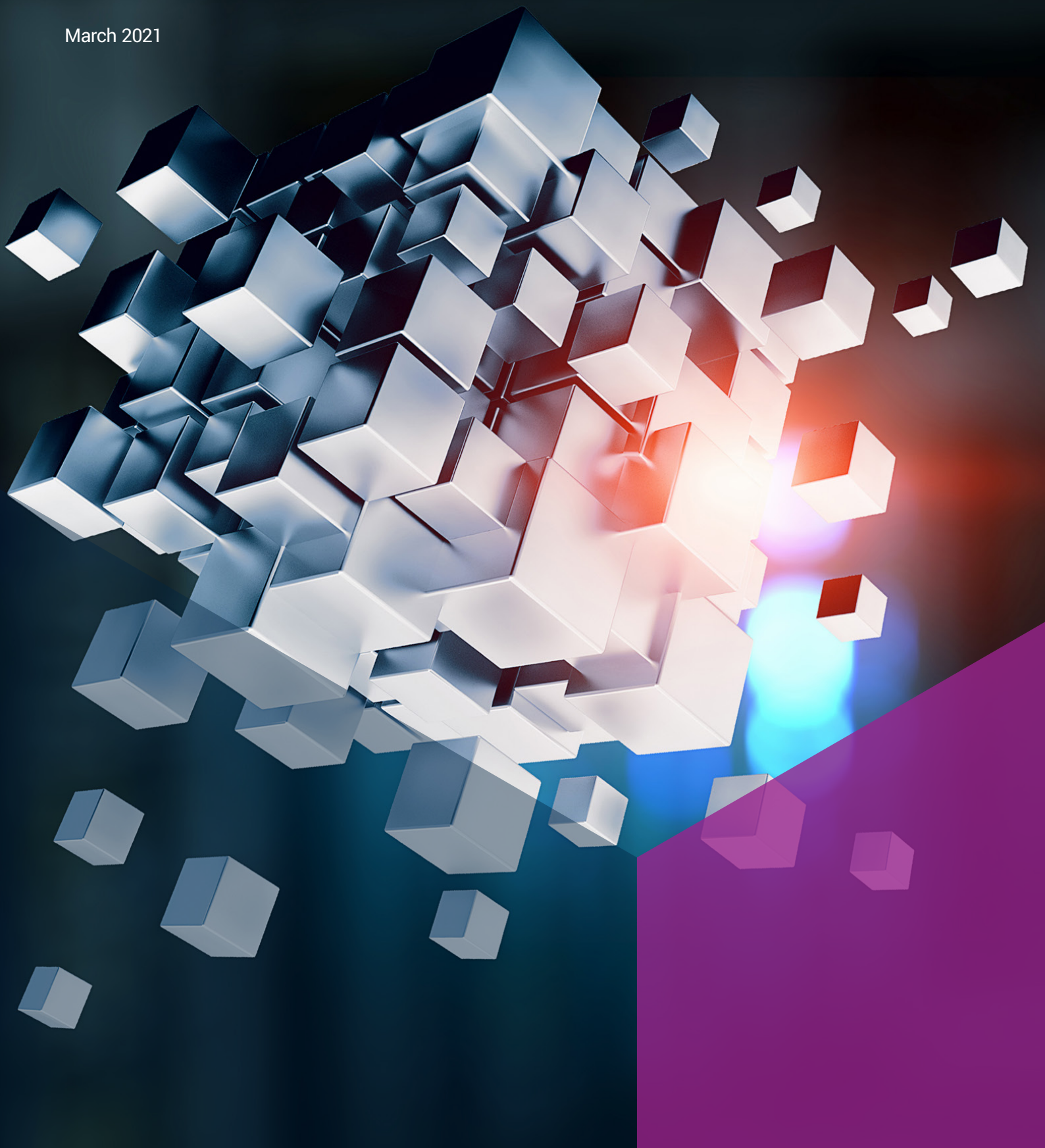
QINETIQ

White Paper

Enabling Integration

March 2021



QINETIQ

Enabling Integration

The case for integration

In its September 2020 document, The Integrated Operating Concept 2025, the UK Ministry of Defence (MOD) explicitly outlines its intent to integrate a wider range of capabilities – nationally, internationally, and across the five domains – to meet modern defence and security challenges. The reasoning is clear: having studied the Western way of war, adversaries understand the risks they face in tackling Western allies head on in military conflict. Their solution? Change the game. Instead of competing against the West's strengths, adversaries are identifying and exploiting its weaknesses. While conflict between militaries remains a risk, hostilities are increasingly directed at non-military targets, such as public institutions, populations, economies and critical infrastructure. The effect of this 'grey zone' strategy is to weaken nations' resilience and global influence without ever engaging in the type of warfare that would favour the West. There is no proportionate armed response to tactics like aggressive economic action or disinformation campaigns. Since these threats are not well suited to being countered with military force, a more integrated approach to national security is required which binds together defence and civil security forces and agencies with a wider range of institutions and organisations. The pursuit of this sort of national security requires these organisations and institutions to be able to communicate and operate together effectively.

