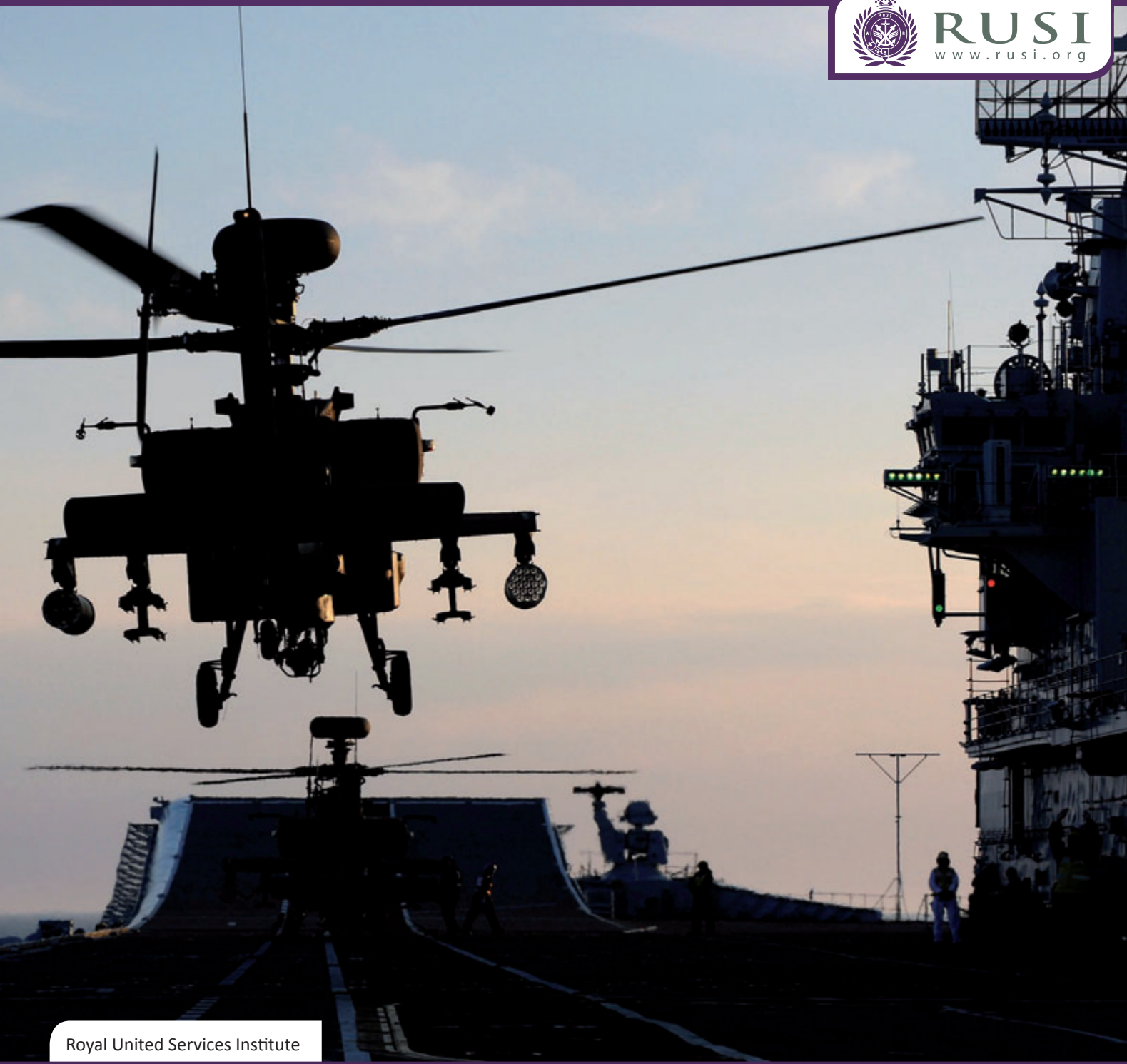
CROSS-DOMAIN OPERATIONS AND INTEROPERABILITY

Elizabeth Quintana, Joanne Mackowski and Adam Smith

RUSI
www.rusi.org



Royal United Services Institute

OCCASIONAL PAPER

About the Authors

Elizabeth Quintana is Senior Research Fellow for the Air Power and Technology programme at RUSI. Prior to joining RUSI, Elizabeth worked for two years running technical conferences for the international defence community. In 2001, she took a graduate assistant position at the University of Texas A&M where she worked for two years on a DARPA project, investigating collaborative robotics. Elizabeth holds an MEng in Automatic Control and Systems Engineering from the University of Sheffield and an MSc in Aerospace Engineering from the University of Texas A&M.

