QINETIQ

Becoming the Hardest Target

Militaries are good at making themselves hard targets for other militaries - but how can societies similarly deter adversaries from attacking softer civilian targets?

Powerful nations like the UK, US and France have traditionally built their status on conventional warfighting capability across the three historically dominant domains of land, sea and air.
For the past 20 years the armies, navies and air forces of the West have boasted unmatchable power, meaning no other nation or alliance could risk taking them on. Possessing such an advantage creates a powerful deterrent by demonstrating to adversaries that a conventional attack would be futile and the risk too great.

Even when two strong adversaries are closely matched, the potential catastrophic consequences of a war between two military superpowers provide a deterrent of their own. Nowhere is this more starkly demonstrated than in the case of nuclear weapons and the threat of mutually assured destruction. Launching a nuclear strike would provoke an inevitable, instant retaliation. World leaders know that to push that button is to sign one's own death warrant.

But here is where things get really tricky. The Stability–Instability Paradox posits that opposing countries locked in stalemate under the threat of mutually assured destruction are more likely to become embroiled in frequent low-intensity conflict. Military theorist and historian Sir Basil Henry Liddell Hart described the problem in 1954:

"To the extent that the H-bomb reduces the likelihood of full-scale war, it increases the possibility of limited war pursued by widespread local aggression."

A quantitative evaluation of the hypothesis, published in the Journal of Conflict Resolution in 2009, found evidence in support of its truth.

The phenomenon can also be clearly seen in the global rise of 'grey zone' competition in the 21st century, in which hostile actors increasingly achieve their strategic aims through offensive tactics below the threshold of war. It is the very effectiveness of Western military power as a deterrent that has led adversaries to turn to these unconventional tactics. Unable to defeat the hard targets of Western militaries, their attention turns to softer targets – infrastructure, institutions, citizens, economies. The trend is evident in cyber-attacks on high-profile organisations; in the spread of disinformation on social media; in the assassination of dissidents on foreign soil; and in the aggressive economic actions of states seeking to increase their global influence.

While conventional capability-overmatch ensures Western militaries remain superior, the societies they are sworn to protect may be more vulnerable than ever to persistent sub-threshold aggression. This undermines social cohesion and steadily erodes political and economic stability. In the past, Western nations have prevailed thanks to their military might – but that alone is no longer enough.

Just as militaries combine technology and strategy to make themselves hard targets for enemies to strike in battle, societies must develop ways to deter adversarial aggression below the threshold of war. A nation must demonstrate to its adversaries that an attempted sub-threshold strike on its institutions, critical infrastructure, or citizens is unlikely to succeed – and will be met with a decisive response. Because grey zone competition is often conducted covertly by unknown actors, having the technological and procedural means to quickly detect attacks and expose the perpetrators is vital. Grey zone aggression deliberately blurs the line between combatant and non-combatant, which in turn blurs the line between military and non-military responses. Intelligence must be used to disambiguate threats and inform timely, targeted responses using proportionate countermeasures.

Fighting on this ambiguous front demands a reassessment of what we in the West think of as deterrence. It is not just about having missiles trained on the enemy, or thousands of soldiers ready for deployment; it is about fortifying society itself against all types of threat – by using all the tools at its disposal to create a holistic defensive posture. Central to this is the ability to not only design solutions, but to deploy them as capabilities in response to, and anticipation of, emerging threats. In this report we explain how a whole-system approach to defence and security at an industrial and civil level can harden a nation's softest of targets and become a deterrent in its own right. This will be essential if nations and organisations are able to extend their position as a hard target in conventional warfare, to become equally unappealing to engage in the new domains and tactical battlespaces that define modern conflict.

Key takeaway: Conventional military deterrents are no longer deterrence enough. Western nations will lose their 'hard target' status if they do not find innovative ways to deter against sub-threshold attacks in this new era of persistent competition.

The challenges of defending a society

The West has become very used to defending its interests overseas, by deploying troops to fight wars thousands of miles away from home. Powerful, well-equipped armed forces are effective deterrents against other militaries.

However, military force alone cannot protect a nation from cyber-attacks, disinformation campaigns, or political and economic coercion. These are urgent threats to sovereign interests from foreign or domestic actors, and yet fall outside the usual defence and security remit. Addressing these threats requires rethinking the scope of defence and security, acknowledging that in the new threat landscape a data scientist may be just as vital to a nation's protection as a highly-trained soldier.

Redefining modern defence and security is the first major challenge facing governments. The dilemma is this: virtually every government function is a vector via which its citizens' security and wellbeing can be diminished. A nation's health can be compromised by disinformation campaigns promoting anti-vaccine propaganda. Its food security and access to resources can be threatened by trade dependencies with unpredictable or unstable countries. Environmental policy will become increasingly significant, as the effects of climate change and food poverty destabilise regions and displace large populations, creating new refugee crises. But defence cannot lead on all of these matters – and nor should it.