Forming this holistic national security capability is a daunting task. In publishing its Integrated Review, the UK Government has taken a crucial first step – but significant challenges lie ahead. In this report, we examine those challenges and offer some thoughts on implementing the UK's ambitions for integration securely, expeditiously and with maximum effect.

Challenge one: defining 'integrated'

The use of the term 'integration' in policymaking poses a challenge in itself. It is literally defined as: "the act or process of combining two or more things so that they work together" – but that leaves a great deal of ambiguity about what 'working together' entails, and the criteria that must be met to achieve it. The very first step in any integration programme is therefore to determine what 'integrated' looks like. Only by having a clear vision of the end state can the process of integration be conducted meaningfully and with purpose.

Unfortunately, when it comes to defence and security, there is no single version of integration that applies to all of the elements being integrated with each other. Not everything requires the closest of all possible relationships, so there is a need to be selective about what to integrate, and with whom to integrate; for example, nations must strike a balance between sovereign and shared capability. A common feature of international grey zone competition is the creation of dependencies that can be leveraged to gain advantage, such as ownership of critical infrastructure. The supply of natural gas from Russia to Western Europe and the prevalence of Chinese technology in US telecoms have both been sources of considerable controversy in recent years. Integration must enhance national security by generating defence capability greater than the sum of its parts; not undermine it by creating unwelcome dependencies.

On a domestic level, integration will necessitate open communication and greater sharing of data between government departments, and even between the public and private sectors. But again, appropriate limits must be set on the movement of data, so as not to breach privacy laws or endanger national security. Consequently, integration is not the act of bringing organisations and institutions as close together as possible, but of optimising the balance between commonality and independence to achieve the desired effect.

Rather than seeking a one-size-fits-all solution, management of this integration spectrum is easier if broken down into distinct arenas, which allows for bespoke integration strategies designed around the specific requirements of different combinations of parties involved. For the purposes of this report, we will focus on what integration means within four arenas: the five defence domains; domestic government departments; the public and private sectors; and allied nations. We make these distinctions purely for ease of understanding – they should not be treated as separate silos, as to do so would undermine the integration intent. All of them should be considered constituent elements of the holistic defence and security suite.

In the following sections we briefly outline the potential benefits of closer working within each of the arenas, before examining which elements must be integrated and how these goals can be achieved.

Four areas for integration

The defence domains

Modern conflict is not limited to physical battles in the environments of land, sea, and air – it is a state of constant competition, happening on all fronts at all times, against state and non-state rivals. A multifaceted threat demands a multifaceted defence. The UK MOD clearly recognises this need, and has advanced its integration ideas both in *The Integrated Operating Concept 2025*, and its November *2020 Joint Concept Note 1/20: Multi-Domain Integration*. These documents call for close integration between the five defence domains: land, air, maritime, space, and cyber.

The literature cites a number of examples in which significant crossover already exists between the domains:

"…army attack helicopters in the littoral operate in the maritime, land and air domains simultaneously; in the space domain, a ground station connects with satellites via the medium of the electromagnetic spectrum while rockets ascend through the air, but all are part of the space domain. Most of the domains interplay in the majority of real-world situations."

Joint Concept Note 1/20: Multi-Domain Integration

However, the specified aim is not to use as many of the domains as possible in defending against a threat, but to create myriad potential combinations of cross-domain capabilities that can be brought to bear as part of a response. The effect of this close integration cannot be reproduced by totalitarian and non-democratic regimes, resulting in an enduring competitive advantage.

Government departments

The multifaceted nature of the modern threat means there is a need to introduce capabilities into the defence and security picture that were not previously considered part of the arsenal. Rather than fighting uncertain and expensive wars against the West's superior military forces, adversaries are turning to less overt tactics designed to destabilise Western democracies, weaken our institutions, and reduce our influence on the world stage.

China's coercive commercial diplomacy is an example of exerting global influence through non-military aggression. 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. The lesson here is that trade policy, industrial policy and security policy are inseparable, and must be integrated into a singular foreign policy to avoid dependencies that will create vulnerability to political coercion.