Joanne Mackowski is a Research Analyst at RUSI. Joanne formerly worked with McLaren Formula 1 before joining the Institute. She also works part-time in risk analysis, specifically on global terrorist attacks. Joanne has an MA from the School of Oriental and African Studies in International Studies and Diplomacy, and a BA from Durham University in History. Her research interests include military history and the militarisation of space.

Adam Smith is a Research Analyst at RUSI. Adam has a BSc in Physics from Loughborough University where he did an industrial placement with the Science and Technology Facilities Council. Subsequently taking a graduate position with MBDA Missile Systems, he is now on secondment in the RUSI Military Sciences department, with interests in space security and space resilience.

About the Programme

The Air Power and Technology programme looks specifically at the future of air power for the UK and for NATO at a time of increasing commitments and decreasing resources. The programme also explores the doctrinal, strategic and ethical implications of the use of air forces and emerging technologies. Current areas of research for this programme include: the future of the UK defence avionics sector; air power and influence; information superiority and cyber-security; and space services and national security.

For more information, please visit: http://www.rusi.org/research/programmes

About RUSI

The Royal United Services Institute (RUSI) is an independent think tank engaged in cutting edge defence and security research. A unique institution, founded in 1831 by the Duke of Wellington, RUSI embodies nearly two centuries of forward thinking, free discussion and careful reflection on defence and security matters.

For more information, please visit: www.rusi.org

Air Power Workshop Sponsors

BAE SYSTEMS

CASSIDIAN

GENERAL ATOMICS AERONAUTICAL

L3 communications

Occasional Paper, July 2012

Cross-Domain Operations and Interoperability

Elizabeth Quintana, Joanne Mackowski and Adam Smith

www.rusi.org

The views expressed in this paper are the authors' own, and do not necessarily reflect those of RUSI or any other institutions with which the authors are associated.

Comments pertaining to this report are invited and should be forwarded to:
Elizabeth Quintana, Senior Research Fellow, Air Power and Technology programme, Royal United Services Institute, Whitehall, London, SW1A 2ET, United Kingdom, or via email to elizabethq@rusi.org

Published in 2012 by the Royal United Services Institute for Defence and Security Studies. Reproduction without the express permission of RUSI is prohibited.

About RUSI Publications
Director of Publications: Adrian Johnson
Publications Manager: Ashlee Godwin

Paper or electronic copies of this and other reports are available by contacting publications@rusi.org.

Printed in the UK by Stephen Austin and Sons, Ltd.

Contents

We live in a world of financial uncertainty, of new and emerging threats, and increasing interdependencies. This calls for an agile posture that allows governments and, if necessary, military forces to intervene in a timely and effective manner. International collaboration will be indispensible, not only for military interventions but also to provide a means to maintain – or in some cases establish – international norms and behaviours. The US pivot towards Asia-Pacific and its approach to the Libya campaign, with US forces encouraging NATO partners to take a more prominent role, reinforces the importance of other NATO nations being willing and able to conduct operations independently both in Europe and further afield.

The US has highlighted the importance of cross-domain capabilities within its Joint Operational Access Concept (JOAC),[1] with the underpinning Air-Sea Battle and Joint Forcible Entry Operations (JFEO) concepts.[2] In essence, these concepts aim to restore contingency across the spectrum of operational intensity and operating environments after more than a decade of land-centric COIN operations, and were primarily designed to counter the anti-access and area-denial capabilities (A2/AD) proliferating around the world. Clearly, few nations aside from the US will have the ambition or resources to configure and direct their forces to address full-spectrum threats at distance from their country's borders, but the concepts still have merit for nations looking to modernise their armed forces. Many of these disruptive A2/AD capabilities have been developed as relatively low-cost solutions to counteract costly and complex US and/or NATO systems. This should cause militaries to pause and think differently about how they acquire and build new capabilities, particularly in the current age of austerity.