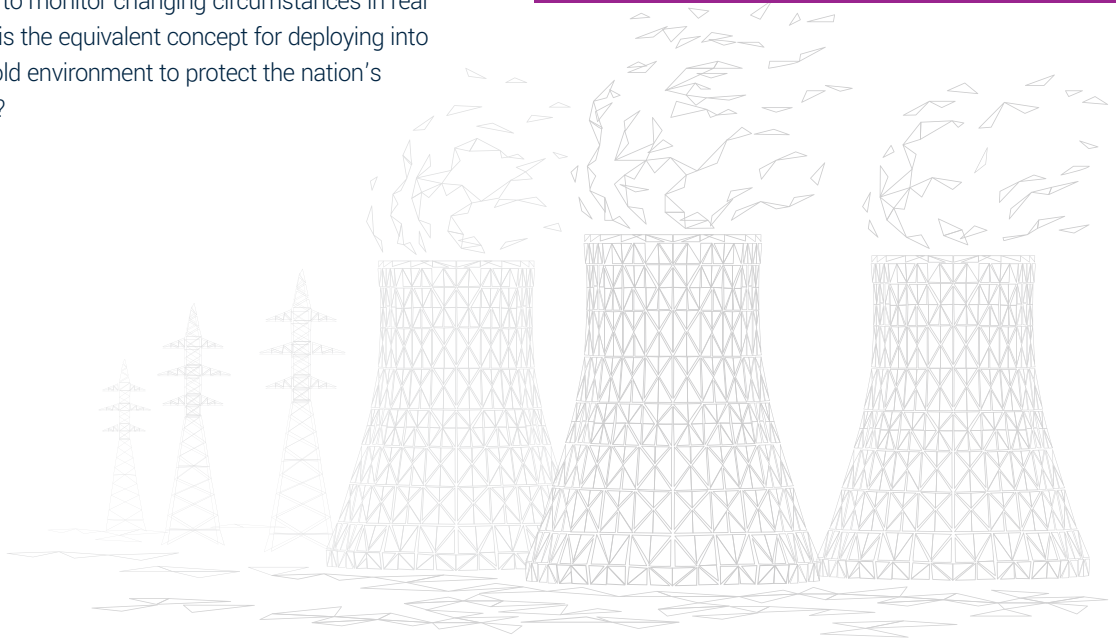
Besides lacking the funding and capacity, the overreaching of defence into civilian concerns is likely to be seen as unwelcome militarisation, making citizens uneasy. Rather, it is about defence understanding the utility of expertise and innovation from beyond the conventional defence and security sphere in protecting sovereign interests.

Equally, other government functions must understand the defence and security implications of their own activities, and draw on defence for support.

Establishing new collaborative frameworks and redrawing boundaries rests on a deep understanding of the threat environment and the nation's overall mission within it. This in itself is another significant challenge, as the modern battlespace can be anywhere at any point in time. Targets may be military, civilian, governmental, infrastructural, institutional, or corporate. When an army deploys to a physical, geographical battlespace it does so equipped with detailed knowledge of the operating environment and the means to monitor changing circumstances in real time. But what is the equivalent concept for deploying into the sub-threshold environment to protect the nation's soft underbelly?

Major conflicts since the early 20th century have seen the emphasis on nations fighting nations, with militaries having evolved accordingly to fight and deter other militaries. During such conflicts, priority is given to the resilience of society and the supply chains that keep the nation fighting. Historic examples include rationing; giving over land to food production; and conscripting women to fill manufacturing roles vacated as the male workforce heads to the front line. However, with today's societies in a state of constant competition with hostile forces, under threat from disinformation, economic disruption and attacks on infrastructure, democracies need to examine how they bring that resilience back to wider society and still maintain the necessary level of deterrence against conventional force.

Key takeaway: Government functions outside defence must learn to view their work through a defence and security lens. Defence must equally understand the utility of non-defence skills and innovation.



The role of conventional defence capability

Conventional military capability remains vital. The reason adversaries have adopted sub-threshold strategies is precisely because they are deterred by the huge risk of engaging in full-blown conflict.

If that risk is perceived to have diminished, those adversaries will become emboldened and the likelihood of war will increase. The challenges facing government defence departments regarding maintaining deterrence in an age of changing conflict are therefore twofold.

The first is to sustain conventional capabilities while developing novel ones, often with little or no additional budget. However, what is often overlooked is that sustaining a capability is not the same as retaining legacy platforms or equipment. It is important to draw a distinction between the capability (the effect delivered) and the technology (the technological means by which that effect is delivered). It is not about retaining the same kit, but about maintaining the ability to deliver the same effect, irrespective of the underlying methods. That is what deters adversaries from stepping into conflict. Governments must consider whether longstanding defence requirements can now be met more efficiently using combinations of newer technologies. It is entirely possible to remain committed to a conventional capability without being wedded to the conventional way of delivering it. It may transpire that delivering a capability no longer requires certain legacy platforms or equipment – although removing these from service, or scaling back their use, may feel uncomfortable to some.

As Liddell Hart once noted:

"The only thing harder than getting a new idea into the military mind is to get an old one out."

Receptiveness to new ideas, and a recognition that progress is not made by simply doing things the way they have always been done, are valuable qualities in today's military leaders. It generates uncertainty of outcome that enemies recognise as a risk that can impact their decision about whether or not to engage.

The second challenge is to increase the effectiveness of conventional capabilities by making them more available, deployable, versatile, and adaptable. Possessing superior technology is not a deterrent in its own right. Technology can only fulfil its promise if it is available where and when it is needed. It also needs correctly trained users, combined with more effective doctrine. Rogue states and violent non-state groups are unencumbered by lengthy procurement cycles, rules of engagement, or safety concerns, enabling them to develop new threats faster than Western nations can develop countermeasures. In the West, by the time a threat has been identified and a solution procured, tested and deployed, the threat has evolved.

