QINETIQ

# Deploying Prototype Warfare

Prototype Warfare is not a new idea. It has been discussed by military strategists and commentators for nearly 20 years and has been applied for decades almost accidentally, but to great effect. But the majority of the conversation has focused on potential, not execution.

We believe that the time has come to move beyond Prototype Warfare as a concept and start exploring how we make it a practical reality for UK defence, and part of the defining culture of the British way of warfare. It is not enough to recognise its potential. We now need to instigate a broader cultural change that promotes a willingness to take the practical steps required to bring prototypes into UK defence.

This report, based on perspectives from both within and outside QinetiQ, is designed to progress the conversation in three ways:

1. It sets out the core principles for changing perceptions of Prototype Warfare within defence communities and explores the commercial world's view of prototyping – specifically why it has become such a crucial aspect of modern capability development, and the benefits it offers.

2. It asks what the potential drawbacks and limitations are and what unforeseen second and third order effects could be. Within this context it defines the practical barriers to achieving the implementation of Prototype Warfare in UK defence and makes recommendations for overcoming each one.

3. It makes recommendations for how the Royal Navy and other maritime forces can embrace Prototype Warfare without disrupting current acquisition processes that are in place to ensure security, reliability, and compliance in fielding required capabilities.

'Deploying Prototype Warfare' is designed to do more than stimulate meaningful conversations and alter perceptions. It is designed to instigate behavioural change across UK defence. Without moving beyond a discussion about the potential of Prototype Warfare we will never be able to benefit from its adoption.

QINETIQ

"Success no longer goes to the country that develops a new fighting technology first, but rather to the one that better integrates it and adapts its way of fighting… our response will be to prioritize speed of delivery, continuous adaptation, and frequent modular upgrades."

US National Defense Strategy

At QinetiQ, we see an inherent tension in UK defence culture. The military recognises the need to embrace technological innovation and adapt rapidly to survive in a complex and uncertain environment. But in practice it remains largely shackled to an acquisition approach which favours a more deliberate process.

The current mindset places a premium on certainty that promotes waiting until technologies, tools and techniques have matured before they are adopted. This risks the UK being out-innovated by both state and non-state adversaries.

Adjusting the direction of travel therefore requires more than just a series of tactical changes. It requires a shift in the military mindset that stimulates a more systemic pan-DLOD (Defence Lines of Development) approach to introducing innovation as part of a continuous cycle of learning, development and adoption – assessing how new technologies and systems allow our forces to operate differently, and constantly adapting to reflect those findings.

We define Prototype Warfare as a willingness to engage in military operations with capabilities that are not normally considered ready for operational deployment.

It is experimentation in contact – albeit with the right safety measures in place. Prototype Warfare is a concept that sits at the fulcrum of defence's relationships with technology, capability, safety, tactics, and culture. More of a mindset or philosophy than a strategy, it centres on a willingness to use experimental technologies, tools and techniques at an earlier stage of readiness in live environments as part of a continuous cycle of learning and optimisation across all DLODs.

The concept is not tied to specific technologies. In fact, the technologies to which Prototype Warfare relates will change over time as new research delivers new experimental tools and techniques that can be applied to defence scenarios.

As a result, Prototype Warfare is less about the technologies themselves and more about the stage in their development at which they are introduced. The challenge is to find a way to do that safely, securely and effectively to achieve maximum operational impact.

Although not formally recognised as a current approach for the military, it is not an alien notion in UK defence. There are many examples over the past fifty years of prototypes being deployed in live environments – both for training and active combat – and our Special Forces regularly test, work with, and adopt early stage techniques and tools to ensure the success of their operations. It could be argued that the UK has been at the forefront in previous technology epochs in a way definable as Prototype Warfare. Continuing the practice and formalising the approach is perhaps not such a fundamental change.

# Why do it?

If Prototype Warfare can indeed allow us to integrate technology faster and better-adapt our way of fighting, its benefits will be realised by many in the UK defence community. From end users to procurement teams, the changes that prototyping brings have the ability to disrupt the status quo in a positive way.

## Users

One of the challenges for users is that the defence procurement cycle is so long that they rarely see anything but the final product. When they receive new equipment it has already been through years of review and adjustment. It is slow to arrive, often out of date, and is 'as formed', so they have little or no chance to input into its development.

Prototype Warfare gives users access to cutting-edge technology at pace. The shorter timescales associated with prototyping also mean users can be actively engaged in the procurement process. It provides them opportunities to feed into the optimisation and acquisition of technology that are not possible through existing approaches to defence acquisition. This empowers users, motivates them to draw maximum impact from the technology, and creates a stronger link between the user and the engineer behind the development. It also ensures their feedback becomes fundamental to their ability to fight and win better next time.

## Requirement setters

Both requirement managers and desk officers want to see the impact of their work framing requirements and creating programmes. The length of current programmes limits their ability to do so.

Prototyping shortens the feedback loop within these programmes, allowing requirement setters to identify evidence of their successes and failures quickly, helping them learn faster, and reflect those learnings back into their work within an appointment cycle to improve requirement accuracy. Faster availability of evidence increases accountability but it also empowers requirement setters to deliver greater impact in a shorter timeframe, energising the entire process.

## Procurement

Current defence acquisition approaches require procurement teams to place a premium on certainty by painstakingly defining a requirement and running complex and lengthy tendering processes.

This leads to an arm's-length approach to dealing with suppliers and a barrier between defence and industry that does not promote success in the field. Prototype Warfare recognises that certainty is not an option for experimentation and therefore allows procurement teams to place a premium on speed and early fielding instead.

Accelerating the process enables procurement teams to fail faster, learn faster, and therefore succeed faster, to rapidly reach the best verdict with more evidence to support that decision. And because prototyping is recognised across multiple industries as a powerful part of the development process, it helps build vital ties between buyers and suppliers in defence.

## Regulators

Often seen as reactive, regulators want to be more engaged earlier in the capability development process. Doing so will help them exercise greater judgement to help optimise the technologies, systems and tools marked for adoption. Prototype Warfare will give them

more opportunity to become actively engaged before technologies are moved into the final stages of design. It will also provide them with more evidence with which to qualify the technologies they are being asked to evaluate for deployment.

Regulators are highly experienced people who need to be engaged not marginalised. Prototype Warfare gives UK defence a proven way to make the most of their knowledge and expertise.

## In-service support

Whilst prototyping may add some support complexity it will also increase the amount of innovative technology used in the field and therefore stimulate the creation of new methods of supporting them in service.

Disrupting existing approaches and introducing novel technology engages support teams by helping them improve the impact they can have on users' operation of these cutting-edge tools. It makes them part of the overall success story.