The domains outlined in the US concepts are air, land, maritime, cyber and space. Recognising that air capabilities already constitute an important element of maritime power doctrine, supplemental air/maritime integration has been the focus of much of the work to date; in addition, the domains of space and cyberspace will also require attention, as these global commons will be increasingly integrated into future operations. Understanding how military forces can exploit each domain without denying access to the civil community will be essential given the dependence modern society has on global trade and communications.

This paper will examine the concepts, capabilities and force structures necessary for cross-domain operations and interoperability, and how they might apply to smaller militaries. Focusing on the British experience, the paper will use lessons learned from recent operations to understand how these might be implemented. The topic was explored at a workshop held at RUSI on 25 May 2012, and the discussions there form the basis of much of the paper.

Concepts

Today, unprecedented peace and stability reigns across much of the world. The global community is highly interconnected politically, economically and culturally through the media, the Internet, trade and the proliferation of diasporas, and so there are tremendous incentives for governments not to destabilise the system through aggressive action. At the same time, there has been a spread of destructive technologies, many of which are available to terrorists and militant groups. Thus the potential for others to cause harm or constrain our freedom is growing. Armed forces (and, indeed, security forces) must therefore understand the consequences of their actions within the wider system if they are asked to intervene, and must also seek to apply a precise and appropriate level of force to bring a successful conclusion to the operation without undermining the societal structures on which we all depend. 'Complexity rather than scale will therefore define future operations and each operation must be taken on its own merit'.[3]

Western forces are losing mass as the cost of military equipment continues to rise and defence budgets are squeezed. Governments, as well as alliances, wishing to maintain interventionist policies must adopt a more strategic approach through collaboration and better co-ordinated capability planning to prevent unsustainable swings from investment to disinvestment to investment again, particularly as it is difficult to predict the skills and capabilities that any one operation will require. Consequently, there will be greater need for pan-governmental co-operation and effective international alliances focused on acquiring the necessary contingent capabilities and employing them in an agile manner in order to respond to a range of threats.

Space and cyberspace have also emerged as domains in their own right in recent years and the JOAC lists the proliferation of A2/AD capabilities in these areas, including:

- Long-range reconnaissance and surveillance systems that provide necessary precision targeting information, including satellites, aircraft, and land- and ship-based radar
- Kinetic and non-kinetic anti-satellite weapons that can disable space systems vital to force projection
- Submarine forces able to interdict friendly sea lines of communication in both sovereign and international waters between US bases and the theatre of operations
- Cyber-attack capabilities designed to disrupt command-and-control systems and critical infrastructure, both civilian and military, in the home base or in deployed locations
- Terrorists willing to attack US or partner bases and deploying forces, even at points of origin in the continental United States or other regions

- Special operations forces capable of direct action and unconventional warfare in the approaches to the operational area.[4]

All of these capabilities can be deployed singularly or in concert, so more than ever militaries need the agility of thought and adaptable force structures in order to achieve the freedom of manoeuvre and effect that their political masters require.

As discussed in the opening section, greater interoperability across domains could provide the additional agility necessary for this new environment. The US JOAC and its subcomponent concepts, Air-Sea Battle and JFEO, look to maximise resilience and achieve the necessary concentration of force through cross-domain operations. This approach suggests greater interdependence between the services, improved cross-domain C4ISTAR down to the most tactical levels, and adoption of a dual track of disruptive technologies and stealth and low-signature platforms. Disruptive technologies may well be an area that smaller nations could focus on, providing new and effective capabilities that require relatively few resources.

Emerging A2/AD capabilities will mean future theatres of operations will be contested in new ways. The JOAC recognises that air, maritime and cyber superiority may not be possible for indefinite periods of time, but that pockets or corridors of superiority should be sought when necessary to fulfil a mission or achieve a particular outcome. It also suggests operating simultaneously in multiple lines of operation and in multiple domains to confuse and overwhelm the enemy. While the latter may be possible for the US, which may be able to retain the mass necessary in all domains to achieve such an effect, smaller nations may have little option but to use multiple domains to enhance the effect of action in one domain; for instance, conducting a maritime attack (including air effects) with cyber and space in support.