Adversaries rely on this lack of agility to outpace us – but if we are able to match their pace we become more of a threat if they engage, removing their advantage.

However, the West must not be drawn into a race to the bottom, lowering its own ethical and safety standards to keep pace. If we do, the enemy has inflicted upon us an ideological defeat. Instead, we must identify smarter ways of procuring military equipment and adapting it throughout its service life. We will return to this important point later.

Key takeaway: Reducing military capability in favour of non-military deterrents makes a nation a softer target. Nations face the difficult balancing act of retaining conventional deterrents while simultaneously increasing deterrence against unconventional threats.

The role of novel defence and security capabilities

In the face of an ever-shifting threat environment, continuing to compete only in conventional ways using only conventional capabilities hands an advantage to modern adversaries. It decreases a nation's competitiveness and consequently weakens its deterrence, making it a softer target. This leaves three other possibilities:

1

Using existing technology to create new capabilities

It is not always practical, or even necessary, to wait for a new technology solution to an emerging problem. As the saying goes: 'necessity is the mother of invention' – and the military has a long history of repurposing equipment in inventive ways. During operations in Iraq in 2007, it was discovered that the gunnery thermal sight fitted to some Warrior armoured vehicles was capable of detecting small heat signatures given off by power sources in improvised explosive devices (IED). The discovery prompted rapid changes in tactics, techniques and procedures (TTPs) to improve survivability, with Warriors repositioned as vanguard vehicles and crews trained in IED detection using the gunnery sights. Human ingenuity is often the most powerful defence capability of all, and should be well supported within a culture of innovation and experimentation.

2

Using new technology to tackle conventional defence challenges

With numerous sovereign territories, including several in Eastern Europe and the Far East, living under constant threat of annexation by foreign forces, the familiar warfighting challenges are not going away. However, new technology may offer a lifeline to smaller nations by helping them to tackle those challenges better. Autonomous vehicles, operating in swarms or as 'wingmen' to crewed platforms, can multiply the combat mass of an army, air force or navy. A main battle tank currently requires a ratio of around four operators to each platform.

In future, with the introduction of autonomous vehicles connected via a centralised command and control console, that ratio could be inverted, to four or more platforms per operator. Such technologies will enable the same number of soldiers to deliver a much greater effect, allowing smaller forces to increase deterrence.

3

Using new technology to tackle new defence and security challenges

Threats are emerging today to which existing defence capabilities do not offer a solution. This is of course nothing new – history's military capabilities have all been conceived in response to changing requirements. But the factors that make the 21st century unique are the accessibility of sophisticated technologies to adversaries and the breakneck pace of their development. A terrorist group with very little capital can: launch an aerial assault using commercial off-the-shelf drones laden with explosives; cause communication blackouts with low-cost signal jammers; or carry out denial-of-service attacks on critical online systems from a home laptop. In many cases, technologies already exist to counter these threats – such as laser directed energy weapons capable of shooting down drones, or radio frequency detection devices that can locate jammers. But where adversaries are nimble in their acquisition and application of technologies, mixing and matching from an ever-expanding kit bag to continually generate new and unforeseen threats, nation states are often slow in their adoption of countermeasures, making them predictable and easy to outmanoeuvre. It is this asymmetry that leaves a nation's soft targets exposed, and adversaries will continue to heavily exploit these vulnerabilities until the gap is closed.

The challenge is to quickly determine which of these approaches are best suited to new circumstances as they emerge. If there is already technology in service that can be repurposed to meet a new brief, using it may be faster than – and therefore preferable to – building a bespoke solution from scratch. If no such technology exists, the requirement must be defined and put out to tender quickly. Keeping pace with fast-evolving threats by quickly identifying and sourcing the best defence or non-defence technology solutions is a vital part of a nation's total deterrent. It may sound simple, but it requires an encyclopaedic knowledge of existing and emerging technologies and their capabilities. Given that the most effective solution to a new defence problem may come from outside the typical defence sphere, this technological awareness must extend beyond the latest innovations from the usual prime manufacturers to those of small and medium-sized enterprises (SMEs) and academia. Building and maintaining this awareness is a daunting but essential task. Failure could result in governments spending many years and lots of money developing solutions that already exist elsewhere, while the resulting capability gaps continue to be exploited by adversaries.

Key takeaway: In a multifaceted and fast-changing threat environment, the ability to quickly identify, source and deploy capabilities – including those from outside conventional defence sources – is a critical component of deterrence.

Technology exploitation as a deterrent

Advantage does not come from simply possessing the most advanced technology, but from being the best at deploying and using it.

A nation's ability to bring technology to bear can be a deterrent in its own right. This is what we mean by becoming the hardest target – powerful technology, deployable with immediate effect, deterring adversarial aggression by making the risk too great. But how is effective technology exploitation defined, and what does it look like in practice? We believe the answer can be summarised as:

"Knowing the mission to guide innovation and operationalise it at pace"

The following sections explore each of these elements in more detail, taking into account relevant technologies and practices that will help to turn technology exploitation into an effective deterrent against military and non-military threats.

Key takeaway: The 'Hardest Target' formula is that superior technology, plus effective exploitation, equals capability and advantage. Effective technology exploitation requires information, innovation, and agility.

Knowing the mission

‘Knowing the mission’ is about understanding the proactive goals you wish to achieve and the threats you must be prepared to defend against using both preventative and reactive measures. This ranges from horizon-scanning for anticipating emerging global threats, to situational awareness capability for detecting immediate specific threats.