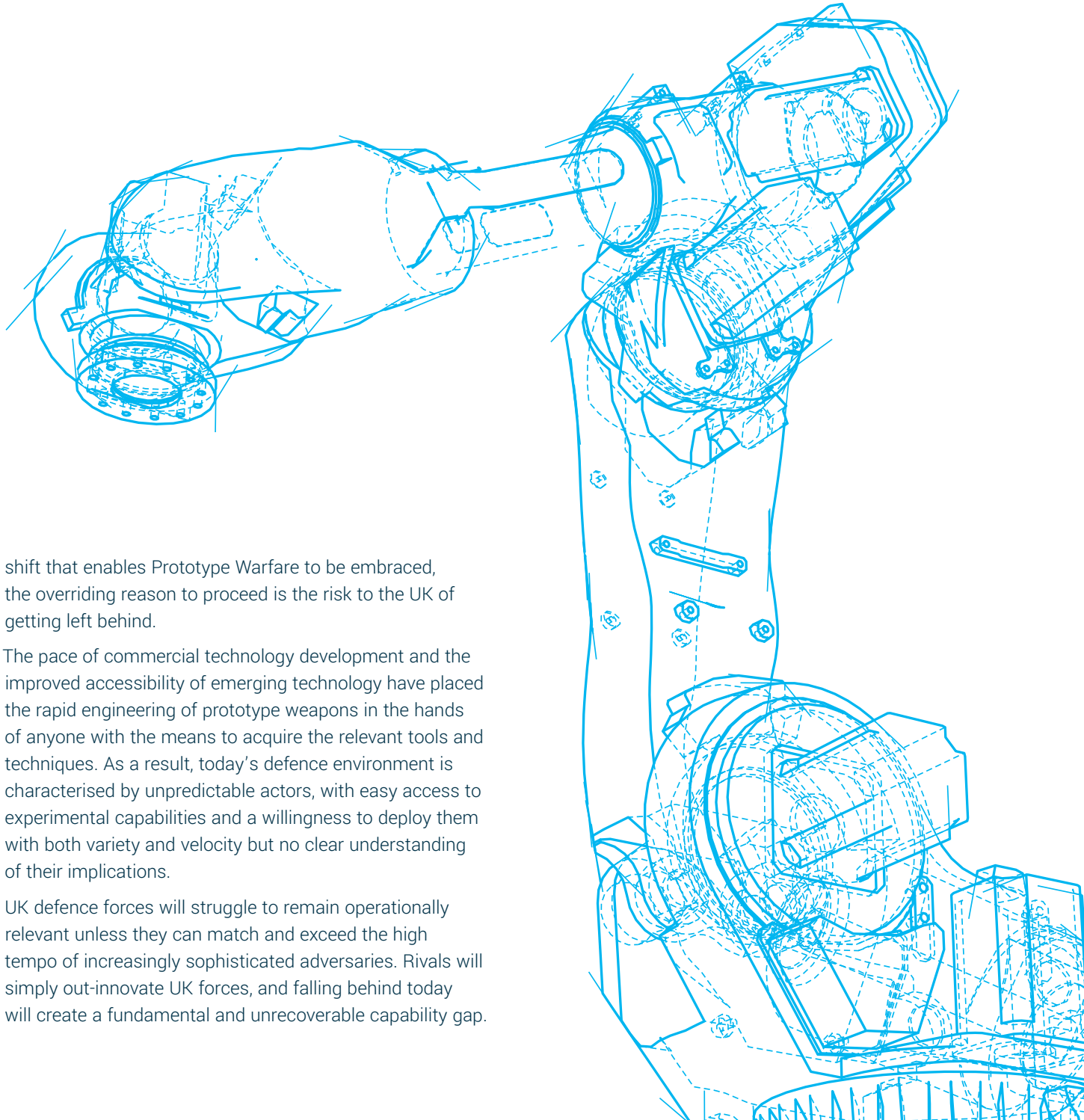
## Industry supply chain

A culture change around the adoption of prototyping would also place greater importance on the links between industry and defence. Industry's capacity for research and development, and its experience of using prototyping as part of continuous development and optimisation processes, is essential. As a result, industry can expect to become better aligned with the military mission, and more ingrained in the innovation process. This will put industry in a better position to demonstrate the need to build new models for research exploitation that recognise the value industry requires from participating.

Together these benefits make a compelling case for change. But beyond all the advantages of a cultural shift that enables Prototype Warfare to be embraced, the overriding reason to proceed is the risk to the UK of getting left behind.

The pace of commercial technology development and the improved accessibility of emerging technology have placed the rapid engineering of prototype weapons in the hands of anyone with the means to acquire the relevant tools and techniques. As a result, today's defence environment is characterised by unpredictable actors, with easy access to experimental capabilities and a willingness to deploy them with both variety and velocity but no clear understanding of their implications.

UK defence forces will struggle to remain operationally relevant unless they can match and exceed the high tempo of increasingly sophisticated adversaries. Rivals will simply out-innovate UK forces, and falling behind today will create a fundamental and unrecoverable capability gap.



# Prototyping in industry

Whilst the concept of Prototype Warfare seems novel for UK defence, prototyping in the commercial world is a well-established practice. Particularly in entrepreneurial organisations, the concept of build, measure, learn, and adapt is fundamental to failing fast in order to continually optimise. This process relies on an ability to experiment with prototypes in real scenarios to fully understand how new ideas perform in situ.

The use of prototyping in this way for product development, particularly in sectors where the cost of failure is high, such as aerospace and healthcare, indicates that defence should be able to implement a successful prototype culture that fits the current risk profile of military scenarios.

To better understand the experience of prototyping in non-defence environments we have spoken with organisations that have direct experience of its use. From start-ups to large public companies and cross-sector bodies, the message is that prototyping is an opportunity not a risk.

## Bob Bradley,
### Scaled Ltd

Dr Bob Bradley has been involved with some of the largest engineering organisations in the world. Today he runs Scaled, an innovative UK start-up that 3D prints objects at large scale for multiple sectors. As a specialist in additive manufacturing – industrial 3D printing – he has a deep understanding of why prototyping is so prolific in product development:

"Prototyping is about speeding up the process of getting to final design but people forget that it is also about reducing the cost of doing so. Prototypes give you a way to test ideas and concepts without committing to lifecycle costs at an early stage. These cost decisions can become prohibitively expensive to recover if the design spec changes late in the process. So prototyping allows you to hedge your bets – offsetting final quality for an earlier, cheaper way to learn and make decisions. It provides a way for you to make mistakes faster so ideas can become reality in time for them to have operational effect."

## Andrew Lytheer,
### Independent Strategic Consultant

Andrew Lytheer is a mechanical engineer by trade but has spent the last 15 years at the forefront of corporate strategic planning and communications at GKN. His work with every part of the product development process has given him a unique insight into the perception of prototyping in several sectors:

"Ultimately the value of prototyping is that it enables designers and engineers to have another frame of reference for the problem they are trying to solve. It's another route – because you are physically creating something that can be tested in the real world, to look at concepts and ideas and what happens when you actually use them.

"What you get from that is a fast, low-cost way to find obvious failure points by giving users and engineers a way to interact properly with an idea in the field. That's why it is seen as so valuable – because it allows you to understand more, learn more and answer fundamental questions at low cost and high speed.

"In the past this has also meant prototypes were of pretty low functional quality. But the emergence of smarter Fourth Industrial Revolution technologies, such as additive manufacturing, has changed the game completely by delivering a huge rise in prototype quality. So much so that the panacea of moving into single batch direct production without a defined prototype phase is very close."

## Sam Turner,
### CTO High Value Manufacturing Catapult

Professor Sam Turner is the Chief Technology Officer at the High Value Manufacturing Catapult, using his technical expertise and industry network to bring collaborators together and focus on innovation:

"Prototypes are an important vehicle for the introduction of new technologies. They present an opportunity to test and validate on shorter timescales and reduce the number of steps to production. They also enable us to quickly generate large amounts of data you cannot get from simulation and modelling alone. This helps us speed up the process and reduce risk.

"New technologies, particularly artificial intelligence, are becoming game changers for converting ideas and designs into real manufacturing processes at pace. They will also improve the quality to an extent where people are no longer distinguishing between prototype and full production capability.

"We will soon be able to simply make what we need when we need it and move straight into testing the performance in the real world. There are risks with experimenting in the field, but there must also be some risk associated with not gaining a rapid advantage if you have the means to do so."

# Why now?

There has always been an operational advantage to deploying novel systems and technologies against opponents, supported by novel tactics. The rapid shift in the US from basic research to full scale production of new missiles triggered by the demands of the Korean War, or the work to swiftly research and develop innovative countermeasures to improvised explosive devices in Afghanistan are both real-world examples. But UK defence has traditionally taken a more deliberate stance. Several changes over the past decade suggest that now is the time to review that position by augmenting traditional systems with the early introduction of prototypes based on emerging technologies with considerable potential:

## Pace of progress

Technology development outside of the defence arena is moving at breakneck speed. The acceleration of that pace is also startling. The emergence of a Fourth Industrial Revolution, underpinned by this rapid development of new commercial technologies, is highlighting a mismatch between the pace of modern innovation and the traditional defence acquisition process.

The UK defence community is in danger of falling behind more agile adversaries. In a global landscape characterised by political and economic uncertainty, and state and non-state actors alike seeking to blunt others' competitive advantage, this may not be a recoverable position.

## Variety of innovation

This extraordinary pace of innovation and its constant acceleration over the last 10 years has delivered an array of new technologies available for adoption. Many of these technologies are reaching maturity so the real-world technology opportunity today is greater than it has ever been before.

