QINETIQ

Confidence in Chaos: Executive Summary

# The growth of grey zone campaigning

QINETIQ

# The growth of grey zone campaigning

In the last decade, grey zone campaigning has become a recognised threat to Western nations. There are three fundamental global changes driving a significant shift from open warfare to sub-threshold tactics. Below we look at each in turn, outlining their impacts on defence and security doctrine.

## Access to emerging technologies

Commercial organisations currently outspend defence on research and development. Last year, Amazon alone invested $22bn, nearly 20 times more than the nearest defence company in the same period. With this level of investment comes a noticeable change of pace. A faster transfer of commercial tech from lab to user provides adversaries with new ways to challenge conventional Western military might. In particular, access to new comms technologies allows non-state actors to reach critical mass, equip and mobilise very quickly. This allows them to be more effective than their size would ordinarily dictate, and removes the need for the rigid command and control infrastructures on which the West still relies. Whilst Western nations are reluctant to move on from the systems and tools that won the Cold War, opponents embrace emerging technology. Adversaries of any size can now employ a broader range of sophisticated tactics that are often based on commercially-available technologies. And, because many of these technologies aren't designed for military application, they are well suited to disguised use. So, the question for the West today isn't "how do I develop new technology?" it's "how do I adapt to take advantage of what's already commercially available, and keep up with new developments?"

## The emergence of a new world system

The world order is changing. The existing rules-based international system, along with current norms and institutions, have been under increasing strain for some time. Russia's annexation of Crimea in 2014 is seen as the most blatant land grab since WW2. President Assad of Syria has been accused of using chemical weapons on his own people. Beijing is accused of eroding Hong Kong's legal freedoms. Questions have been raised about the effectiveness of NATO, and even the United Nations' relevance has been brought into question. At the same time, traditional Western democratic values are waning. The rise of a more nationalist political agenda is apparent in many states. In Brazil, Hungary, and the Philippines, nationalist leaders have taken the popular vote. Growing domestic divisions offer fertile ground for the seeds of discord and destabilisation.

## The growth of novel domains

The pursuit of political and territorial supremacy takes place on more fronts today than ever before. Two new domains have grown in significance in the past decade: cyber and space. Globalisation of the cyber environment has expanded the tools that can be used to influence and destabilise. Mobile connectivity, the Internet of Things, and social media all provide unregulated access, often through untraceable means. The potential to influence perceptions and behaviours is considerable and unpredictable. And the cost of entry is low, making cyber particularly attractive to organised crime. Cyber has also massively expanded the attack surface: the desire to increase efficiency and reduce costs has led most sectors to adopt cyber technology as the backbone of their operations. These benefits come at the cost of increased exposure. And then there is space, a domain that governments are quickly losing the ability to regulate. Reliance on space assets across military, government and civilian services is sizeable, and growing. This presents new opportunities for malicious actors: such as spoofing or jamming anything reliant on satellite signals. A coherent understanding of existing space vulnerabilities is yet to be established, but this domain represents a significant threat for organisations, especially those reliant on other countries' global satellite systems.