When deploying into a warzone, a well-prepared unit understands exactly what it seeks to achieve and the potential barriers to achieving it. It knows the ways in which the adversary fights; the locations of enemy bases; the sentiments of local populations; and the geography of the battlespace. Once in theatre, it can monitor in real time the positions of hostile forces and gather evidence to determine their likely intent. All of this is aided by intelligence, surveillance, target acquisition and reconnaissance (ISTAR) technologies – gathering information from multiple sensors and sources and combining it to build a detailed picture of the operating environment as a whole.

Battlespace situational awareness is well established, well practiced, and deters enemies – but when threats are unconstrained by geographical regions or warfighting norms, the concept breaks down considerably. Defence alone is not optimised for awareness of sub-threshold aggression at a whole-society level, in which unseen adversaries launch unpredictable and often untraceable attacks against non-military targets. How does a nation define its mission in the face of such uncertainty?

Combine knowledge to compete on unconventional fronts

It has long been argued that warfighting domains should not be compartmentalised, but treated as constituent parts of a whole. In recent years, this approach has been formalised in joint doctrine papers published by numerous Western nations, and has been followed by a growing recognition of the need for closer integration across military domains and between the defence capabilities of allied states. To similarly compete in the sub-threshold environment, this integration must be taken further still – to include industries and government departments not traditionally associated with defence. Again, this does not imply a defence takeover of wider government, but a shared understanding of the new fronts on which conflict is taking place. What are the defence implications of public health policy, or the public health implications of defence policy? And what of environment, education, or media and culture?

China's coercive commercial diplomacy is one example of this thinking in practice. The Chinese Communist Party has repeatedly been accused of wielding trade and market access as political weapons to tip international policymaking decisions in its favour. In response, countries worldwide are seeking ways to reduce their dependence on China for their supply chains and exports.

In September 2020, a group of senior military and business leaders called Securing America's Future Energy (SAFE) warned that the US must urgently establish a domestic electric vehicles industry or risk becoming dependent on China. It is a demonstration of trade and industrial policy being considered through a defence and security lens – the type of thinking needed across virtually all functions of government.

Seize the information advantage

In a combat situation, knowing the environment better than the adversary allows the war fighter to remain at least one step ahead, anticipating the next move to react faster and with greater impact. This principle is equally important for societies in the face of grey zone aggression.

There is more data available to defence and security forces than ever before, driven by the ever-increasing interconnectivity of modern technology and its users. Open-source online data has been used to trace terrorist cells, child abusers, cyber-criminals, and illicit traders. But the ubiquity of data poses a new challenge. Multiplying the amount and availability of data increases the administrative and cognitive burden of sorting and interpreting it – which itself becomes an exploitable weakness. Data has to be both timely and relevant to be effective. Decoding a message that you are about to be attacked is futile if the attack has already happened, or the information didn't reach the executive decision-maker in time. Addressing this challenge requires an information integration system which combines human and artificial intelligences to ensure the most relevant and urgent data is presented to the right decision-makers at the right time. An artificial intelligence (AI) data fusion engine can automate key elements of data mining, prioritisation, and distribution to ease the burden on the human decision-makers. The system must be explainable to enable users to interrogate the computer's decisions and correct mistakes. It must also provide a transparent audit trail to demonstrate accountability.

The public sector is in a strong position to harness data for defence and security purposes. It understands the public it serves, can see the 'big picture' when it comes to political and socioeconomic issues, and wields the legislative weight to negotiate legal pitfalls. However, there are potentially large skills gaps facing governments, as they compete with the private sector for talent in data science and related skills. Combining the public sector's strengths with private sector expertise through closer cooperation between government and industry could create a formidable force.

Plan for the unplanned

Another paradox of 21st century defence and security is that to maintain a mission-led focus requires the ability to deviate from the original mission. This is because the mission, which was typically a singular goal in days of old, is no longer a static objective or a linear path. As a crude example, in conventional warfare the adversary's mission might be to seize territory, while the opposing forces' mission is to prevent them from doing it. The purpose of sub-threshold aggression however is not necessarily to achieve a specified outcome, but to constantly disrupt and destabilise. Adversaries' goals and methods change frequently, often while hitting multiple targets concurrently – and Western defence and security forces are not always equipped to fight back.

The principle challenge facing Western policymakers is that the mission of today may not be the same as that of tomorrow. It is at odds with the lengthy innovation and procurement cycles of government defence departments. For example, a requirement may be drawn up for a vehicle designed for desert warfare, based on the geopolitical circumstances of the day. But in the decade or so it takes to get it from procurement to entering service, the requirement may have changed to one of urban conflict.

While long-term horizon scanning remains vital, it must be combined with a means of continually reassessing present and emerging threats, and building an acquisition system that makes provision for the rapid introduction of relevant countermeasures into service. The ability to outcompete the development and system evolution process of the adversary is a key part of becoming the hardest target. Having a top-flight, agile science and technology base is absolutely vital to this.

Knowing the mission – key takeaways:

- Adversaries are highly dependent on the element of surprise when launching attacks. Knowing the enemy and anticipating their next move removes their advantage. The nation that does this best is the hardest target to strike.
- 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.
- 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.
- Knowing that the mission is not fixed but fluid must be a key factor in all forward planning, resulting in strategies with built-in flexibility and redundancy.

