order of magnitude im-provements to the ability of NATO ASW fleets to track Russian submarines by improving the real time tracking and detection of targets. This would help deter Russia by demonstrating that NATO's limited ASW assets would be able to scale the human through AI, in order to track and engage its submarines.

In sum

This software-defined stance would bring immediate capability benefit at lower costs and greater pace than traditional defence investment. This is critical as Russia will likely present a threat to the Eastern Flank within three years of breaking contact in Ukraine.[7] It follows that the Eastern Flank nations must take bold action and pursue the advantages of AI-enabled software and edge processing now, or potentially face a renewed Russian force in five years with the same capability potential that they have today.

Contact

Sam Cranny-Evans

thought leader for European defence tech company Helsing. He is a former RUSI Analyst, and before that was the lead analyst of land warfare platforms at the Janes Information Group, he has focused on the technologies that shape modern warfare.

Sam.cranny-evans@helsing.ai

3 https://www.thetimes.co.uk/article/british-network-builds-drones-for-ukraine-to-fight-russia-2dcln069g
4 The Russian Air War and Ukrainian Requirements for Air Defence (rusi.org)
5 Kognitiver Elektronischer Kampf – die gemeinsame Lösung von Saab und Helsing - ESUT - Europäi-sche Sicherheit & Technik
6 NATO's 'Dynamic Mongoose' ASW exercise demonstrates alliance deterrence capability - Armada International
7 RUSI analysts speaking at the RUSI Combat Air conference, 2023.