This world of emerging technology is very accessible for UK defence, enabling it to broaden the capability it can deploy and boost the chances of combatting opponents' attempts to erode its superiority. It now needs to adapt its position and bring these technologies into live environments early to determine what will and will not deliver real operational effect.

## Risk and cost reduction

The convergence of several advanced commercial manufacturing technologies, including additive manufacturing, advanced modelling and simulation, and advanced materials is dramatically disrupting product development. The result is cheaper rapid prototyping and a significant improvement in the quality of what can be produced at speed, making the introduction of prototypes in live environments lower risk.

These circumstances mean that adopting Prototype Warfare is now an appropriate way to adapt faster and smarter. Bringing emerging technologies and capabilities into live environments to supplement the UK's existing deterrent can provide a way to achieve decisive operational advantage.

# How do we make it happen?

Making Prototype Warfare a reality in the UK requires the defence community to overcome some practical barriers in the way it acts. In the next section of this report we make some clear tactical recommendations for how to mitigate the impact of those obstacles. But before we can make those changes it is essential to recognise that Prototype Warfare is first and foremost a philosophy of modern warfare and therefore requires the right military mindset. A cultural change has to underpin the tactical changes or they will not work.

## Mirror industry's positive perception

In the main, industry favours prototyping as an essential part of the development process. It considers it a low risk, cheap way to test concepts without committing to heavy lifecycle costs too early. Companies often see it as a way to make mistakes faster, address issues earlier, and learn quicker – shortening the entire innovation cycle. They are enthusiastic about the advances in rapid prototyping that will allow them to learn even more. UK defence needs to echo that view and move into prototyping with a positive understanding of how it will reduce cost and risk, whilst boosting quality, operational effect, and speed. Any perception that prototyping increases risk is outdated and reduces the capability of UK defence forces to counter the threat of modern adversaries.

## Augmentation not replacement

There must be greater understanding that Prototype Warfare is designed to supplement traditional capabilities not replace them. Prototyping in defence is about accelerating the process of enhancing existing capabilities rather than supplanting them with emerging technologies.

This change in perception affects more than just defence's technology choices; it affects everything from its interaction with industry to its procurement processes. For example, the idea of phased introduction, where assets are acquired in stages, each group being adjusted on the basis of the knowledge gained from the preceding deployment, promotes the culture that enables mistakes to be identified when they can have less impact on the overall outcome.

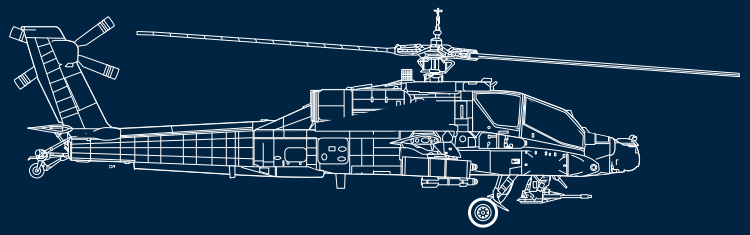
This test-measure-learn culture is fundamental to the philosophy of Prototype Warfare and mirrors industry's approach to capability development. Fostering greater understanding about how this achieves operational advantage, both now and in the future, will increase the defence community's appreciation of prototyping's role in modern warfare.

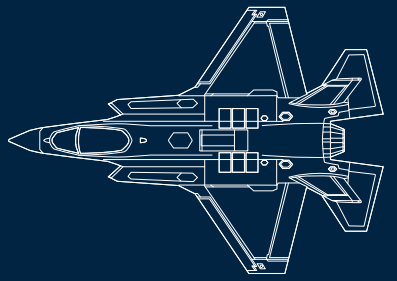
## Understand the scope of the opportunity

The vast pool of emerging technologies that defence organisations can now access could deliver a considerable tangible operational effect. Understanding the scope of innovations such as autonomous systems, machine learning, and robotics, and maintaining a working knowledge of the opportunities each represents is essential for successfully determining which to progress and which to avoid. Defence organisations will need to work closely with industry partners to test each technology's performance with suitable accuracy and build the knowledge required to make these decisions.

## Senior support

A new idea that requires both cultural and tactical changes cannot be achieved without a willingness from senior determinants to take the risks necessary to move from concept to reality. Prototype Warfare will not work unless the leadership adopts an alternative mindset that opens the doors for greater proactive experimentation in defence.





# Seven barriers to change

Along the way to instilling a prototyping culture, we will encounter practical barriers that will only be overcome by challenging certain perceptions and practices. In some cases we will completely change our way of working to accommodate prototypes, while in others we will need to take great care to ensure our use of technology remains consistent with fixed standards and protocols.

Having examined prototyping as a philosophy, we will next explore seven areas in which important questions must be answered to move it from concept to reality.

## Technology

Can a platform that is not fully mature really be effective in battle?

## Users

Do end users trust prototype platforms and understand how to work with them? Will prototyping create a disproportionate training burden?

## Safety

Can we deploy prototypes on the frontline without endangering users or civilians and their property?

## Ethics

Are we able to match adversaries' pace of technology deployment without compromising our ethical standards?

## Regulation

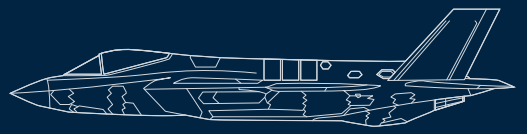
Could inflexible laws impede our ability to defend ourselves?

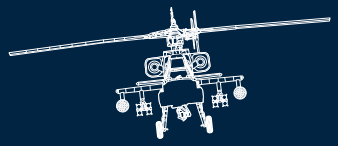
## Procurement

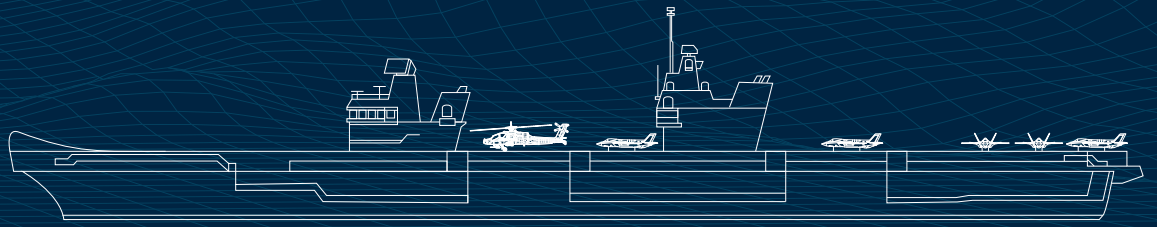
Are defence's procurement culture and processes compatible with acquiring equipment quickly to counter immediate threats?

## Security

Is it possible to incorporate prototypes into our arsenal without creating physical and cyber security vulnerabilities?







# Overcoming barriers:

# Technology

A prototype warfighting capability will be fielded without having been through a typical assurance process – either because it is still in the early stages of its development, or because it was conceived for commercial purposes and is being adapted for use in defence.

The bar for assuring systems for deployment in a defence environment is traditionally very high, raising obvious questions as to whether a prototype can ever be robust and secure enough to be effective in battle.

The answer is that it can – if supported by the right practical measures and a shift in the way we think about battlefield technology.

## Reframing risk

It sounds paradoxical, but in seeking to avoid risk we may inadvertently create more. The safe option is not always the most advantageous.

A platoon may avoid immediate danger by taking cover in a trench, but staying there allows the enemy to organise, increasing the risk of being overrun. Only by putting itself in harm's way can the platoon exercise its advantage. In the technology world, rather than accept a new capability that may have vulnerabilities, we tend to favour familiar capabilities, even when they are known to be vulnerable. Clearly there is an argument that a known risk is easier to mitigate than an unknown one – but instead of taking the binary view that 'known risk is good' and 'unknown risk is bad', we must weigh up the potential risk against the potential reward and to decide whether it is proportionate.