Guiding innovation

‘Guiding innovation’ is about using acquired knowledge to make informed decisions about which technologies to adopt and how to apply them to execute your mission with the greatest effect.

If understanding the nature of the mission is the essential first step, determining the tools needed to fulfil it is the obvious second. Great stock has been placed in innovation to counter modern threats, with the UK positioning science and technology, and research and development, firmly at the centre of its defence and security strategy. As powerful technology proliferates globally and becomes more accessible to those intent on using it maliciously, maintaining technological superiority becomes a more decisive factor in future conflict. The ultimate goal is to use technology to produce capabilities so advanced that they cannot be replicated by less sophisticated adversaries. Directed energy weapons, high-speed missiles, and space technology are all examples of these.

The advantage of becoming a ‘tech superpower’ is not limited to the ability to win battles. It also has the potential to exert significant economic and diplomatic influence, both through the export of intellectual property and by increasing the nation’s perceived value as an ally and strategic partner on the global stage. However, this approach is not without its pitfalls. Economies and defence industries built on innovation create strong commercial incentives for businesses to keep developing new technologies and marketing them to government. This can lead to an overabundance of ideas and solutions, making it hard to determine which best meet the specific mission requirements. There must be ways to quickly identify and prioritise the most relevant innovations, discarding those which are not appropriate. What processes must be implemented to achieve this?

Match innovation to the mission

With the arrival of the Fourth Industrial Revolution and the associated tech explosion, there is a broader range of technological challenges facing defence and security than at any time in history. But there are also more potential solutions to those challenges. Keeping abreast of the latest threats and opportunities presented by technology is a significant undertaking, but crucial to maintaining the innovation advantage. It is also only half of the story.

Knowledge of the defence and security mission must combine seamlessly with knowledge of technology threats and opportunities to ensure continued alignment between challenges and solutions. Insufficient awareness of the mission can cause innovation to lose focus, leading to the development and procurement of technologies that do not meet the requirement.

Insufficient awareness of the latest technology developments can result in missed opportunities and duplication of effort. It is a waste of time and money to invest in developing a bespoke solution when the requirement could be met faster and at lower cost using existing technologies.

Collaboration is key

Keeping innovation focused on the mission demands open, two-way lines of communication between the innovators and the end users. The ‘user-centred design’ approach has been a mainstay of computing for decades, defined by its iterative development process that involves the end user throughout, resulting in a more tailored and user-friendly product. In more recent years, the idea has gained ground in defence and security – but will require further modernisation to meet 21st century challenges. Although military products have long been produced by non-defence entities, the practice of user-centred design in defence has taken place primarily between innovators and end users within the industry. Closer integration between defence and non-defence organisations raises new questions about security clearances and data integrity when communicating up and down the chain.

As data moves between government departments and private sector organisations, classification and categorisation must be considered. Not all data is suitable for distribution to all parties, whether for reasons of national security, privacy, or commercial confidentiality. In drawing up data integration protocols, security risks arising from data aggregation must also be considered. For example, five separate unclassified pieces of information may become classified when combined. Identifying how to brigade data for effective and safe sharing should now be seen as key in any programme.

