QINETIQ

Confidence in Chaos:

Executive Summary

QINETIQ

The emerging growth of Grey Zone threats

The supremacy of traditional security and defence systems has driven adversaries towards alternative methods. These 'grey zone' approaches include a myriad of new threats described by multiple buzzwords, from asymmetric to hybrid and from 5th generation to sub-threshold. All these make up the "grey zone" and explore the widest range of social, political, economic and military instruments available to achieve maximum effect - but without provoking a conventional response, or even being recognised as formal acts of aggression.

Countering this requires significant change in a number of areas – from risk appetite, to the equipment used, and the skills employed. Technology will play an increasing role in each area as nations adapt to fit the way in which adversaries now behave.

The growth of grey zone campaigning

Understanding what has driven the shift can help us identify how best to adapt to grey zone threats. The first driver is the increasing access to emerging technologies. The accelerating transfer of consumer technology from lab to user lowers the bar for entry, providing adversaries with greater reach and making it easier for them to instigate a challenge. The second driver is the emergence of a new world system. Global norms, rules, accords and institutions face increasing challenges. The third driver is the growth of novel domains. The pursuit of political and territorial supremacy takes place on more fronts today than ever before. Two new domains, cyber and space, are starting to rebalance power between large and small actors.

Six major grey zone challenges

Grey zone tactics reveal capability gaps in both security and defence disciplines, which need to be addressed through an integrated strategy dealing with six key challenges. Below we have explored the most pressing challenges that grey zone campaigns pose.

The first is creating the information advantage. Traditional strategies dealt with conventional conflict, but now adversaries use knowledge-based tactics. Separating truth from "fake news" and creating effective counter narratives are now a priority.

Emerging technologies under-funded: Commercial sector continues to outspend on R&D

A report by PwC states that whilst aerospace and defence invested about $25bn in 2018, computing and electronics industries invested almost six times as much. And last year Amazon alone invested $22bn on R&D, nearly 20 times more than the nearest defence company

The second challenge is improving cyber resilience, which remains one of highest priorities for all organisations. There are well known international aggressors online, but a significant and faster-growing threat is serious organised crime.

The third challenge is improving threat detection. The nature of grey zone campaigns is that they are disguised, so organisations can be targeted without even knowing it.

The fourth challenge is adding sophisticated capabilities. As threats become more clandestine, organisations need to increase their ability to expose hostile tactics from adversaries.

The fifth challenge is adapting at pace. Organisations struggle to react quickly enough to the changing nature of threats. Current procurement processes don't help, with the scale and bureaucracy proving a hindrance.

The sixth and final challenge is introducing new skills. Grey zone competition is perpetual and unpredictable. In this environment, training must be linked to real operations to ensure that its always relevant.

Five modes of grey zone hostility

Although the combinations and permutations of grey zone tactics are legion, we have grouped them into five 'modes'.

The first mode is deniability and central to grey zone competition. Adversaries may seek to sabotage a rival's critical infrastructure with methods that can't be traced to the instigator. The second is information operations. There are two separate but complementary elements in an information operations strategy namely the collection and the dissemination of information. The third mode is the use of proxy forces where an aggressor may leverage another nation's forces to achieve its aims. Fourth is economic coercion; there are many ways to exert economic power, or limit that of its rivals. Lastly is territorial encroachment by offering resources to a country under false pretences or even being welcomed in as peacekeepers before gaining control.

QINETIQ

Adapting emerging technologies to meet grey zone challenges

Whilst the nature of grey zone attacks is constantly evolving, QinetiQ's research suggests that there are ten front line technology capabilities that need to be developed in order to mitigate threats.

1 **AI, analytics and advanced computing –** The ability to process massive volumes of data at pace enhances situational awareness. By drawing and fusing data from multiple sources, AI can be used to identify locations and model behaviours.

2 **Cyber and electromagnetic activities –** The cyber domain is a vital front in grey zone competition. Less discussed is the vulnerability of the electromagnetic spectrum. Communications signals, including Wi-Fi and GPS, can be jammed or spoofed for service denial or misdirection.

3 **Novel weapons, systems and effects –** There are a wide range of alternatives to kinetic weapons, but in the context of the grey zone, directed energy is the most relevant.

4 **Power sources, energy storage and distribution –** Most frontline capability relies on electricity. In some cases, this can be drawn from the grid, but other scenarios require highly specialised energy storage and power delivery systems.

5 **Robotics and autonomous systems (RAS) –** In the grey zone, the collective power of multiple systems to provide more granular situational awareness and expand the user's sphere of influence.

6 **Secure communications and navigation –** Communication lies at the epicentre of virtually all grey zone operations. Moving information around is fundamental to building a detailed picture.

7 **Sensing, processing and data fusion –** The key to grey zone advantage is awareness: of adversaries' locations, their activities and intent, of public and political sentiment, and of the physical and digital domains in which grey zone competition takes place.

8 **Advanced materials and manufacturing –** The grey zone's rapidly shifting nature means new capability must often be fast-tracked into service in response to emerging and evolving threats. The ability to manufacture quickly and at scale is therefore crucial.

9 **Human protection and performance –** New capabilities cannot be introduced safely or effectively without first understanding how humans may interact with them. Unexpected human responses can undermine the advantages of technology.

10 **Platform and system design and assessment –** The primary role of large platforms is to act as a deterrent against aggression. However, there is an apparent tension between their long service life and the need to adapt them quickly to tackle changing threats so their core capability must be readily augmented to serve a multitude of roles.

Shifting mindsets to counter grey zone threats

There are some underpinning principles on which to base the implementation of emerging technologies to adapt to grey zone campaigns. If adopted, they will assure these changes for operational use and accelerate the ability to deal with grey zone threats.

Multimillion-dollar defence remains important as a deterrent, but in the grey zone, it must form part of a suite of tactics

Sometimes it provides little advantage against low-cost improvised devices, or other grey zone threats such as cyber-attacks. This asymmetry is laid bare by the case in 2017 when a $3m Patriot missile was used to shoot down a $200 consumer quadcopter drone.

Develop an integrated approach: Grey zone threats don't discriminate, they just seek to achieve their means through whatever channels are most vulnerable. Innovation underpins this approach, requiring a systemic approach to testing and experimentation with a continuous cycle of learning, development and adoption.

Make innovation mission-led: Today's innovation process often leaves the end user without significant input, and the end result fails to deliver. A mission-led approach ensures that all new ideas are driven solely by mission outcomes.

Practice 'positive experimentation': This requires a shift in mindset, one which stimulates a more systemic approach to innovation. A continuous cycle of learning, development and adoption is needed.

Make testing perpetual and dynamic: To match the pace at which threats change, a more dynamic process of testing and evaluation is required.

Encourage an open architecture environment: The current architecture makes it impossible to quickly modify existing assets in order to adapt to grey zone threats. Open architectures could provide the ability to 'plug and play' with new innovation.

Embrace a new training philosophy: Training should be a constant process, not a set piece activity. This allows organisations to continuously adapt to changes in the environment and incorporate new skills into operations.