This paper considers interoperation between all five domains: air, land, maritime, space and cyber. However, air/maritime operations represent an area of significant risk to NATO forces following a decade of relatively benign air and maritime environments and a necessary focus on air/land operations. It was suggested that the NATO maritime strategy of the 1980s would be worth revisiting as an appropriate starting point for future contingent air/maritime operations.[5]

In addition, the broader impact of the deterrent effect that these networked, adaptable joint forces would have needs to be considered. However, the requirements for air/maritime operations will be location-specific: militaries might need to field very different capabilities for operations at distance, for example, than if they were operating in their own neighbourhood,

particularly if there is limited access, basing and overflight in the region, or if there are environmental challenges – operations in the Arctic would prove particularly demanding, for instance.

Many nations now have global interests, diasporas and relationships with partners around the world. These bring with them responsibilities. Raw materials, for example, are in increasingly short supply and it may become necessary to protect trade routes (as demonstrated by the anti-piracy operations off the Horn of Africa). As a consequence, it will be important to understand the requirements for power projection, which may include the availability of carriers and sea-basing for logistics as well as access, basing and overflight for essential support air assets (ISTAR, transport and tankers) within these potential regions of operation. The US already recognises that access, basing and overflight is increasingly difficult and cannot be guaranteed without sustained prior engagement. Indeed, Canada is already investigating a small footprint of forward-deployed forces to Singapore as part of a wider programme of engagement with Pacific nations, and a logistics hub within Europe to support its operations in the Middle East.

Finally, it goes without saying that personnel represent the ultimate contingency for any nation as they maintain the corporate knowledge and the ability to respond to (re-)emerging threats. A strategy is therefore needed to retain (access to) and develop internally those with the skills and knowledge to provide the organisational agility necessary to respond effectively.

Capabilities

Future operations will exploit all five domains. This section examines some of the capabilities required for each of these domains in the future operating environments, and particularly those that will facilitate cross-domain operation.

C4ISTAR and cyber capabilities, or joint enablers, are key to joint warfare. In the past, these capabilities have been underfunded as governments focused on the acquisition of platforms rather than bearers, sensors and mission systems that provide a platform's capability edge. In the new environment, nations will need to continue to fund development in their networks to ensure sufficient bandwidth to meet the growing ISTAR requirements and to be able to defend against future cyber-threats.

Sovereign ISTAR will be critical for the UK in support of the nuclear deterrent, for strategic (national) intelligence, and in support of special forces contingency operations and committed forward-deployed maritime operations. Afghanistan as a land-based theatre has been well-resourced in this regard through Urgent Operational Requirements, but now these capabilities will need to be made available on a more contingent basis. Whilst unmanned

or remotely piloted air systems (UAS and RPAS, respectively) are prized for their persistence and precision-attack capabilities, the slow integration of unmanned platforms into civilian airspace (and more specifically, the requirement to provide assured resilience in the various C2 and sensor links) may mean manned surveillance assets are a more affordable solution in the near term for smaller nations. Indeed, the UK's experience with Sea King helicopters in the land, maritime and air domains, Sentinel R1 (which provides wide area surveillance) and Shadow R1 (which provides more tactical support) has proved very positive. Moving forward, NATO's solution, the Alliance Ground Surveillance (AGS) system, offers a model for smaller nations to pool their collective assets to achieve the desired operational outcomes. Such pooling can come at the price of being able to task national assets; however, the UK and France have opted to provide contributions-in-kind (national assets) to the NATO AGS system rather than provide funds for an Alliance-owned capability, which overcomes this problem.

The survivability of ISTAR platforms will require greater attention if future operations take place in an A2/AD environment, but it will be essential to balance survivability against cost in order to retain the capability, as defensive aid suites for ISTAR platforms are expensive. Furthermore, international law will likely preclude the routine overflight of nations by small (often unmanned) intelligence platforms, such as the Reaper MALE UAS, which has been used extensively in recent counter-insurgency operations. As a consequence, larger platforms will be needed to undertake stand-off surveillance and reconnaissance tasks, and militaries will need to reconsider the mix of space, air and special forces capabilities required to derive understanding of fleeting targets. Forces will also need to consider methods of countering ISTAR platforms, particularly UAS, as the capability becomes more widely adopted both by conventional military forces and by proxy forces or insurgent groups.