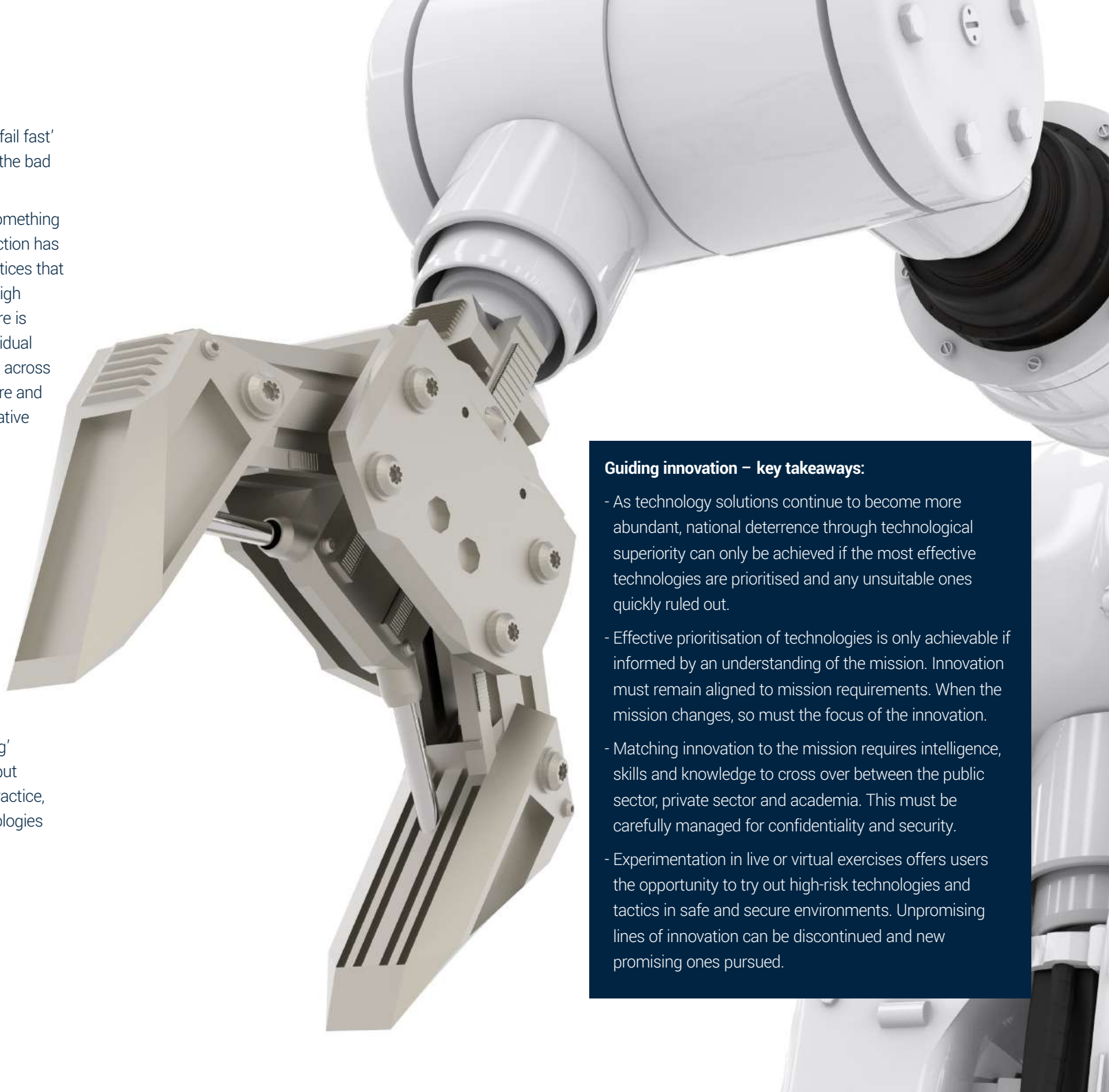
Embrace experimentation

The sheer scale of availability of technology in the 21st century can lead governments into decision paralysis. Unlike conventional defence capabilities, for which only a handful of prime manufacturers usually compete, solutions to grey zone threats and other modern defence and security challenges could come from virtually anywhere. A robust means of funnelling is required to narrow the broadest range of ideas quickly down to the fewest, most effective ones.

Silicon Valley start-up culture achieves this using a ‘fail fast’ philosophy, in which ideas are tested at a high rate, the bad ones ruled out, and the good ones taken forward.

In defence and security, failure is often treated as something to be avoided at all costs – but this pursuit of perfection has created a procurement culture and contractual practices that delivers the capability a decade too late. Given the high stakes in defence and security, this aversion to failure is understandable. However, seeking to eradicate individual failure raises the risk of being outclassed and failing across the board. A modernised defence and security culture and revised contractual framework can provide collaborative experimentation environments in which ideas can fail safely and securely, whether live or virtual.

Even the greatest innovative minds cannot predict all possible outcomes when bringing new capabilities into service. At some point users need to get their hands on the kit to find out in practice what it can and cannot do. For a life-and-death defence capability, discovering its shortfalls in theatre at the end of a ten-year procurement exercise is too late. Live experimentation offers a way to expose such unforeseen difficulties early in the development process, but it also provides a way to uncover hidden opportunities. By ‘wargaming’ scenarios in live or virtual exercises, end users can put their own innovation and frontline experience into practice, solving problems by applying and combining technologies in ways the developers could not have envisioned.



Guiding innovation – key takeaways:

- 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.
- Effective prioritisation of technologies is only achievable if informed by an understanding of the mission. Innovation must remain aligned to mission requirements. When the mission changes, so must the focus of the innovation.
- Matching innovation to the 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.
- 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.

Operationalising at pace

‘Operationalising at pace’ is about doing all of the above as rapidly as possible to stay ahead of adversaries. This will require 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.

The mission is fully understood, the requirements have been identified, and the last remaining step is to get capabilities into service. In defence this whole procedure typically happens via lengthy competitive tendering followed by testing, evaluation and certification of the chosen solution before being handed over to the end user. These steps exist for a reason and it would be cavalier to begin taking risky or unethical shortcuts. Competition remains necessary to ensure all solutions are given fair consideration and the one ultimately selected is the best suited to the task. Assurance is absolutely vital to ensure equipment is safe, secure and fit for purpose. However, the time taken to move from identifying the requirement to deploying the solution provides adversaries with a window in which to act. Closing that window by bringing new countermeasures to bear quickly makes a nation a harder target. An efficient system for operationalising technology is a deterrent in its own right, and a valuable asset in the defence of a nation. How can nations accelerate technology adoption without compromising fairness or safety?

Develop solutions iteratively

A capability in the pipeline is not an effective deterrent in the present moment. The trouble with technology horizon-scanning is that there will always be a more effective solution just a year or two away, making it tempting to wait for them to arrive – but that opens the window for adversaries and exposes that vulnerability. The key is to not wait to adopt the best upcoming capability, but to adopt the best useable capability available right now. Knowing that more effective solutions are in the pipeline, provisions should be made now for their introduction and integration into the system when they arrive later.

A capability implemented today should not preclude the introduction of superior capability tomorrow. It should be configured in a way that allows it to be continually updated and augmented, as new technologies become available.

For military capabilities, especially large expensive assets like main battle tanks, submarines, destroyers and fighter aircraft, this represents a significant change in culture. To remain credible deterrents, such platforms will in future need to be deployed earlier as ‘beta’ capabilities. This may seem counterintuitive, but one can think of the platform as a reliable and versatile base to which capabilities can be introduced or removed at pace as threats evolve. These must be based on open architecture that allows technology from multiple partners to be ‘plugged in’. Many non-military tech companies are already highly proficient at this, such as software developers who regularly release updates to products already in widespread use, like computers and smartphones.