## Don't panic if the tech is flawed

The quest for perfection leads to developmental inertia. Hypothesising about all possible weaknesses and hedging against them prior to deployment is a time-consuming endeavour and, if there is no strong agreement on the acceptable level of risk, can stall a project indefinitely. To instil a prototyping culture we must stop viewing failure as something to be avoided at all costs and start embracing it as something that can be useful if it happens safely and responsibly, and if we move on from it quickly.

We must also become comfortable with the idea that the technology we rely on may have flaws. Subconsciously, we do this already. For instance, we know a radio can be jammed, but it is still considered a vital and trusted piece of equipment. One vulnerability does not render a piece of technology useless.

## The supporting ecosystem

The use of imperfect technology will place additional value on the architecture that surrounds it, and will require mental agility from the user.

The following factors will contribute to a supporting ecosystem that will de-risk deployment and ensure continuity during operations:

- **Training** – an educated and sufficiently skilled user will not be fazed when a new piece of technology behaves in an unexpected way, but will have the knowledge and confidence to adapt operations accordingly, and be empowered to do so.
- **Testing and evaluation** – uncertainty about a technology's performance is greatly reduced by building a body of evidence to demonstrate its expected capabilities and limitations. Test and evaluation programmes may be accelerated by placing greater emphasis on computer modelling and simulation. Data will be collected throughout testing and deployment, and fed back into the cycle to inform training and further development.
- **Post-deployment support** – the product developer's role will not end at the point of delivery to the user, but continue as part of an ongoing cycle of user feedback and capability enhancement. This may be facilitated through contracts for comprehensive technical support, or through alternative ownership models such as leasing.

New technology will not be introduced straight into the harshest environment, but deployed progressively, with lessons from each phase informing improvements to the next. Because the prototype is designed to augment and not replace existing capabilities, the user can always fall back on established concepts of operation in the event of technical failure.

## Integration and interoperability

To realise its potential, a prototype must fit into the command chain, complementing all the other technological and human elements in the battlespace. Deploying a prototype capability will rarely be like introducing a standalone item .

For instance, unmanned platforms are tasked from their understanding of the environment, and so need to draw information from the network. Payloads and sensors generate information and feed it back into the network to build an intelligence picture and task unmanned platforms. The whole system works together to reduce operator workload and cognitive burden, enabling better decision making at pace. All this can be achieved only if the constituent parts are integrated and interoperable.

Achieving this integration is likely to be a challenge, as introducing a new capability into a network of systems can have cost, security and commercial implications, as explored in the subsequent chapters of this report.

If due consideration is given to these implications, and sufficient investment devoted to targeted integration, it need not be a barrier to deployment.

## Perception of technology

It is not enough for prototyping to be effective – it must also be seen to be effective. Sceptics may seek to establish a narrative that troops are being sent to the front line ill-equipped with underdeveloped technology. We must seek to counter this by clearly explaining the rationale and illustrating the benefits.

This will be achieved by openly communicating our thinking via journalists, MPs and other influencers in the public sphere.

# Overcoming barriers:

# The User

Putting the right technology in the wrong hands risks negating all progress made up until the point of deployment. A promising capability will never realise its potential if the end user is unable or unwilling to fully engage with it.

User barriers to deployment will manifest in two ways:

1 **Insufficient knowledge**

The UK Ministry of Defence applies various measures of readiness relating to both technologies and systems for new capabilities. The lowest levels of readiness require only the exploration of a concept, while the highest demands full qualification and demonstration under mission conditions. When users receive a new prototype, they will need to know where on which scale it sits if they are to understand how to work with it. Insufficient understanding of a technology's abilities and limitations could lead to poor choices when faced with critical decisions about where, when and how it should be deployed.

Education must extend beyond the end user and up the chain to the strategic decision makers. An informed customer base, well-versed in high-tech systems, will be fundamental to smart requirement setting and procurement choices.

2 **Resistance to change**

The force of human will should never be underestimated. When that will assumes the form of resistance, it only takes a minority to outgun advocacy and block its advance.

We tend to encounter the strongest resistance when a person feels threatened – for instance, by a new technology that could challenge the existence of a field squadron or an individual role. In World War II mechanisation and air combat shone a light on how to win – but despite the new technology offering a significant tactical advantage there were those who continued to resist.

Of course, air combat became the norm once it became obvious the advantage it offered, and the same will happen with the technologies of today that are currently being eyed with suspicion. But the speed at which that transformation happens depends on the number and, more importantly, the spread of the status and role of those advocating change.

Half-hearted adoption by those on the front line will lead to powerful technology being underexploited, but a small, determined group of opponents that wields influence high up within the public sector could prevent it from ever reaching the battlefield.

There are a number of aggravating factors which, if left unchecked, will increase the knowledge deficit and reinforce users' unwillingness to change:

- early scepticism and a lack of trust in 'unproven' technology
- acceptance of the prototype, but uncertainty about how to use it
- 'adoption fatigue' from cont inually learning and adapting to new systems
- disenfranchisement, prompted and reinforced by negative experiences

Failure to address these issues will further inhibit adoption of prototyping and the implementation of a culture that supports it – however, there are a number of tactics that we can employ to prevent them or minimise their impact:

## The golden rule: involve the user

Bringing the end user into the development cycle is the surest way to pass on knowledge while nurturing trust and advocacy. Offering first-hand experience of the design and testing process, and the opportunity to influence it, encourages the following outcomes:

- demystifying the decision-making process, building trust through transparency
- educating the user in real time, reducing the training burden prior to deployment
- instilling a sense of pride and ownership, laying the groundwork for advocacy

It is also advantageous for the developer, who benefits from direct access to the product's most important critic. The end user can critically assess the technology's ability to fulfil its objective, creating a live feedback loop that enables continual review and improvement.

## Counter scepticism with evidence

When a new technology is introduced, no user should ever take it on faith alone that it will be safe and effective. The burden of proof sits squarely with those extolling its virtues, which places a hefty premium on empirical evidence.

This evidence should be generated through robust testing and evaluation programmes, during which meticulous performance records are kept and regularly shared with the user. A method of capturing and exploiting user feedback must be built into the programme. If a doubt is raised the creator must not give unwarranted assurances, but provide an honest appraisal of the technology's ability, based on transparent and explainable data. All this empowers the user to make informed decisions with confidence.

## Provide a meaningful alternative to formal operating standards

While the International Organization for Standardization (ISO) standards for user participatory design do exist (ISO 9241-210), the absence of standards specifically for prototypes in defence may be seen as a problem.

Anything less than precision may be deemed inadequate, under the assumption that technology developed for critical applications must have an exact specification against which to measure its performance.

By the very nature of prototypes, it will not always be possible to provide an exact specification. The key is not to provide a specification of the technology itself, but of its intended effect – for instance, its operating range. This approach is already practiced by the UK Ministry of Defence.

By accumulating empirical evidence through modelling, testing and evaluation it is possible to qualify – perhaps even quantify – its probability of success in a given scenario. The user then has a performance envelope to work with when deciding whether or not to deploy it.

## Make the technology intuitive

People form habits around familiar technology, and when forced to break them are prone to hesitation or interaction error – both of which are highly undesirable in battle, especially under pressure.

The challenge here is that in designing something to accommodate users' existing habits and preferences, we end up with a variant on an incumbent capability instead of trying out a disruptive new one.

Take for example the familiar QWERTY computer keyboard layout, conceived to prevent type hammers on early typewriters from colliding and getting stuck. Since the introduction of the electronic keyboard, more efficient layouts have been devised, but the short-term disadvantage that comes with 'reprogramming' the reflexes of the world's touch-typists trumps the long-term efficiencies of the new layout, and so we find ourselves tied to the suboptimal version.

In defence, we need users' operation of technology to be second-nature, but don't want the tactical disadvantage of using suboptimal capability. So, do we keep designing capability to accommodate users' habits at the expense of progress, or demand that users break their habits at the expense of responsiveness?

In fact, habit-breaking and intuitive design are not mutually exclusive. By involving users in the development cycle and training them iteratively, new habits will form in parallel with the prototype's evolution.

## Start with a receptive user

Some users will adapt to a prototyping culture more easily than others. A difficult first deployment can leave a lasting negative impression, so we should seek to work first with individuals who are receptive to new technologies and present the right skills and behaviours to deploy them successfully.