Allied to the growing requirement for ISTAR is the need for more efficient analysis of the intelligence it provides. Joint analysis of data is currently difficult but could be a force multiplier. Whilst a number of bespoke solutions exist, it has been suggested that using an 'app' (mobile device application), similar to the approach employed by smart phones, could help reduce the growing analysis burden. There is interest in exploiting commercially available technology (for example, iCloud) on the battlefield instead of defence technology; indeed, the US Army already has an app (which can be accessed in theatre) to train its forces.

The cyber-domain will be increasingly important, particularly in the early phases of an operation. The effects of cyber capabilities are sometimes limited by the bandwidth of communications bearers, which in turn hampers the security restrictions; but, generally speaking, the current limits are not technical but policy-related. Worryingly, cyber-defence has not had as

much attention as cyber-effects, although it is likely that space and cyber capabilities will be more rapidly eroded than others by A2/AD capabilities. Maritime forces, intelligence services and unmanned vehicles, which all rely heavily on reachback, will need to operate in an information-denial environment and mission command will become a more fundamental basis for operations.

More personnel with the necessary skills are needed across the cyber sector – in the military, the security services and the supporting industrial sector. Currently, the commercial sector pays much better than government agencies, which means that some of the best operators are being lost to the private sector. As a consequence, there has been some debate whether cyber experts and cyber-warfare specialists need to be uniformed personnel; however, many consider that an in-depth military understanding of the use of cyberspace remains necessary and that there are a number of legal and sovereignty issues with 'outsourcing' cyber.

Space is also highlighted by the JOAC as a domain that will become increasingly important and contested. It is a global common; there are over sixty nations with assets in space, and societies are increasingly reliant on access to such assets. Many of the services used, even by militaries, are provided by the commercial sector and therefore represent a potential vulnerability. A number of nations are developing anti-satellite technologies and there are also natural threats to space platforms through space weather and debris. For those countries without significant holdings of national space assets, it will therefore be important to understand the risks and to build in the necessary resilience, should space services become unavailable.

Air operations will be essential for any intervention operation, providing rapid access to the theatre of operations and enabling superiority in the land and maritime domains. Operation *Ellamy*, the UK's military action in Libya in 2011, identified a number of capability gaps for NATO's European forces: support capabilities such as C2, ISTAR and air-to-air refuelling had to be provided by the US in the main. These capabilities should not be neglected. Combat air will always remain a requirement, and fifth-generation aircraft with enhanced stealth and greater range will become increasingly relevant against A2/AD threats. Indeed, for nations with smaller combat air fleets, fourth- and fifth-generation aircraft will need to be successfully integrated and supported by a robust information network in order to maximise the combat-air affect. Cost remains a major factor when developing air capabilities, and it may become necessary for smaller nations to opt for regional air forces rather than national services in order to retain the necessary mass and expertise. Such an approach has been suggested for Eastern Europe in a paper by the NATO Joint Air Power Competence Centre.[6]

Security in the maritime environment has always been vital and despite an exponential rise in air traffic, over 90 per cent of all freight is still shipped by sea.[7] Piracy in the Horn of Africa and in the Straits of Malacca is a reminder that military forces may be increasingly required to secure trade routes in the future. In addition, with around 80 per cent of the world's population living within 100 miles of the sea, it is reasonable to assume that the land-locked theatres of the past ten years will be an exception rather than the rule. Maritime security will require a range of capabilities, both air and maritime, in order to understand the exact nature of potential threats and deliver both surface and sub-surface effects. Again, ISTAR is an important capability. For the UK, the lack of persistent, wide-area maritime surveillance is troubling, particularly with regards to identifying underwater, surface and air (including unmanned) threats to capital ships and task groups. Maritime platforms, like air platforms, are also resource-hungry, so maritime operations often require a multinational approach. In 2005, the US Navy developed the '1,000 Ship Navy' concept (which became the 'Global Maritime Partnership' concept), prompting larger navies and regional players to co-operate to ensure regional security. The Combined Joined International Task force (CJIAT) counter-narcotics operation in the Caribbean, operations under the auspices of ReCAAP (the Regional Co-operation Agreement on Combating Piracy and Armed Robbery against Ships in Asia) in the Malacca Straits, and coalition counter-piracy operations off the east coast of Africa are all good examples of this concept in action.[8]

As combat operations in Afghanistan wind down, it is hard to foresee another long-term, land-centric operation, yet history teaches us that the next intervention will usually be the one we least expect. In the meantime, there are a number of areas in which the British Army can improve its contingent capabilities through extreme environment training and joint exercises with allies and partner nations. Armies can also provide a range of options to their governments by helping to strengthen the indigenous capabilities of security forces in failing states through training programmes, which could inculcate cross-domain thinking from the outset. Special forces also continue to provide a range of means of responding to developing crises.

