CULTURAL SHIFT

Helen Dudfield *explains the growing need to build a defence from a solid foundation of training*

The democratisation of technology has made it possible for society to navigate seismic shocks like those seen by the pandemic, but for those in defence, it presents new challenges in the form of the rise of asymmetric – or grey zone – warfare. This battleground is one in which the weapons of warfare are not the conventional rifle or tank, but rather commercial-off-the-shelf (COTS) computers, which give bad actors the ability to inflict considerable economic and physical damage on their targets, as shown by the £50-million losses caused by the drone disruption at Gatwick airport in 2019. Nowadays, potential enemies are increasingly harder to identify as those with access to a computer or an off-the-shelf drone are capable of causing as significant harm as conventional weaponry, while at the same time not provoking a conventional response or being recognised as a formal act of aggression.

The weaponisation of everyday technologies is blurring the lines between the skills applied and tools used by those within and outside the military, with acts often combining both. The lack of distinction between what is a military skill and what is not, presents a major challenge to the defence sector.

BEING AN EARLY ADOPTER OF DISRUPTIVE FORMS OF TECHNOLOGY PUTS THE UK AHEAD OF ADVERSARIES

Introducing those with relevant skills and knowledge firstly requires a change in the recruitment process. Approaching those who fit the traditional military hire is no longer enough to address the growing forms of attack. The net must now be cast further, in order to court the digitally native generation who may not have seen the defence sector as the natural home for their skillset. Secondly, recruiters must illustrate to potential talent why a job in the defence sector is a worthwhile career choice, as they will be competing directly with the strength of the private sector, the promise of tech start-ups and the huge salaries on offer within the banking sector.

However, the tech talent pool in the UK may not be ready to service the demand. Research from recruitment firm Robert Walters Group found that the pandemic has put pressure on demands, with 58 percent of hiring managers putting information security as their most required skill, while only 10 percent of IT professionals have the skills needed to fulfil the roles.

With a small talent pool, focus must also be put on a second approach: targeted investment into reskilling current personnel so that they are capable of countering the new threats being posed. This calls for a shift in focus.

CONTINUOUSLY ADAPTING

The linear process of 'train – deploy – return – train again' no longer matches the constant nature of grey zone campaigns or the unpredictability of their impact. Training should be a constant process – not a set piece of timed activity. Defence and security forces need to continuously adapt to changes in the environment and incorporate new skills into the way they operate. This is particularly important when force numbers are reduced but strategic effect needs to be maintained.

Secondly, the spread of learning and development tools needs to widen to make the most of novel technologies including mixed reality, AI and robotics. This is increasingly necessary as defence and security forces will be training across multiple generations and incoming personnel are likely to be more comfortable with new digital ways of learning. It also enables a shift from basic 'muscle memory' training to more cognitive training, which in turn helps individuals to shift more easily between traditional fighting skills to those required for effective protection, deterrence, assurance and civil support.

Finally, training should be more collaborative. Regular training with allies reinforces the message of how powerful integrated responses can be, and provides a visible deterrent for adversaries no matter what novel tactics they may be exploring for grey zone conflict.

Experimentation has become more prevalent in recent years, spurred by the success of the rapid prototyping and innovation cultures championed by Silicon Valley: fail fast, learn and improve. The value of experimentation in defence has already been realised in several interdisciplinary multi-national exercises, such as the Unmanned Warrior exercise, which provided a testing ground for unmanned systems and Formidable Shield which tested eight NATO countries' defence capabilities versus ballistic missiles. These accelerate the development and integration of technologies and operating concepts by allowing them to be tested in a controlled, safe environment.

Applying this capability to the grey zone could take the form of incorporating penetration testing and Red Teaming to ensure defenders are prepared. Penetration tests actively attempt to practically exploit vulnerabilities and exposures in an organisation's infrastructure, applications, people and processes. Red Teaming on the other hand is scenario based and a goal driven test, with the ultimate aim of emulating the real-world adversaries and attackers who are trying to break into a particular system or steal information.