These individuals will have a high tolerance for uncertainty and setbacks, and will speak the language of both engineers and troops. They may take up a new position as a special prototype warrior, who is not part of the development team and is not the end user, but who bridges the gap and facilitates the technology's transition between the two.

To identify and recruit these individuals, the employer will need to implement competency assessment programmes, embedding psychologists within the ranks to recognise employees who demonstrate the right qualities. A successful candidate will encourage wider advocacy by generating and communicating positive outcomes, and building a body of evidence in support of the prototype warfare approach.

# Overcoming barriers:

# Safety

Safety must never be dismissed simply as a barrier to overcome, but embraced and integrated into the whole development cycle. Failure to do so creates risk, and we have a collective duty to ensure any prototype destined for the front line does not endanger the user or civilians and their property.

Linked to our duty to safeguard against physical harm is the need to preserve users' trust in the technology. Every incident that occurs as a result of safety failings will fuel suspicion of prototype technology, leading to its underutilisation in theatre and adding weight to the arguments of those who seek to undermine it.

Safety need only be a barrier if it is implemented poorly – so how can we ensure we do it well?

## Safety legislation: help or hindrance?

All new machinery deployed within the European Union must, by law, comply with the relevant EU supply directives, generally enacted in the UK by specific regulations – for example, the Air Safety Regulations. A new technology is certified compliant when the manufacturer or a similarly responsible party issues a Declaration of Conformity. This takes place upon completion of a rigorous assessment process, in which the participant must show that all obligations have been met. These obligations include:

- complying with all relevant essential health and safety requirements
- producing comprehensive user instructions
- demonstrating in the technical file how compliance has been achieved

On the face of it this appears incompatible with prototyping, for the following reasons:

1. The technology will be compliant with all health and safety requirements at the point of deployment – but we are urging the user to experiment with new concepts of operation that were not considered during the assessment phase.
2. By issuing comprehensive user instructions we risk becoming too prescriptive and stifling user innovation.
3. The concept of a technical file assumes the product will be handed over to the user in its final form. This is not sufficient in cases where the design process will continue beyond the handover.

However, there are existing routes that enable capability to be deployed rapidly in a way that is consistent with health and safety legislation, generating precedents that we can point to as examples of good practice.

## Exceptions to the rule

To achieve the degree of flexibility required to make Prototype Warfare viable, we will need to shift away from rigid certification requirements and towards provisional safety cases and caveated operating envelopes, both of which must be allowed to evolve as the technology is used in the field. This is not completely unknown territory – it is similar to the approach adopted by the UK Ministry of Defence for Urgent Operational Requirements (UOR) in Iraq and Afghanistan, replaced by Urgent Capability Requirements (UCR) in 2016.

The Health and Safety Executive (HSE) also offers an exemption to the armed forces for certain requirements deemed critical to national security, although in reality it is rarely exercised. This exemption must be personally authorised by the Secretary of State for Defence.

There are also certain exemptions for research purposes or temporary laboratory use – but we mustn't forget, the ultimate aim is to field a product the military can use, safely.

We often see real-world examples of operations conducted before qualification is complete, which could serve as templates for the Prototype Warfare approach. For instance, when taking a new weapons system to a range for testing, we face an apparent Catch-22: we need to know that it's safe to fire, but can't prove that it's safe without firing it.

Draconian legislation would make this dilemma unsolvable, rendering the activity impossible – but in reality, the built-in provisions mean it can be achieved.

## A different approach to risk

When fielding prototypes, we may be working without predetermined safety standards, meaning risk must be managed in other, smarter ways. This starts with the supplier and customer acknowledging that nothing can ever be 100% safe, but agreeing between themselves how much risk they are willing to accept.

The health and safety concept 'as low as reasonably practicable' (ALARP) enables the setting of goals based on a cost-benefit analysis in which we weigh up the risk against the time, effort and expense required to manage it.

Although the term 'as low as reasonably practicable' may sound like the starting gun in a race to the bottom, there are numerous safeguards that can prevent that from happening:

1 **Build trust through evidence**

In the absence of a formal safety case, the user will rightly insist on alternative assurances that the product does not pose a disproportionate risk to life and limb. It is likely that customers' demand for evidence, acquired through rigorous test and evaluation programmes, will increase as decision makers seek to compensate for less specific safety standards. A supplier's ability to present a large body of credible evidence will be instrumental in reassuring the end user that the technology is worthy of their trust.



**2 Make virtual mistakes**

Test and evaluation programmes need not exist exclusively in the physical world. Risk in the early stages of development can be greatly reduced by modelling predicted performance and conducting simulated trials in a synthetic environment.

This philosophy can be extended to user training. By introducing the user to the prototype in a virtual world, the user can push the technology beyond its safe operating thresholds to gain an understanding of its limits, before trialling it in a live environment where the stakes are higher.

In turn, the developer can observe how users interact with the technology, how they react in emergencies, and ways in which they deviate from the suggested concept of operations – then manage any risk accordingly.

**3 Educate and empower the user**

If we are to deploy technology without a complete safety case, we will only achieve ALARP if we empower the user to exercise judgement. Overreliance on checklists and instruction manuals has, in the past, led directly to serious safety lapses – some fatal.

In instances where changing circumstances force users to alter the way they use a product, the criteria for safe operation will almost certainly shift. Once the mode of operation has changed, the behaviours required to meet the agreed safety standards should no longer be considered adequate. Users' application of good judgement should bridge this gap.

To achieve this we need to train users differently. Instead of a prescriptive approach, which conditions the operator to resolutely follow a mandated procedure, we should train users to understand the functions, limitations and risks of the technology and apply that knowledge to make informed decisions within an agreed framework. Users must also be granted sufficient authority to make those judgements and act on them decisively.

**4 Invite continuous feedback**

Improvements to a prototype's safety must not cease once it is handed over to the user, but continue throughout deployment in a constant cycle of enhancement. To facilitate this, the supplier must provide the user with the means to record safety concerns that arise in service, and offer a channel through which to report them.

Hosting the prototype's technical file and hazard logs in the cloud and granting the user access to them upon handover will enable live relay of emerging issues and allow an audit trail to be maintained throughout the development cycle.

**5 Build in fail-safes**

Given that prototypes cannot be fielded with the same degree of assurance as established technologies, it will be vital to identify potential problems during the very first concept stages and factor appropriate fail-safe mechanisms into the design. These can be physical (such as a kill switch) or procedural, and may not need to be complex or costly to be consistent with ALARP methodology.

# Overcoming barriers:

# Ethics and perception

Rogue states and non-state actors will not let ethics stand in their way when seeking to use new technology to cause harm. In August 2018 we saw commercial drones used as improvised airborne explosive devices in an attempt to assassinate Venezuela's president, Nicolás Maduro. He is unlikely to be the last target of such an attack.

While we are taking our time to do things ethically, adversaries are gaining advantage by adopting technology faster, in ways that threaten our safety.

We must stay ahead of the pace of changing threats – but does our duty to protect our citizens and troops necessitate relaxing our ethical standards?

## Conquer the ethical high ground

The only acceptable answer to this question is a decisive 'no' – there is no justification for relaxing our ethical standards.

Aside from the ethical case for doing the right thing, there are several practical incentives:

- Delivery of a product that breaches sanctions or is likely to be used in human rights violations will incur substantive legal and financial penalties, cause severe reputational damage, and will limit the vendor's ability to operate in international markets.
- Visibly occupying the ethical high ground is vital in maintaining public and political support. Swimming against the tide of opinion makes progress slower, not faster.
- Doubt in users' minds that a capability is ethically sound will demotivate them and cause them to hesitate in deploying it, reducing its effectiveness.

It is clear we must adapt – but in doing so we must become smarter, not reckless, and move faster without compromising our values.

## Tackling the asymmetric threat

While it is true that an imbalance in the application of ethical standards gives an edge to those willing to play dirty, for us to sink to the same level, or get drawn into an eye-for-an-eye exchange, would be a serious mistake. We must seek to counter the threat, not match it.