Optimised logistics are fundamental to effective joint warfare and, as NATO Operation *Unified Protector* in Libya reinforced, support assets are as important as war-fighting capabilities to retain the necessary tempo of operations. Due to the logistically intensive nature of force projection, effective sustainment will be critical to future joint force success – and will therefore be a likely target for enemy attack. The JOAC recommends:

- Decreasing the logistical appetite of joint forces in all classes of supply, but especially in fossil fuels
- Improving supply chain management by increasing visibility of both

expenditure rates and available inventory levels
- Improving the capabilities and capacities of military airlift and sealift. Airlift provides the means to respond rapidly but in low volume, whereas sealift provides the means to respond in volume but at a slower pace
- The use of sea basing, which reduces the requirement for forward bases. The inherent mobility of sea bases can complicate the enemy's defensive preparations by making the true objective ambiguous while holding a large coastal area at risk.

The JOAC also proposed new concepts for forward basing, including developing the ability to operate out of austere bases with rapidly deployable infrastructure and C2 nodes to reduce the forward footprint. Rapid ramp-up and shut-down of austere bases would allow a certain agility of operations and retain the element of surprise, particularly useful for special forces operations. However, austere bases would not be able to provide the same range of activities and functions as more established bases.

Force Structures

Pan-Governmental Efforts
First, in order to be able to predict and respond to developing crises, it will be essential to have a global engagement and intelligence-gathering strategy. The intelligence communities do not have a natural tendency to share information (even across government) and yet good intelligence is key for governments to be able to respond in a timely manner. Whether they generate the intelligence themselves or receive it from other government departments, ministries of defence will need to have access to an effective international horizon-scanning capability. This should include broad situational awareness that takes into account the effects of crises on neighbouring countries, the geopolitical effects of events in one country, papers on geopolitical problems and expertise on culture and tribal structures, and so forth. Defence intelligence services often focus on the equipment and the technical capability of foreign armed forces rather than the actual military capability (including training, the proficiency of forces operating their equipment, logistics and so on). In fact, a proper order-of-battle (ORBAT) assessment is required. This will help to elucidate the types of strategies that will work and the measures that need to be taken to avoid unfortunate ripple-effects.[9]

Alongside this, the MoD engages in upstream activities such as capacity-building overseas and routine maritime deployments to areas of strategic interest, which is also an effective way of contributing to regional security and stability at much lower costs than full-scale operations. Furthermore, integrating defence exports, particularly as part of a wider engagement

strategy, would provide a more comprehensive approach. Operations in Iraq, Afghanistan and Libya also integrated international development projects, providing humanitarian aid and additional activities to stimulate the economy and generate goodwill amongst the local population.

International C2 Structures

It was suggested that for international operations, the current NATO C2 model was an appropriate template. The EU's Operation *Atalanta*, countering piracy off the Horn of Africa, uses NATO doctrine and technical standards to allow all nationalities to interoperate, and not just communicate, with each other. Operation *Unified Protector* also proved the dual importance of national componency and NATO interoperability to bringing non-NATO partners on board. If NATO is to be the model of the future, member states must continue to invest in the Alliance, particularly those who wish to be framework nations. This will require an investment in the necessary networks and technical standards that underpin Alliance interoperability, and personnel in the relevant NATO posts to influence the evolving doctrine and tactics, techniques and procedures (TTPs).