Get your people ready

Operationalising capability is not just about the technology, but the people required to develop and use it. Let’s take quantum computing as an example. Still in its infancy, quantum computing is predicted to have revolutionary applications in any field that requires large volumes of data to be processed quickly. It could achieve in hours or days what today’s computers do in weeks or months. We have already discussed the importance of data for defence and security, and with that in mind, the first to master quantum computing will seize an unprecedented information advantage.

The race is on, primarily between the West and China – but the first to build a working unit will not necessarily be the ultimate winner. Even once the tech is perfected, exploiting it will rely on a domestic workforce able to roll it out at scale, and end users trained to operate the systems effectively

Training and skills must be considered an inseparable part of capability development, alongside innovation and technology design, and therefore part of any disincentive to engage in conflict. Technology can only become a meaningful deterrent if it can be placed into the hands of the people who need it when it is needed, and if those people are adequately trained in how to use it effectively. It brings us back to the user-centred design principle from the previous section. By making users part of the development cycle, they can help to shape the capability, make it more intuitive to other new users, and become familiarised with it by the time of its deployment.

Formalise accelerated processes

A formal framework is necessary to ensure a consistent and comprehensive approach to rapid technology adoption. Without structure and focus, innovation can become chaotic, shooting off into multiple disparate lines of development – some incompatible, some needlessly duplicated. Accelerated technology development programmes exist in various forms in most advanced nations, although few step outside a specific remit, such as defence, space, or commerce. In addition to fast-tracking development of military technology for military applications, or commercial technology for commercial applications, governments should seek ways to accelerate technology transfer between disciplines.

As discussed in the opening sections of this report, the best solution to a problem may come from an unexpected source, and so a nation's innovation framework should take this into account by facilitating the crossover of ideas between public sector, private sector, academia, prime manufacturers, SMEs, and so on.

An example of such a framework exists in the Accelerated Capability Environment (ACE) used by the UK Home Office within its Office for Security and Counter Terrorism. Founded in 2017, ACE draws on its community of more than 260 organisations from the public sector, private sector and academia to select and combine capabilities to tackle defence and security challenges. Its approach has been instrumental in fast-tracking innovative technological solutions to problems including maritime security, extremism, cyber-crime, and online child exploitation. ACE takes defence principles and applies them to tacking crime – but the model could be expanded into other applications. Health departments could use it in support of vaccine security, by quickly identifying solutions to disinformation campaigns designed to reduce vaccine take-up among citizens, or attempts by hackers to steal the intellectual property of vaccine developers.

The key to rapid innovation across multiple sectors and disciplines is community. A diverse collection of innovative minds can help to avoid the 'groupthink' that often plagues decision-making within isolated teams. However, leadership and structure are vital to keep innovation focused on the mission, necessitating the appointment of an independent overseeing body.

Operationalising at pace – key takeaways:

- 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.
- Do not seek to procure perfection, but a minimum viable product capable of fulfilling the requirement quickly. Delivery of an 80%-ready solution at the time of need is better than a 100%-ready solution several years too late.
- 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. Technology is only a deterrent if it can be rolled out and used effectively.
- 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.

How to become the hardest target

Understand; innovate; operationalise. This is the mantra Western nations must adhere to if technology is to become a meaningful deterrent against both military and non-military aggression. Without a deep understanding of the mission, gained through information and data, innovation becomes unfocused and chaotic.

Without focused innovation, technology solutions cannot be operationalised at the pace needed to counter threats. And, without effective and timely operationalisation of technology, nations become easy targets for adversaries. Conversely, having better information and data at every stage of the mission maintains focus; being focused on the mission guides innovation; and innovating at pace deters adversarial aggression by making the nation too hard a target.

We have identified a number of technologies and practices that should be applied at a whole-nation level to maximise the effect of innovative new capabilities as deterrents, throughout the whole cycle of strategic planning, testing and evaluation, procurement, training, entering service, and through-life support.

- 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, or 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.

Integration means facilitating the crossover of information, technology and skills between defence domains, government departments, public and private sectors, and allied nations. It does not necessitate the closest of possible relationships in all cases, but appropriate cooperation based on common goals and mutual understanding.

- Data collection, fusion and classification

The information advantage comes from understanding the enemy, the threat environment, and one's own vulnerabilities. The availability of information has never been greater, but that in itself creates huge challenges. The sheer abundance of data can lead to decision paralysis, or cause crucial details to get lost in the noise. Access to data can also be a limiting factor. Data must be managed in line with domestic and international privacy laws, such as General Data Protection Regulation (GDPR). And, when sharing data between agencies, some will require greater access than others due to varying security clearances and commercial sensitivities.

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.

They must also provide transparent audit trails to demonstrate accountability. 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.

For a nation seeking to become a global leader in AI, progress is not just about inventing new models, but developing the ability to integrate those models into the operating environment.

- Collaborative experimentation and training

Nations must recognise that technology is only as effective as its users. While it is easy to focus on innovation, equal weight must be given to exploitation, and that 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, in which problems can be tackled from multiple viewpoints and solutions developed with the end user's experience in mind. Experimentation during the development cycle helps to focus innovation, by quickly ruling out inadequate solutions and pursuing the most promising ones.