Our response to adversaries' use of aerial improvised explosive devices cannot be to produce something equally damaging – we must instead use our technological superiority to develop novel counter-UAV solutions that

can neutralise adversaries' unethical tactics. The value in prototyping is in ensuring we can deploy countermeasures as quickly as the enemy is able to develop threats, removing their unfair advantage.

## Drawing red lines

The legality of an action is sharply defined, but its ethicality can be more ambiguous. There are tactics permitted by law that may be considered unethical, so it's important for an organisation to clearly draw the lines it is unwilling to cross.

An organisation can take the following steps to formalise and enforce these red lines, granting enough autonomy to enable ethical practice without blocking progress:

- Set up a Business Ethics Committee, comprising Board members, corporate responsibility professionals, legal advisors and other key stakeholders.
- Agree an independent principles charter, with Board approval, specifying what outcomes the organisation deems unacceptable for its prototypes to enable.
- Share the charter with all employees and stakeholders to secure buy-in and open a line of communication through which they can seek advice and report breaches.
- Implement a 'triage' approach, based on a robust framework, to quickly assess developing ethical issues and identify those which must be escalated to the Board.

## Future-proofing standards

The nature of the Fourth Industrial Revolution means technologies and attitudes towards them will evolve quickly. This accelerated pace of change will present the following ethical challenges for prototype developers and users:

- A lag between the emergence of a capability and society's consensus on its ethical implications may create a window in which the prototype can be deployed with minimal scrutiny. An organisation must resist exploiting this window, or risk finding itself on the wrong side of history once the debate has caught up.
- In setting its ethical standards, an organisation should not hold itself hostage to the zeitgeist of the present day. Technologies throughout history have made the transition from resistance to acceptance. As long as no red lines are crossed, standards should not block development of technologies that are ethically justifiable, but to which society is not accustomed.

Defence organisations will need to maintain a keen awareness of technological and ethical trajectories if they are to avoid these pitfalls and prevent their standards from becoming obsolete. This requires a commitment to issues-monitoring and horizon-scanning, through both in-house research and by leveraging public resources, such as the UK Ministry of Defence's 'Global Strategic Trends out to 2045' report.

Ethics and policy must not wait for the problem – we need to go out on the front foot. Corporate responsibility and risk professionals should be involved throughout the product development cycle, and the prototype's developers should offer full transparency by unambiguously communicating their intentions.

## Real vs. perceived ethical issues

There is a need to disentangle genuine ethical concerns from those which are merely the product of factors such as:

- media sensationalism – for example, depictions in popular culture of artificially intelligent systems rising up against humanity
- popular misunderstanding, which can arise from ambiguities in the language used to describe new technologies – for instance, 'autonomous' being taken to mean 'self-governing', when in fact there is a human decision-maker in the loop

Failure to address these issues may result in unnecessary delays to the delivery of capabilities which are urgently needed on the frontline.

Managing perception may sound like a publicity exercise, but a well-informed legislature and electorate are vital allies in achieving the right blend of accelerated progress and moral stewardship. Being transparent and offering critics opportunities to learn about new technologies, like live demonstrations, are crucial in obtaining trust.

To develop public and government thinking, defence organisations will need to be thought leaders – calmly and persuasively leading the public and government in a direction where the ethical issues around prototypes and innovative solutions are understood.

# Overcoming barriers:

# Regulation

As technology advances and the rate of innovation accelerates, regulation will need to evolve in tandem or it may begin to restrict our ability to exploit innovation that is vital to our national security. We must strike the right balance between adhering to the fundamental tenets and retaining the flexibility to rise to emerging challenges.

## What cannot change?

The fundamental tenets to which we must adhere are separate to national regulation and outlined in international law; for example, the Geneva Conventions, Hague Conventions, and the Law of Armed Conflict.

While there will be much discussion about how specific international laws should be interpreted in relation to emerging technologies, the technology will mould to fit these laws, not the other way around.

The ultimate standard when designing a new capability or defining the rules of engagement surrounding its use is compliance with these laws.

## What can change?

There are opportunities for greater agility in the drafting and application of operational regulations, governed by such bodies as:

- Civil Aviation Authority
- Defence Maritime Regulator
- Health and Safety Executive
- Maritime and Coastguard Agency
- Military Aviation Authority

New technologies have always pushed these regulatory boundaries, and the regulations have always adapted to accommodate them. But navigating the process faster will be crucial if we are to match the pace of change set by adversaries in the Fourth Industrial Revolution.

## Pulling in the same direction

We must not get drawn into the trap of seeing regulations as a hindrance, but instead respect their necessity in enabling operations to be conducted safely and responsibly. Equally, regulators must understand that we are not seeking to evade these responsibilities in deploying prototypes, but to achieve outcomes faster without compromising on standards.

Operating prototypes in a real-world environment will require energetic engagement between the experts in defence and those in regulation, with risk and safety at

the centre of the discussion from the outset. There is no substitute for open and honest conversation – both parties ultimately want the same result, but will only achieve it through close collaboration.

## How big is the regulatory challenge?

It is important not to overstate the extent to which regulations prohibit prototype deployment, as many existing laws are broad enough to make provision for the introduction of new technologies. For example, if a driver using an ordinary car causes injury through negligence, they are liable under existing laws. Negligence at the controls by an unmanned ground vehicle operator can be dealt with in the same way.

Similarly, if a newly installed home boiler explodes, the manufacturer or installer can be punished if found to be at fault. Failures when deploying a new technology should be treated no differently, and so liability and the threat of prosecution will necessitate a degree of self-regulation within industry.

Responsibility for accelerating the regulatory process does not lie solely with the regulators – it will often be incumbent upon defence to become quicker at proving that new technology is compliant with existing laws.

However, the extent to which regulation does prohibit activity will vary according to the technology in question. For example, regulations around unmanned ground vehicles will have to break new ground, while those for unmanned aerial vehicles are comparatively well-established under civil and military aviation regulations.

For some emerging novel technologies, there will be no existing use case or back-catalogue of experience. Where new technologies expose such regulatory gaps, we will need to be more creative in how we test and evaluate them.

## Tactics for faster assurance

There are several available tools and practices that can support a streamlined route to regulatory compliance while maintaining high standards:

1. early engagement with regulators to understand what is required from the assurance process, so it can be shaped accordingly
2. computer modelling to predict the performance of a prototype and the risks of deploying it. This will quickly rule out those which are unlikely to be compliant
3. synthetic testing to build confidence that the prototype complies with existing regulations. For instance, it is possible to place a virtual unmanned surface vehicle in a simulated shipping lane and monitor a year's worth of behaviour in a very short space of time, to see whether it is compatible with collision regulations
4. live testing on ranges and in other segregated spaces to establish systems' operating limits by exceeding them in a safe environment

These might not be used in sequence, but individually or concurrently depending on risk. It is the defence sector's responsibility to do what is necessary to satisfy the regulators by clearly defining the rules of engagement, training standards and operating limits.

We also need to provide a route for progression into the real world. For example, it is not enough to fly unmanned aircraft solely above a range in segregated airspace – we must work towards integrating them into civil airspace, and this is where engagement with the regulators is absolutely essential. This engagement should continue into and beyond the prototype's deployment to encourage an ongoing cycle of review and improvement.

## Regulation as a fig leaf

Regulatory barriers may be put up by people for whom the regulations aren't actually the problem. Decision makers who have a personal or political objection to an emerging technology may hide behind regulation in an attempt to obstruct its route to acceptance. As outlined in the Ethics and User chapters, we must attempt to turn sceptics into advocates by being transparent about our intentions, educating them about the benefits of our approach, and providing empirical evidence that it works as well as we claim.

## Interpretation and international disparity

It may not always be clear how existing regulations apply to a new capability. For example, Maritime Coastguard collision avoidance regulations are written from the perspective of people on board ships, assuming there will be someone maintaining a lookout. What does a 'good lookout' mean for a vessel that has nobody on board?

This ambiguity is compounded by the fact that the rules for operating unmanned surface vehicles in mixed maritime traffic areas are different in every country. There is no international agreement or common approach.