Trade is not the only government department that must work more closely with security organisations to ensure a secure future. Environmental policy will play a significant role in future security, as the effects of climate change and food poverty destabilise regions and displace large populations, creating new refugee crises. The environmental policies of today will dictate the security and defence policies of tomorrow. Climate monitoring and forecasting will inform future military resource allocation, whether managing conflicts or providing humanitarian aid.

Cross-departmental integration may require disruptive change in the way budgets are allocated and planning is undertaken. In the current silo mentality, a budget is allocated to each department, which then uses the money in pursuit of its own goals. For instance, tanks and warships procured by the defence department are of no use to the health or education departments. In an integrated environment, budgets will not just need to be allocated to departments, but to capabilities. Budgets given to the development of big data, artificial intelligence, or cyber security can serve multiple departments, whether protecting the nation against threats, improving the health of its citizens, or educating its young.

The public and private sectors

Closer alignment between trade, industrial and defence policies will require consultation with businesses. Speaking to the Financial Times in December 2020, Anna Stellinger, director of international and EU affairs at the Confederation of Swedish Enterprise, argued:

"Trade is, unfortunately, not just about trade any more: it's security, geopolitics, it's linked to integrity and level playing fields. There have been calls for reshoring, bringing home production and even deglobalisation during Covid. What is worrying, though, is that it generally seems to be mostly a political or ideological debate, with a lot of discussions and opinions about companies' value chains but less discussion with companies."

Reducing trade dependency on China will have huge economic knock-on effects for every UK business that relies on Chinese goods or services for its supply chain. This highlights the urgent need for integration between private and public sectors in striking the balance between open trade and national security.

An advantage of closer integration between the public and private sectors is the opportunity to combine skills to counter modern threats. For example, effective data exploitation is fast becoming a decisive weapon in defence and security, but it is not a skill traditionally abundant in the public sector. The private sector is the breeding ground for talent in data science and related skills, but many businesses lack the expertise and confidence to take on the daunting regulatory challenges associated with data collection and exploitation. The public sector cannot compete with the private sector for technical skills, but does wield the legislative weight to negotiate legal pitfalls. It also possesses an understanding of the public it serves and the 'big picture' when it comes to political and socioeconomic issues. Integrated, these strengths could be a formidable force.

Allied nations

Countries already integrate and partner on conventional warfighting capabilities, with some contributing ground-based air defences; others, a nuclear deterrent; and others, aircraft carriers – all of which can contribute to deterring (and fighting) a common enemy. The Five-Eyes partnership also enables sharing of intelligence in a more integrated way. However, the aim is to move beyond simply sharing assets to working multinationally in a far more integrated way across all domains. Military strategists refer to interoperability – the extent to which different platforms, people and systems are able to work together to fulfil a common mission. There are three levels: deconflicted; compatible; and integrated. The UK MOD defines these terms in a 2017 Joint Doctrine publication, in descending order of interoperability:

"Integrated means that forces are able to merge seamlessly and are interchangeable. Compatible means that forces can interact with each other in the same geographical battlespace in pursuit of a common goal. Deconflicted means that forces can co-exist but not interact with each other."

Joint Doctrine Publication 0-20, UK Land Power (UK Ministry of Defence, June 2017)

At the Atlantic Future Forum (AFF) in October 2020, First Sea Lord Admiral Radakin spoke of 'interchangeability' as a level of even closer integration, beyond the three currently recognised. He defined it as the ability to scale and transform based on key national relationships, going beyond simple agreements at a government-to-government level, to interchangeability of ecosystems and ideas at all levels, enabled by a shared vision. As a sign of progress toward this goal, the world's first international 'tech bridge' joining the US and UK was announced at the AFF. The tech bridge is a US-led initiative designed to promote the overseas interchange of ideas between governments, industry, academia and citizens.

Closer integration between nations' militaries creates a big opportunity: multiple forces using multiple assets working as one cohesive unit, leading to a dominant strategic posture that cannot be matched by lone states or non-state groups. This applies equally outside the traditional defence sphere. As enemies seek out a broader range of softer targets, a water treatment plant or power station may be as much at risk as a military base. Accordingly, domestic capabilities must first be integrated across defence and civil security, then that whole capability integrated with those of other nations. Allied countries that demonstrate a coherent, aligned and organised counter-threat position across their defence and security sectors will pose a greater deterrent to adversaries than fragmented, isolated states.