After development, collaborative experimentation can be used to form new capabilities, by testing different combinations of technologies and practices. Multi-agency joint training exercises bring together users around the capability to share accumulated knowledge. Training is critical, and must happen in parallel with the development of a capability to ensure it can be put to effective use as soon as it is ready.

Collaborative experimentation and training can take place in live exercises, or be facilitated using the latest digital technologies. Scenarios can be simulated in a synthetic environment accessible to trainees from multiple organisations in multiple geographical locations. Digital testing and evaluation allows different organisations, even with varying degrees of security clearance, to collaborate in the development of highly sensitive capabilities. All of these technologies and practices make a nation a harder target, by closing the knowledge and capability gaps that adversaries can exploit to their advantage.

- Winning the perception war

For a nation to be a hard target is not sufficient; it must be seen to be a hard target. Adversaries already know that a conventional military strike on the West, even if successful, will be met with swift retaliation by a cohesive international alliance equipped with superior warfighting capability. That is the nature of NATO and Western military deterrence. The point is expertly made using live multinational military exercises, which, in addition to preparing forces for battle, provide powerful demonstrations of ideological unity and technological capability. For any adversary considering launching an attack, these exercises are stark reminders of the stakes.

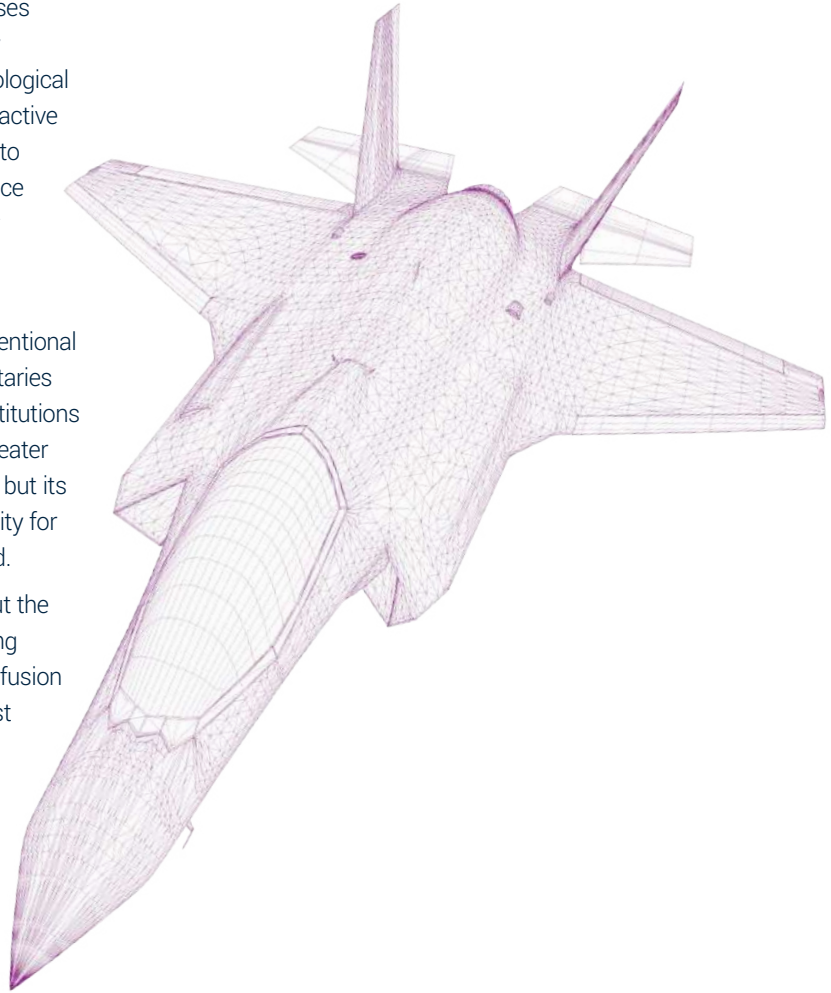
A similar psychological effect must be produced if non-conventional defence capability is to become an equally effective deterrent.

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. As with military deterrents, highly visible live exercises will play a part – but this must be accompanied by demonstrations of political will to become a technological superpower, through investment in innovation and active promotion of progress. A nation visibly committed to mastering technology in pursuit of sovereign defence and security interests presents as a risky target for any type of attack.

A nation's deterrence must exist on two fronts: conventional warfighting, and societal sub-threshold. Western militaries already make for hard targets, but their societies' institutions and citizens represent a soft underbelly in need of greater protection. Technology is often touted as a panacea, but its effectiveness is limited by factors such as its suitability for the mission and the pace at which it can be deployed.

Selecting suitable capabilities requires certainty about the mission, but the multifaceted and constantly changing nature of the modern threat environment breeds confusion and uncertainty. Under these conditions, the very best equipment can be rendered ineffective through its misapplication or slow deployment.

The scope of deterrence is therefore becoming wider than simply having weapons, platforms and technology. To seize the technological advantage, the ways in which these assets are used, and the speed at which they can be deployed and evolved, are just as important as the functions they perform. Rapid innovation and effective technology exploitation, informed by data intelligence, combine to form a capability that is a powerful deterrent in its own right. The nations able to perfect this holistic approach to technological deterrents will make themselves the hardest targets for enemies to strike.



Cody Technology Park
Ively Road, Farnborough
Hampshire, GU14 0LX
United Kingdom

+44 (0)1252 392000
insights@QinetiQ.com
www.QinetiQ.com

QINETIQ

QINETIQ/21/03268