Fortunately, there are already strategies in motion to tackle these issues. The Maritime Autonomous Systems Regulatory Working Group interprets existing legislation and rules to see whether they are adequate for modern operations, and then approaches the United Nations' International Maritime Organization to flag up inconsistencies. Similar approaches have proven successful in enabling unmanned aircraft, like Protector, to fly in UK airspace.

These provide examples of best practice that regulators in other sectors can emulate.

# Overcoming barriers:

# Procurement

Procurement – the process of specifying, acquiring and supporting materiel – is traditionally an area where governments invest a lot of time and money. In defence, the system is optimised for precision and certainty, tending to prioritise performance over time and cost.

This current approach makes sense when bringing submarines or aircraft carriers into service, where there is a need to produce an acceptance specification and assure the asset for 20 years or more. But such a process is incompatible with tackling short-term threats, which may evolve beyond recognition or even disappear within a year or two. The requirement is to act immediately.

Prototyping is designed to explore potential. It prioritises acting at high speed and at low cost, compromising on performance in the early stages of development. But how can defence make the shift to this way of working?

## A precedent

From the turn of the century, UK defence successfully conducted multiple accelerated procurement programmes in the form of Urgent Operational Requirements (UOR), to fill capability gaps in Iraq and Afghanistan. The UOR was superseded by the Urgent Capability Requirement (UCR) in 2016.

UORs were as much for novel technologies as they were for proven technologies. For example, the threat from Improvised Explosive Devices (IED) spawned a programme to deploy a ground-penetrating Doppler radar, fitted to the front of a Land Rover, which could detect freshly laid command wires underground and alert the driver to stop.

Defence has proven it is capable of procuring innovative technologies quickly in response to fast-emerging threats. The difference in the Fourth Industrial Revolution is that low-tech IED-style threats are becoming more diverse, more prolific, and more dangerous. Rather than employing the UOR approach as a reactive tactic, it needs to become a continuous proactive strategy and culturally ingrained.

## Greater flexibility in processes

There must be a realisation that existing processes are not set in stone and must be allowed to evolve to accommodate changing circumstances. A process is usually put in place by an intelligent person for a good reason – but the architect would probably admit that a

process they devised a decade ago was not designed with modern circumstances in mind.

Rigidity in process can lead organisations to hold themselves hostage to it. Ultimately, a process is just an idea created by a human to solve a specific problem at a specific time – there is nothing that says another human cannot amend or replace it. Employees should be empowered to challenge processes by moving from a hierarchical management culture, in which communication flows exclusively down, to one where feedback is encouraged to flow back up the command chain.

## Horizon scanning

Essential to moving from a reactive to a proactive procurement culture is an acute understanding of current and future threats.

Defence research organisations like the Defence Science and Technology Laboratory (Dstl) in the UK and Defense Advanced Research Projects Agency (DARPA) in the US already lead the way in this domain. Collaboration with such organisations should be accompanied by investment in trend monitoring and intelligence in-house.

## SME culture, corporate resilience

Small and Medium-sized Enterprises (SMEs) have a less bureaucratic culture than large organisations, meaning they are better at making quick decisions and developing solutions at pace – but their solutions often lack scalability, and the companies are less resilient, creating risk. The answer for large organisations that find themselves becoming sluggish is to instil elements of culture that make SMEs agile, such as:

1. **The sandbox approach** – rapid experimentation and prototyping can be facilitated by allowing it to operate independently of the normal buying process, within a separate environment and in a freer way.
2. **Breaking down silos** – good ideas can get swallowed up in large organisations, but reducing the physical and figurative distance between employees can facilitate the flow of ideas into practical solutions.
3. **Succeeding by failing faster** – we should not be reluctant to set out on a path that may lead to a dead end, but learn to be comfortable with imprecise specifications. If concepts are going to fail we must allow them to do so quickly and at low cost, and then move on rather than clinging to a mistake because it took a lot of time and money to make.
4. **Clarity of purpose** – success starts with an acute understanding of what needs to be achieved. Progress should be mapped out via bold short-term targets and measured against clear criteria. Employees should then be empowered to deliver the specified outcomes in a flexible way, rather than having to follow a mandated process.

## Competition vs. collaboration

Defence procurement has a strong preference for competitive bidding, based on a legitimate need to ensure contracts are awarded fairly and on merit. While this remains an important aspect of the acquisition process, to introduce it too early can stifle innovation by encouraging competing organisations to jealously guard their ideas and develop solutions in silos. A collaborative phase prior to competition will allow bidders to form partnerships that enable them to bring together complementary products and ideas, resulting in a more rounded and effective capability. Introducing prototyping into this collaborative phase will promote early troubleshooting and give concepts space to evolve, minimising the risk of the buyer making a long-term commitment to a costly white elephant.

To facilitate this approach, the buyer must be rigorous in its requirement-setting to keep the collaborators focused on delivering a solution that is fit for purpose but does not exceed the requirement. However, it must also be open-minded in its evaluation of bids, accepting that the solution that best meets the requirement may diverge significantly from early predictions.

# Overcoming barriers:

# Security

Failure to support the deployment of prototype technology with an adequate security strategy could have extremely damaging implications.

As technologies become increasingly connected, we must ensure the introduction of a new device does not provide hackers with a route into the network, through which they can disrupt the wider system.

In the physical domain, we must not allow our enemies to boost their own capabilities by capturing, studying and replicating ours.

Given that prototypes will be fielded following a less intensive assurance process than is typical for an advanced capability, will it be possible to incorporate them into our arsenal without creating vulnerabilities?

## Mitigating the cyber risk

Intuitively, the more sophisticated a prototype, the greater its ability to ward off attack – but in fact the converse can be true. Physical platforms increasingly acquire data from the external environment via sensors and other input sources, each of which is a potential target for a cyber-attack. Greater complexity creates more opportunities for hostile parties to penetrate the system and influence its behaviour or performance, making it absolutely imperative that cyber security be built into the development of any complex system. This can be achieved by engaging cyber security experts at the very start of the process and keeping them involved throughout.

## Safeguarding physical security

Cyber security is vital in preventing loss of capability or data, but redundant if the enemy is able to physically seize or destroy the asset. If a prototype unmanned vehicle is navigating the battlefield unaccompanied, what is stopping it from being picked up and taken away?

A robust physical security policy is just as important as cyber security and should not be enacted in isolation, but as part of an integrated, whole-system approach.

This is compatible with a strategy in which prototypes are used to augment existing tactics – for example, unmanned surface vessels as escorts to manned vessels in a high threat environment.

The degree of oversight required will vary according to the mission, based on the commander's assessment of the potential risks and benefits.

A very new unmanned capability will not be thrown straight into the harshest environment, but initially operated within a limited radius of base. Once its performance is better understood, or in situations where the benefit of deploying it outweighs the risk of its damage or loss, it will be deployed increasingly remotely.

## Exploiting simple systems

One solution to both of the above issues without creating a disproportionate security burden is to embrace simplicity. A prototype does not necessarily need to be complex to fulfil an objective – in fact there can be considerable benefits in deploying low-value assets:

- if hacked or captured, a low-tech device does not reveal any useful intelligence to the enemy or provide them with an advantage if used in retaliation
- if lost in action, there is no need to risk lives by sending personnel in to retrieve it
- ease of manufacturing and a lower threshold for assurance save money and enable quick replacement in the event of loss or damage

To leave assets unattended on the battlefield is not unusual – automatic rebroadcasting stations and sound ranging equipment are often left behind, and this can apply to the maritime environment as well. If a product can be both effective and disposable, to over-engineer it may create unnecessary security risk.

## Maximising value through integration

While a single low-capability asset may be of limited benefit, deploying multiple units as part of a co-operative network increases their effectiveness and reduces the security risk. As with an army of ants, an attacker can immobilise a number of individuals but the system as a whole remains effective.

Another benefit of an integrated system is the ability to simultaneously monitor all its constituent elements and flag up any that are behaving anomalously. For instance, when installing a new software package on a fleet of unmanned air surface and sub-surface systems, we can compare the performance of all the units in operation to identify when one may have been compromised.

To implement this approach securely and effectively, open architecture is needed that enables new technologies to immediately 'plug in' to the network and be operated via a simple user interface.