More specifically, the JOAC 'envisions that future joint forces will organise tactically into tailored joint formations able to deploy, operate, and survive autonomously. While manoeuvring independently, they will maintain the ability to concentrate smoothly into larger formations as necessary'. In response to the Strategic Defence and Security Review (SDSR) in 2010, the Royal Navy introduced just such a concept, and Operation *Cougar 11*, which took place in early 2011 off the coast of Cyprus, proved the Response Force Task Group (RFTG) to be a valid vehicle for achieving very-high-readiness contingency across the three services, and with allies and partners. Elements of the RFTG were already deployed in various locations and were very quickly able to assemble for Operation *Unified Protector*, integrating further units as the operation developed. Thus, even in its infancy, the task group was able to have an effect off the coast of Libya and throughout the Mediterranean, Red Sea, Gulf of Aden and Arabian Gulf, providing reassurance during a period of instability that had the potential to escalate, and concurrently delivering military effect in support of UNSCR 1973 and Operation *Unified Protector*. It is expected that this concept will be extended to a joint UK-French task force to be proven later this year as part of a Combined Joint Expeditionary Force (CJEF). It could easily be extended to joint operations.

National C2 Structures

National C2 structures may need to be optimised for cross-domain operations. The UK is setting up a Joint Forces Command (JFC) with a remit to better establish jointery across defence and remove unnecessary redundancies. Lessons from the highly effective Joint Air Land Organisation (JALO) and Joint Helicopter Command suggest that maintaining a tight focus on efforts, a fully

joint governance structure and a rotational command chain could ensure that the JFC operates at maximum effectiveness. Despite the great gains that have been made on air/land integration in recent years, it seems that the lessons have not been fully institutionalised, and instead have to be actively maintained by JALO. There is concern within the MoD that after 2015 the experiences of the last ten years may be lost or watered down as the focus in both the army and Royal Air Force switches to regenerating contingent capabilities. On a more positive note, the JALO will eventually be integrated into the JFC and should be expanded to cover joint air/land and air/maritime effects in the round, which would provide a one-stop shop for cross-domain capabilities and interoperability, if equitably resourced.

Lessons from Operation *Unified Protector* regarding the operation of Apache helicopters onboard HMS *Ocean* also highlighted the importance of training forces from each of the services to be familiar with each other's C2 structures and environments. There were some challenges as the Apache, an army asset (which was more used to operating in Afghanistan under an army headquarters), was deployed onboard HMS *Ocean* – a naval asset – and was subsequently tasked through the NATO CAOC (Combined Air Operations Centre) at Poggio Renatico. Ironically, the Apache was always supposed to operate within a wider COMAO (Combined Air Operations) package but training opportunities had been lost with the focus on Afghanistan. It is thought that with the adoption of networked synthetic trainers, such cross-domain expertise might be more easily retained.

Special forces are due to grow and future operations will look more like small-scale interventions with special forces fully integrated, rather than small-scale conventional operations supplemented by them. However, for small nations, a separate special forces budget is not practicable and the three services may have to be prepared to adapt their platforms either permanently or temporarily to support special forces operations; furthermore, some special forces capabilities will become core capabilities, which will also require additional training for both special and conventional forces.

Training

The JOAC emphasises the importance of multinational training and exercises to build relationships in potential areas of operation. It was pointed out that NATO is very good at joint, multifaceted training and could also help to smooth out the C2 and intelligence problems that arise when operating in a coalition.

Secondly, the US routinely runs its war games against real-world scenarios, making them more effective, enabling a level of detail that would not otherwise be possible, and allowing US forces to properly test their force structures.

Finally, training and development in synthetic or constructive environments (that is, a combination of live and synthetic exercises) will naturally form part of the future training requirement and may make it cheaper to run joint and combined exercises on a more regular basis. Synthetic environments are particularly useful for developing and testing C2 structures, which will be useful if forces do migrate towards cross-domain operations. The UK has already used synthetic training to improve C2 and air/land integration, as part of pre-deployment training for Afghanistan, to great effect. Owing to bandwidth and connectivity issues at sea, fully synthetic training is not so achievable in the maritime environment at present, but it must continue to be developed in parallel on land. Given the widespread availability of space surveillance capabilities and the orbiting patterns of low-earth-orbit satellites, synthetic trainers offer the additional benefits of allowing military training to take place in secret. However, networked synthetic environments have high bandwidth requirements and, if adopted extensively, might also become the target of a cyber-attack.

Summary and Conclusions

The world is evolving and the range of threats is widening during a time of relative peace and stability. Given the interconnected nature of our global society, militaries may be required to undertake expeditionary operations to protect trade routes, support allies and partners, or for national reasons – for example, conducting non-combatant evacuation operations even where there is no direct threat to national security.

