QINETIQ

Confidence in Chaos: Executive Summary

The role of emerging technology in adapting to meet grey zone challenges

QINETIQ

The role of emerging technology in adapting to meet grey zone challenges

We have identified ten technology areas that can help the West reclaim its advantage in the grey zone via technological superiority, without lowering legal and ethical standards. Front line technology areas are those deployed directly in grey zone competition. Supporting technology areas indirectly assist grey zone operations; aiding the design, manufacture and assurance of front line technologies.

Front line technology areas

AI, analytics and advanced computing

AI's ability to rapidly process massive volumes of data lends it perfectly to situational awareness. By drawing and fusing data from multiple sources, AI can deduce enemy locations and even model predicted behaviours. It can then prioritise the most urgent information for the operator, avoiding cognitive overload.

Cyber and electromagnetic (EM) activities

Hackers working for crime syndicates or hostile nations can target public services and critical infrastructure to inflict economic harm or political pressure. They may also undertake espionage to obtain intel or state secrets. Technological developments can help to mitigate threats, but equally important is an organisation's ability to bounce back from attack: this relies on human training and behaviour. Less known are EM vulnerabilities: comms signals, like Wi-Fi and GPS, can be jammed or spoofed. The result can be just as disastrous as a cyber-attack, but it may be less obvious that an attack is taking place, and thus harder to trace its source. Specialist tech can flag EM attacks, but must be paired with human training for best effect.

Novel systems, weapons and effects

In previous wars, the visual spectacle of ballistic bombardment served as a show of strength, in the tactic known as 'shock and awe'. Using the same approach against aggressors acting below war's threshold may appear wildly disproportionate and could provoke escalation. Directed energy can achieve traditional military objectives, but covertly and deniably. Directed energy also addresses the asymmetric threat posed by militias equipped with inexpensive, improvised weaponry. A ship could expend millions of dollars' of munitions defending against a swarm of cheap explosive-laden quadcopters, or small rigid inflatable boats. Alternatively, a laser weapon could neutralise them at the reported cost of a dollar per shot.

Power sources, energy storage and distribution

Most (if not all) of these technology areas rely on electricity. In some cases this can be drawn from the grid, but other scenarios require highly specialised energy storage and power delivery systems. Directed energy weapons require systems capable of delivering massive bursts of power in a short period. A battery used in the front line must be hardened, and strike a delicate balance between size, weight and power. Another consideration for power provision in the grey zone is how to sustain operations when the electrical grid has been compromised. Organisations need a contingency plan, and should review combinations of batteries, generators, renewables and other sources to keep vital systems online when the mains is out.

Robotics and autonomous systems

In warfare, robots and autonomous systems often do the jobs that humans can't or shouldn't do. But in the grey zone, the use of autonomous systems is far more nuanced: harnessing the collective power of multiple systems to provide greater situational awareness, and an expanded sphere of influence. An autonomous surveillance network may consist of several aerial and ground-based vehicles, equipped with sensors operating on various parts of the spectrum. The sensor data is fused into a single 'map' of activity, which is presented to the operator. Alternatively, with the introduction of AI into the loop, a robot may receive combined data, recognise suspicious activity, and act accordingly. Robotics and autonomous systems also maintain an important role as a deterrent against direct aggression. As hostile nations use A2/AD tactics to keep defending forces out of the region, the ability to monitor and respond at standoff distance is critical.

Secure communications and navigation

Communication lies at the heart of virtually all grey zone operations. But, every movement of information creates a possible threat vector: private channels can be intercepted, navigation signals may be jammed or spoofed. Organisations must maintain the ability to operate independently of public cellular networks, both to prohibit interception and enable continuity in the event of network failure. Similarly, it's important to secure GNSS signals and receivers: to evade spoofing, jamming, and the tracking of receiver locations.

Sensing, processing and data fusion

The key to grey zone advantage is awareness: of adversaries' locations, activities, and intent, and of public sentiment, plus the physical and digital domains where competition occurs. Advances in sensor technology create new opportunities to gather information. Sensors can also be fitted to new platforms, like CubeSats and UAVs, allowing them to collect and transmit data from previously inaccessible locations. However, the true value in new sensor technology can only be realised once data is collected. Situational awareness can assembled from sensor networks in multiple locations and different parts of the EM spectrum. Manually interpreting raw data from these networks is challenging, so information must be prioritised before being presented to the user. AI will play a role here, as will 'smart sensors' that process data at the edge, preserving comms bandwidth and reducing central computing demands.

QINETIQ

Supporting technology areas

Advanced materials and manufacturing

The rapidly-shifting grey zone requires new capabilities to be fast tracked into service. So, the ability to manufacture quickly and at scale is crucial. Accelerating production, whilst responding to changing demands requires factories to be less specialised and more adaptable. Specifications will be moved to factories near to the point of need. Items may also be manufactured via 3D printers on ships or bases. Materials research also plays an important part; in particular, new low-visibility materials for covert assets. There are promising developments in the field of superconductors, with applications in radar, energy management and mine countermeasures, while nanomaterials show promise for sensors and protective coatings.

Human protection and performance

Unexpected human responses can undermine a technology's advantages. New capabilities can't be introduced safely or effectively without first understanding how people interact with them. All new technologies and procedures should be developed with the human in mind, and tested live to expose risks.

Many hostile grey zone tactics exploit human weaknesses to achieve their aims; such as disinformation campaigns that target human biases, or cyber-attacks which exploit poor security practices. Understanding how people respond to such campaigns illustrates how to nullify them, or turn them against adversaries.

Platform and system design and assessment

High-value platforms (like warships and tanks) remain important for conventional deterrence. However, there's a tension between these platforms' long service lives and the need to adapt them quickly to new threats. Modularity must be factored into new designs from the start. The impact of each new module can be modelled via a 'digital twin', allowing the 'real thing' to enter live testing in a more ready state. But a cultural shift is also required. Future design and assessment must occur within a culture of open collaboration and experimentation: governments must increase their risk appetites and defence companies must become less possessive of intellectual property. There must also be a shift from platforms to systems; recognising that hardware is useless without supporting information architectures and equipment.