QINETIQ

The four key targets for integration

We have discussed which areas need to become more integrated: defence domains; government departments, the private and public sectors; and allied nations. These areas must also integrate with each other. Having looked at the 'who' of integration, we must now turn to the 'what'. Which specific capabilities, functions and practices must be brought closer together to achieve the desired outcomes? We have identified four aspects common to all four of the above arenas: information; technology; culture and values; and people and skills.

Information

The importance of 'information advantage' is widely acknowledged and defence and security communities have undergone a shift in mind-set in recent years. Where data and intelligence were once seen as supplementary to platforms and equipment, they are now placed at the very forefront of operations as effectors. The reason is simple: when faced with a complex threat, unpicking that complexity to understand the nature of the threat is fundamental to neutralising it. When an adversary is simultaneously targeting or attacking a nation's military, public institutions, infrastructure, economy and citizens in various ways ranging from physical violence to disinformation campaigns, it is incoherent to tackle these issues separately. The very objective of such covert multifaceted aggression is to overwhelm a nation's ability to protect itself by forcing it to extinguish multiple fires concurrently, then exploit the resulting chaos and confusion. The key to staying above the chaos is to respond to the threat in the strategic context – as well tackling the tactical level symptoms.

In building the 'whole-picture' view, data cannot be collected, analysed and held within silos; there cannot be separate intelligence pictures for each of the defence domains and each government department; data also needs to be shared between allied nations in a smarter way. The information must be drawn from multiple sources, combined and made available to all relevant parties. However, this creates an enormous 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. Addressing this challenge requires information integration system which combines human and artificial intelligences to ensure the most relevant and urgent data is presented to the right people 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. 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. 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.

However, there remains the challenge of data classification and categorisation. As mentioned in the introduction to this report, not all data is suitable for distribution to all parties, whether for reasons of national security, privacy, or commercial confidentiality. What is allowable for domestic government departments may not be allowable for foreign governments, or for private sector partners. In drawing up data integration protocols, security risks arising from data aggregation must also be considered. Five separate unclassified pieces of information may become classified when combined. Given this, 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.

Lastly, when it comes to data, integration should not be confused with centralisation. The structure of the data-sharing ecosystem should be federated, with relevant data delivered from the fusion engine to localised, empowered decision-makers. This approach allows the system to operate at a greatly increased tempo, without the central decision-making team acting as a bottleneck.

Technology

The integration of technologies will be a defining factor in the success or failure of tomorrow's defence and security operations. The threat changes faster than ever before, meaning countermeasures must evolve quickly and constantly to remain effective. Historically, this type of agility has not been a quality strongly associated with defence. Typically, a large expensive platform is procured over the course of a decade before beginning its 30-year service life. The asset is designed to fulfil a limited range of roles, often within a single domain. The proprietary technologies on board make adaptation expensive and time-consuming. None of this is sustainable.

The first step toward technological interoperability is enabling different platforms and assets to access a common communications, command and control architecture – a 'digital backbone' that connects all the constituent elements, allowing them to function as a cohesive unit. This is a natural progression from the integration of information; converting the digital picture into real-world effects.

The second step is ensuring different systems and subsystems work with each other, using compatible communications protocols, messaging formats, programming languages and software development standards. This opens the door to interchangeable modular capability; adaptable multi-mission platforms that allow subsystems to be introduced or swapped out as threats evolve.

The effect of this shift will be to move from having a high number of single-purpose assets, to a smaller number of highly adaptable ones that can be quickly reconfigured for multiple mission-types. It introduces the possibility of a 'sandboxing' culture, in which multi-team experimentation takes place in live exercises to develop and test new capabilities at a vastly accelerated pace. It also enables the 'Prototype Warfare' philosophy (described in previous QinetiQ reports) of devising and fielding new capabilities to adapt quickly to changing conditions and threats.

Scaled internationally with military forces, this approach could multiply combat mass many times over by allowing fighting forces of different nations to combine capabilities – although this also requires development of a shared vision, as outlined in the following section.

Culture and values

Technology is created and used by humans with belief systems, cultures, values and cognitive biases. These human characteristics are harder to change than technological ones, so technology should always be designed with humans in mind. However, there is no such thing as a 'typical' human. Two different technology creators may have radically different beliefs about the nature of a problem and the best solution to it. Two different technology users may have opposing ideas about applications of the same technology. In some cases, the greatest barriers to integration may not be the technology, but differing beliefs about its use.

