QINETIQ

Confidence in Chaos: Executive Summary

Common challenges for defence and security

QINETIQ

Common challenges for defence and security

Grey zone tactics don't discriminate between defence and security targets, and neither should the West's responses to such tactics. Western organisations must tackle, in an integrated way, the capability gaps that these tactics reveal - rather than seeing them as discrete challenges to address individually. Below are six of the most pressing challenges of grey zone conflict that are common to defence and security organisations.

Challenge #1:

Creating information advantage

Whilst the West plans for conventional conflict, its adversaries wage a knowledge-based war. Today, a potent narrative has the power to disrupt, confuse, agitate, and radicalise. Separating truth from lies and creating effective counter narratives are key battlefields for victory.

The way to address this is to gather more intelligence, process it faster, and fuse it to create a clearer picture. This can then be used to diffuse adversarial tactics, and underpin informed responses across both security and defence forces. This is how you win the information war.

Challenge #2:

Improving cyber resilience

The scale and sophistication of organised crime is growing, which presents an ever-increasing threat. The job of a cyber-attacker is now made easier by the mix of technologies on which our infrastructure relies. Some is old and some is new. Lots may be located on premises, but more is moving to private, hybrid, or public clouds.

It's becoming harder to maintain resilience when the scale of digital transformation makes the technology picture so fragmented. Technical changes bring huge opportunities, but also usher in new threats.

Challenge #3:

Improving threat detection

As threats have changed, identifying them has become harder. The nature of grey zone campaigns is that they are disguised, so a nation can be engaged in conflict without even knowing it has been targeted.

Early detection is critical. Identifying unconventional tactics requires significant focus. Improvements in information gathering, processing and utilisation could boost Western detection capabilities. This should be combined with a change in Western perception about what constitutes conflict today.

Challenge #4:

Adding covert capabilities

Western forces have successfully achieved conventional deterrence. They must now achieve it in the grey zone. As conflict becomes sneakier, it's not enough to deter adversaries only from open war.

The West needs to increase its ability to expose enemies' clandestine actions, whilst improving its ability to mask its own. This requires an adaptation of conventional assets to improve their covert capabilities through the use of stealth, autonomy and increased information gathering and processing - the use of covert forces to neutralise covert threats.

Challenge #5:

Adapting at pace

Defence and security organisations struggle to adapt quickly enough to the changing threat landscape. The scale and bureaucracy within defence and security forces can make them slow to change. Adversaries, on the other hand, are happy to work with off-the-shelf technology, nimbly adapting as required.

There's a lot that can be done to make Western forces able to adapt faster and with greater impact. This includes adapting some commercial best practice, and increasing the role of experimentation in live environments, pushing innovation from lab to user faster.

Challenge #6:

Introducing new skills

New skills must be continually introduced to counter adversaries' ever-evolving tactics. This is as much about changing the way existing personnel are trained as new recruitment. It means moving away from today's linear process of 'train, deploy, return, train again'. Instead, training must be linked to real operations to ensure it is always relevant.

It is also about extending training beyond the development of conventional 'muscle memory' abilities into more cognitive skills. Training can no longer be about pre-defined tasks. It must evolve to become more about understanding how to deploy existing cognitive skills proactively. If defence and security can cross-fertilise training, both stand to benefit from each other's experience.