QINETIQ

The Hardest Target:

Executive Summary

For decades, Western militaries have boasted unmatchable power. This overmatch created a powerful deterrent, by demonstrating to adversaries that a conventional attack would be futile.

But such conventional deterrents are no longer enough. Unable to defeat the hard targets of Western militaries, adversaries have turned their attention to softer targets - infrastructure, institutions, citizens, and economies. In this new era of persistent competition, Western nations will lose their 'hard target' status if they don't find innovative ways to deter these sub-threshold, 'grey zone' attacks.

Technology exploitation as a deterrent

The reason adversaries adopt sub-threshold strategies is precisely because they are deterred from full-blown conflict. So, conventional military capability remains vital, but not sufficient. Western nations now face the difficult balancing act of retaining conventional deterrents while simultaneously increasing deterrence against unconventional threats. The challenge facing government defence departments is therefore twofold. First is to sustain conventional capabilities while developing novel ones, often with little or no additional budget. Second is to increase the effectiveness of conventional capabilities by making them more available, deployable, versatile, and adaptable.

This is why becoming the hardest target in today's conflict environment requires powerful technology, deployable with immediate effect; deterring adversarial aggression by making the risk too great. But, how is effective technology exploitation defined, and how does it look in practice? The answer can be summarised as: "Knowing the mission to guide innovation and operationalise it at pace". Below, we explore each of these three elements in more detail, covering the technologies and practices that will help to turn tech exploitation into an effective deterrent against military and non-military threats.

1 Knowing the mission

This is about understanding a) the proactive goals you wish to achieve and b) the threats you must be prepared to defend against, through both preventative and reactive measures. This ranges from horizon-scanning for emerging global threats, to situational awareness for detecting immediate specific threats. To do this, defence and security should combine knowledge to compete on unconventional fronts: non-defence government departments must learn to view their work through a defence and security lens. Equally, defence must understand and communicate the security threats facing non-defence departments. Defence must also seize the information advantage: data is critical to understanding the defence and security mission and therefore maintaining the advantage. It should be drawn from across government, but refined, prioritised and distributed in a highly targeted and timely way. Lastly, defence and security must plan for the unplanned: knowing that the mission is not fixed, but fluid; this must be a key factor in all forward planning, resulting in strategies with built-in flexibility and redundancy.

2 Guiding innovation

'Guiding innovation' is about using acquired knowledge to make informed decisions about which technologies to adopt, and how to apply them for best success. This requires defence to match innovation to the mission: as technology solutions continue to become more abundant, national deterrence through technological superiority can only be achieved if the most effective technologies are prioritised and any unsuitable ones quickly ruled out. Here, collaboration is key: matching innovation to mission requires intelligence, skills and knowledge to cross over between the public sector, private sector and academia. This must be carefully managed for confidentiality and security. Defence must also embrace experimentation: experimentation in live or virtual exercises offers users the opportunity to try out high-risk technologies and tactics in safe and secure environments. Unpromising lines of innovation can be discontinued and new promising ones pursued.

3 Operationalising at pace

'Operationalising at pace' is about doing all of the above as rapidly as possible to stay ahead of adversaries. This requires a change in defence and security culture to one in which new innovations can be fielded quickly, and capabilities can evolve in real time as geopolitical circumstances change. Defence must develop solutions iteratively: the ability to bring advanced technologies to bear quickly is a deterrent in its own right. If a nation's industry is equipped to innovate and operate at the pace of relevance, it becomes a significantly harder target for adversaries. To do this, get your people ready: operationalisation is not just about fielding technologies quickly, but ensuring a nation's training and skills remain aligned and up-to-speed with its innovation. Tech is only a deterrent if it can be rolled out and used effectively. Finally, defence should formalise accelerated processes: a rapid innovation culture must be underpinned by a formal framework to maintain structure and focus. This can be achieved by building a community of innovators, overseen by an independent and impartial body.

Recommendations: how to become the Hardest Target

Integration of organisations and capabilities: a holistic system of complementary capabilities creates a harder target than multiple disparate ones. Vulnerability lies in the gaps between responsibilities, such as those which arise when threats are classified solely as a defence matter, a security matter, or a trade matter. Adversaries can exploit the grey areas between these classifications, knowing that disagreements, miscommunication or skills gaps between agencies slow a nation's response. In contrast, a unified system set up to counter multiple threat types is a powerful deterrent.

Data collection, fusion and classification: AI can help to automate key elements of data mining, prioritisation, and distribution. Humans will need to train the AI to 'understand' what data is important, to whom, and when – and ensure that the key element of human intuition is not lost in the process. Systems must be explainable, allowing users to interrogate the computer's decisions and correct mistakes. The whole system of information integration must be overseen at the highest level by a security-cleared authority able to work with all integrated parties. If done well, such a system can funnel a massive quantity of data to ensure the most relevant information is delivered to the right parties at the right time.

Collaborative experimentation and training: nations must recognise that technology is only as effective as its users. While it's easy to focus on innovation, equal weight must be given to exploitation, which requires placing people at the forefront of capability development. In practice, this means breaking down the barriers between agencies through closer integration, minimising the risk of either threats or opportunities falling between the gaps. Integration clears a pathway for collaborative, user-centred innovation, where problems can be tackled from multiple viewpoints and solutions developed with the end user's experience in mind.

Winning the perception war: for a nation to be a hard target is not sufficient; it must be seen as a hard target. Nations seen to be in possession of effective innovation programmes are more likely to create new ways to defeat enemies, thus becoming a less attractive target. Just as international cooperation generates a powerful deterrent against military aggression, collaboration between government departments, industry sectors and academia deters sub-threshold aggression through combined intellectual force. Nations must be proactive in demonstrating the fruits of this collaborative innovation: novel capabilities, brought to bear quickly and deployed with maximum effect.