Training using virtual reality is cost-effective, and boosts learning and retention rates

The use of virtual and constructive simulations allows personnel to train with scarce or high value assets and means that live training capabilities can be adapted to meet evolving operational needs. A technology-agnostic approach should be taken throughout; integrating training systems, simulators and equipment supplied by different manufacturers to build the most effective synthetic representation possible. Training using virtual reality is cost-effective, and boosts learning and retention rates. 'Rehearsing' operations in a realistic environment leads to increased operational efficiency and production, and cuts downtime required to carry out maintenance.

While an intention to improve training is important, with the issue of grey zone, forces will need the science and technology being used by the enemy to hone their skills on. Traditionally slow to take on new forms of technology, the West needs to do more to accelerate the adoption of technologies and ensure that forces have the necessary equipment to train and develop capabilities to combat grey zone attacks.

To achieve this, a path needs to be cleared for the accelerated transfer of civil sector technology into military and security use to improve its effective response to attacks that also stem from the civil sector. For the UK, being an early adopter of disruptive forms of technology will go some way to putting it ahead of adversaries and giving it a leading role in this area among its allies.

However, to successfully integrate technologies from the civil sector calls for further collaboration with those in the industry. Defence and security forces have first-hand understanding of their operational challenges, while academia and industry are continuously exploring potential solutions; close communication and collaboration between all parties is essential to ensure development and innovation

remains mission focused. And this all falls back into the need for a modernised training programme, both in terms of techniques and tools which are used. Training partnerships with industry and allies will be able to deliver the needed tactical training to combat realistic threats while forging closer cross-government, inter-Service and international integration.

RECRUITERS MUST SHOW POTENTIAL TALENT WHY A JOB IN THE DEFENCE SECTOR IS A GOOD CHOICE

The primary obstacle to increased collaboration is the tendency of defence enterprises to be extremely protective of their intellectual property, and open collaboration can feel at odds with the need to maintain the necessary competitive advantage. Collaborative training spaces can be configured in ways that meet these confidentiality requirements, by sharing key outputs without giving away knowhow. Data would remain the property of the various partners, overseen by an independent curator that understands and mines the data to produce a coherent picture.

Defence enterprises must work together to agree common standards and principles on the use of collaborative environments, threads and twins. Only once this is understood, and a collaborative culture is embraced, can the timesaving, cost-saving and performance-enhancing benefits of collaborative training be realised.

The accelerating transfer of consumer technology from lab to user continues to lower the bar for entry and we are likely to see an increased number of those with the capabilities and technology to deploy commercial, consumer technologies to great effect within the defensive sphere. With such undefined battle grounds, there is really no limit to the potential growth the grey zone could enjoy. What's more, it's becoming increasingly clear that we are set to see both state and non-state actors become willing to operate within it in order to achieve whatever their aims may be.

The British Forces have already begun their immediate response to the new form of battle, as Royal Marine commandos begin to be deployed on covert missions overseas with the specific task of operating in the space between peace and war to disrupt enemy activity. Nevertheless, a further cultural shift is needed, and can be achieved through putting in the framework that ensures employees are prepared for grey zone threats.

While in the short-term, tactical recruitment will go some way to helping, in the long-term the necessary capabilities can only be delivered through a focussed and modernised training programme, which provides further credence to the Government's Integrated Review and Defence Command White Paper. The structure emphasises the importance of science and technology to the strength of defence going forward. A cross-industry collaboration will ensure the UK's forces can explore, experiment, evaluate and exploit new technologies, techniques and tactics vital to future operational advantage, security and prosperity ●

Helen Dudfield is Chief Scientist for Training and Human Performance at QinetiQ. Over the course of her 20-year career with the company, Helen has played an essential role in the Simulation and Training department, currently acting as a Senior Fellow and Chief Scientist for Training and Human Performance and Senior Fellow. Helen is also a RAEng Visiting Professor at Nottingham Trent University.

Critical training should take place during deployment to shorten the timeframe for achieving maximum strategic effect

Picture credit: US Dept Defense