## Achieving secure integration

It may seem as though by allowing prototype systems to be introduced to an established network, a single rogue element could compromise the whole system. However, modern mobile communications technology provides an analogous model that demonstrates how open architecture can be secured:

- Google owns the Android operating system, which can be installed on any compatible device.
- Via the operating system, Google is then able to place specific limitations on what the device can do.
- The package is designed to facilitate custom augmentation by allowing the user to select applications from independent third parties.

In a warfighting scenario, the 'operating system' can be as secure as the mission requires, and can set the operational boundaries for platforms under its control.

Cyber security measures built into the system as part of its design can prevent infected systems from compromising the network if mistakenly plugged in.

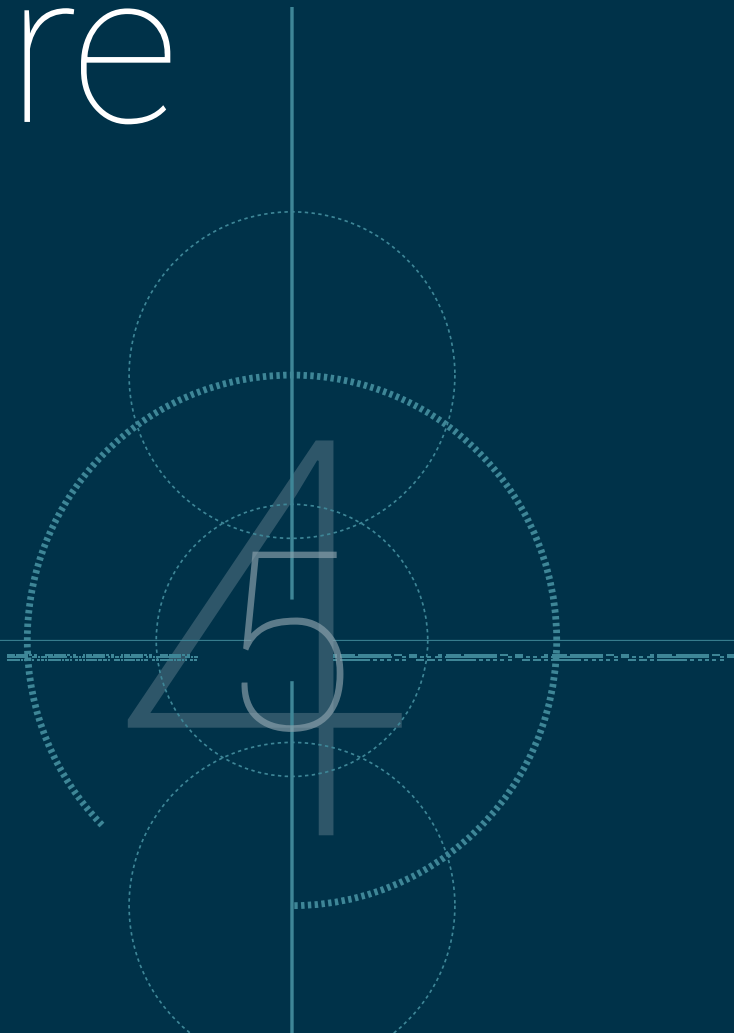
## Shared responsibility for security

While strong cyber security measures can protect the network against malign systems, an acute awareness of the supply chain will ensure they do not end up being plugged into the network at all. Organisations' procurement and security teams must develop strong overarching policies in collaboration with those of all industry partners.

Some of these policies will flow down from governmental regulations or guidelines, such as the U.S. Department of Homeland Security's advice that commercial off-the-shelf drones manufactured in China should not be flown over secure domestic sites.

# The steps to deploying Prototype Warfare

We have identified five principles and four recommendations that should be part of any plan to deploy prototypes in live environments.



1

## Embrace horizon-scanning

Always be alert to emerging technologies and capabilities – take advantage of new opportunities and protect against emerging threats.

2

## Encourage an experimental user mindset

Recognise that users who are keen to experiment with new concepts and ideas will achieve the greatest benefit from prototype technology.

3

## Assure safety early

Identify safety challenges early to allow issues to be mitigated ahead of prototype deployment.

4

## Maintain security awareness

Avoid the rapid acceleration of capability lulling users into a false sense of security. Assess security issues as a priority.

5

## Harness collaboration

Approach Prototype Warfare as a sector-wide opportunity, reliant on combining the strengths of multiple organisations to realise its potential.

# Recommendations

The factors preventing UK defence from applying the principles can be distilled into four categories: public money; bureaucracy; risk to life; and culture. In closing, we recommend the following actions to address these factors and deliver the biggest impact in the shortest time.

### 1. A fear of failing with public money

**Challenge:** Public money must always be used wisely. Defence already funds innovation but these budgets rarely stretch deeper into experimentation, where prototyping sits.

**Recommendation:** In relevant programmes funded within the command equipment plan, a small percentage of the upfront spend should be allocated to prototype technology. This adjustment will require a change in the way business cases are developed, identifying upfront the risk incurred when procuring early-stage technology that may not perform as planned when fielded. This will mitigate the risk to public money and reduce the number of instances in which exceptional ideas are denied the opportunity to prove themselves in theatre.

### 2. Bureaucracy

**Challenge:** Overcoming bureaucracy is a challenge for most organisations of significant scale. It is an acute problem in the public sector, and in defence in particular.

**Recommendation:** Integrated teams that bring together operators, regulators, buyers and users into a single unit will bridge gaps between functions, easing the flow of ideas into practical solutions. The spread of expertise across multiple stakeholders will be the key to success. Without excellent people, the chances of moving beyond rapid acquisition and into accelerated deployment will be reduced. Technical members need to have deep technology expertise; users need a desire to innovate; and operational participants need to be incredibly proficient. Defence should not limit itself to teams built on forces personnel alone.

### 3. Risk to life

**Challenge:** The safety of a prototype is paramount, but is dependent on risk being identified at an early stage, and on the user having a clear understanding of the technology's limitations.

**Recommendation:** Safety will be achieved through effective training and rehearsal. Allowing industry to work with users to experiment with equipment will improve safety by enabling the operators to understand how it will perform and how it can be improved. Defence must engage regulators early in the prototyping process and include them in the integrated project teams outlined above. This offers the ability to discount aspects of a capability before it heads too far into development, promoting early identification of critical safety issues rather than waiting until the technology is close to deployment. Involving regulators throughout the process will also ensure legal compliance and help safety policy to evolve.

### 4. Culture

**Challenge:** At present, UK defence culture risks denying our forces technology that would very likely save lives – but which has not yet been developed, experimented with, or fielded.

**Recommendation:** Defence can benefit from drawing on elements of culture that make successful small companies agile. It must identify determined, entrepreneurial people and empower them through a shift in reporting structures, so that innovation boards and teams within front-line commands report directly into the Chief or the Deputy. Sponsors should be people of significant rank who own the responsibility for instilling a bottom-up approach to innovation from the grassroots. Lots of entrepreneurial thinking already takes place within UK defence, but it will only be fully exploited if talented people are given the freedom to combine their experience, perspective, and knowledge.

---

# Conclusion

In developing this report we have identified areas for change that relate to technology, process, and culture. But overwhelmingly the critical factor influencing a successful move towards Prototype Warfare is people – and in particular, the combination of people involved. Defence usually plans and delivers progression through the actions of its own community but, in this instance, it may just be impossible for those closest to some of the subjects involved to provide an objective view. If we look at historic successes for Prototype Warfare, such as the introduction of Chain Home Radar during the Second World War, and the development of the 'bouncing bomb' that was used in Operation Chastise, progress has been driven not by established defence personnel alone, but by collaborations of industry, defence, finance, and academia. Concluding this report, we would suggest that the implementation of Prototype Warfare relies on forming alternative groups to achieve the desired outcomes – and by rethinking both tactics and the defence mindset.

**The UK has been at the forefront of previous technology epochs, developing systems and standards that are both responsible and fit for purpose.**

**We believe that, through the deployment of Prototype Warfare, it could again be at the vanguard.**

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

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

QINETIQ

QINETIQ/19/00558