Here is an illustrative, non-defence example of the challenge, taken from QinetiQ's 2020 Enacting Prototype Warfare report:

A driverless car may be forced to prioritise whose lives to preserve in the event of an unavoidable collision. Country A's culture places greater importance on youth and potential; Country B's culture values age and experience. Should the car's decision on who to save be different depending on the country it is in at the time? Or should it maintain the standard of the country in which it was manufactured, regardless of its location at the time?

The scenario may seem abstract, but the consequences of this type of disagreement between allies in battle could be catastrophic. The cultural norms of a society influence its concepts of operations. When integrating capabilities across societies and cultures, it is necessary to identify the commonalities of purpose and principle that unite the collaborators. It is also necessary to understand the differences that cannot be resolved, and build concepts of operations that can accommodate both sides. This is almost impossible to do from within the confines of one's own culture, so it is imperative that technical, doctrinal and cultural challenges are tackled collaboratively. Joint experimentation in live exercises exposes cultural barriers in a safe environment; barriers that may otherwise go unnoticed until it is too late. For this reason they warrant continued investment (and expansion).

People and skills

Assembling an integrated, multidisciplinary team to work within the modern multifaceted threat landscape will bring together people of different skills and backgrounds, many of whom would not typically interact with each other in everyday life.

The first challenge created by this combination of cultures is one of communication. Can a data scientist understand a briefing given by a military general, littered with acronyms and unfamiliar references? Equally, is the general able to understand a threat as described by a data scientist, using complex, industry-specific technical terminology? If not, critical information may be misinterpreted or overlooked, impeding response and creating vulnerability. Shared information must be presented to all parties in a common language that can be quickly understood, irrespective of the recipient's expertise or background.

The second challenge is one of trust. It is human nature for an established team to treat an outsider with a degree of scepticism, in lieu of witnessing first-hand evidence of their trustworthiness and competence. This is especially true in the armed forces, where colleagues must literally trust one another with their lives. Consequently, military training is built around building that trust and camaraderie – both of which remain absolutely vital. But how can those bonds be extended beyond the military to the civilian contributors in the new integrated defence and security force?

The solution to both of these challenges is to give all parties exposure to each other in a low-risk collaborative training environment. This may be entirely virtual, taking place across a distributed network of simulators; or take the form of a live exercise with virtual elements introduced at key points. It is a chance to test communication between teams, identifying sources of miscommunication and adapting language accordingly. Training together also grants all parties the opportunity to demonstrate their trustworthiness and competence first-hand, building that vital trust and camaraderie between teams.

QINETIQ

Some thoughts on what next….

Integration – between defence domains; government departments; the public and private sectors; and allied nations – is critical to protect against multifaceted and constantly evolving threats. However, the act of bringing together formerly disparate functions and cultures will expose new challenges that must be managed throughout the integration process.

The benefits of integration will far outweigh any downsides – but nonetheless, the impact of the downsides could still be significant. We believe the following recommendations will help mitigate potentially negative effects:

1. Information must be collected from a wide range of sources, but be shared in the most targeted and focused way possible. This will rely on a deep understanding of the relevance and classification of different data to different recipients, and a means of automating data fusion and distribution accurately and securely.

2. Trust between teams must be built through collaborative training across all levels – whether live, virtual, or a combination of both. This process must be used to generate a common information language that can be understood by all integrated parties.

3. When working across cultures, common principles and shared purpose must be established early, and tested in live exercises to expose hidden differences that may cause indecision or conflict in theatre.

4. Integration is not the closest of all possible relationships in all cases, but the optimum balance between commonality and independence. This balance will vary depending on the parties involved and the specified objectives, so must be constantly monitored and managed by a nominated overseer.

5. Interoperability must be a key design requirement of all defence technology, with multi-domain integration the operating norm. This will be facilitated by a 'digital backbone' enabling separate systems to work as one, with platforms built on modular architecture for ease of adaptation in response to evolving threats.

The overarching principle, and the thread that runs throughout all aspects of any integration programme, is the importance of understanding your risk and balancing it against the potential gains of closer integration. For instance, multiple nations using the same interoperable equipment may increase their combat mass and deliver cost savings; but could it come at the expense of assured sovereign capability, or an individual nation's ability to compete? And do we risk becoming predictable as a result of integration, by creating scenarios in which a weakness of one becomes the weakness of the whole?

Ultimately, these risks are manageable and the potential upsides are significant. But we can only reap these rewards if we are guided by a deep understanding of capabilities at our disposal, and a strategy for optimising the balance of sovereignty and interoperability at all levels.

QINETIQ

For further information please contact:

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

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