This means that despite shrinking defence budgets, armed forces will need to retain the ability to meet the demands of the new environment. Recent US concepts present one way to tackle the A2/AD problem, but smaller nations may struggle to keep up with such an ambitious programme. As such, nations may wish to use existing alliances and partnerships to better spread the risk and ensure the necessary depth of capabilities and expertise to meet a variety of threats, without having to respond in contact and pay a premium for capabilities.

Militaries will need to consider the political, economic and social impacts of their operations – and not just within the bounds of their theatre. This requires a broad and robust intelligence capability and effective pan-governmental co-ordination of efforts. Space and cyber capabilities will be increasingly employed prior to kinetic operations and both forces and their command chains will need to be prepared for information-denied environments. In many nations, space and cyber capabilities are not exclusively owned by the armed forces and so will also require pan-government efforts and close co-operation with industry.

Cross-domain operations will require greater interdependence between the services, improved and robust cross-domain networks providing information down to the most tactical levels, and the adoption of a dual-track approach of disruptive and stealth technologies. ISTAR and counter-ISTAR capabilities will be especially important in the future. A variety of basing options will also be necessary in order to retain the flexibility to respond to events.

Effective sustainment of forces will be important in the new environment and this includes a reduced logistical footprint, improved air- and sealift capabilities, and, again, sustaining a variety of basing options.

Training will also be an essential component to ensure cross-domain operations run smoothly, and it may be necessary to focus on specific cross-domain capabilities in the short term in order to maximise their effectiveness. Synthetic and constructive training will provide the opportunity to undertake cross-domain training and exercises more frequently and in a more cost-effective manner. The UK's experience shows that joint organisations and units will require fully joint C2 structures and command chains for them to truly fulfil their remit. The NATO C2 model is seen to be an effective template for international military operations, both doctrinally and from a C2 perspective.

In summary, the JOAC espouses the concepts of network-centric warfare, with smaller units being able to deploy, operate and survive autonomously while maintaining the ability to mass into larger formations if required; however, it expands on this idea, also pushing the importance of cross-domain units to create effect. Nonetheless, one of the risks highlighted by the JOAC was that integrating cross-domain capabilities, particularly across multiple lines of operation, might become too complicated to be practicable or too inefficient. This was the US Army's view of Effects-Based Operations in Iraq. It will be important, therefore, to ensure that C2 structures adapt alongside the integration of fourth-, fifth- or even sixth-generation capabilities – but this is not trivial.

The UK will likely adopt many of the concepts laid out in the JOAC, if only to ensure that it can continue to operate with its closest ally. However, as this paper has explored, there are both risks and benefits to smaller nations adopting such an approach. For the UK, there is the risk of overstretch if it aims to do too much with its limited resources, particularly as the MoD seeks to reconstitute contingent capabilities across all three services. However, this also presents an opportunity to generate innovation through cross-domain operations and closer integration with its NATO partners.

Notes and References

1. Department of Defense, 'Joint Operational Access Concept (JOAC), version 1.0', 17 January 2012.

2. With regards to the Air-Sea Battle concept, see Norton A Schwartz and Jonathan W Greenert, 'Air-Sea Battle: Promoting Stability in an Era of Uncertainty', *American Interest*, 20 February 2012; in relation to Joint Forcible Entry Operations, see Department of Defense, 'Joint Forcible Entry Operations', JP 3-18, 16 June 2008.

3. Air Commodore Ian Teakle, Director of the Air and Space Operations, Development Concepts Doctrine Centre, speaking at the Cross-Domain Capabilities and Interoperability workshop, 25 May 2012.

4. Department of Defense, 'Joint Operational Access Concept', p. 10.

5. NATO, 'Tactical Air Support for Maritime Operations', ATP 34 (B), which has since been superseded by NATO, 'Air-Maritime Co-ordination', AJP 3.3.3, 2005.

6. Joint Air Power Competence Centre (JAPCC), 'Regional Fighter Partnership: Options for Cooperation and Cost Sharing', March 2012.

7. Schwartz and Greenert, 'Air-Sea Battle'.

8. Counter-piracy operations off the east coast of Africa combine EUNAVFOR Operation *Atalanta*, NATO Operation *Ocean Shield* and the US-led Combined Maritime Force.

9. Department of Defense, 'Joint Forcible Entry Operations'.