Royal United Services Institute
for Defence and Security Studies

Conference Report

Strategic Command Conference 2021

Paul O'Neill

Strategic Command Conference 2021

Paul O'Neill

RUSI Conference Report, July 2021

Royal United Services Institute
for Defence and Security Studies

190 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 190 years.

Published in 2021 by the Royal United Services Institute for Defence and Security Studies.

RUSI Conference Report, July 2021. ISSN 2397-0286 (Online).

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

Strategic Command Conference 2021

RUSI'S STRATEGIC COMMAND Conference took place on 26 May 2021 at the IET, London. It followed publication of the Ministry of Defence's (MoD) Integrated Operating Concept (IOpC)[1] and Defence Command Paper,[2] and the UK government's Integrated Review.[3] Participants highlighted integration as an important organising principle for the UK's armed forces and Strategic Command's central role in its delivery. The conference examined three dimensions of 'integration': multi-domain integration within the military instrument; integration across government; and integration with allies and partners. Integration with industry was addressed in a separate industry day.

Integration

Integration is a response to an increasingly 'sneaky' era where warfare has moved from Clausewitzian force-on-force encounters to Sun Tzu's more indirect approach. Adversaries are integrating and manoeuvring in conceptual, geographical and organisational boundaries to sow confusion and exploit uncertainty. Alliances represent the West's greatest strength, but adversaries are targeting alliance cohesion and decision-making. NATO seeks to restrict adversaries' ability to deny it manoeuvre space by focusing on strengthening its political unity and societal resilience.[4]

Russia and China increasingly act in ways antithetical to Western interests. Some conference participants viewed this as a failure of deterrence, while others saw adversaries' attempts to exploit the seams and remain hidden as demonstrating the success of deterrence. They noted this highlighted a need for new approaches that might reset the bar and deter the current forms of unacceptable behaviour. The armed forces remain important tools of deterrence, and they will be used routinely in engagement and shaping activities (what the MoD calls 'operate') – no longer just as an insurance policy against warfighting – alongside other levers of government. Traditional capabilities and mass still matter, with a premium placed on intelligence and the ability to attribute actions to actors and respond quickly in line with long-term strategies and aims.

Integration must serve a grand strategy that aligns the instruments of national power in overt and potentially covert shaping of the environment. The strategy provides the means for democracies to drive the international agenda and cohere action nationally and with allies

1. Ministry of Defence (MoD), 'Introducing the Integrated Operating Concept', September 2020.
2. MoD, *Defence in a Competitive Age*, CP 411 (London: The Stationery Office, 2021).
3. HM Government, *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*, CP 403 (London: The Stationery Office, 2021).
4. NATO, 'NATO 2030: United for a New Era', November 2020.

over when to respond and what action, if any, to take in response to provocation. The need for a modern equivalent of George Kennan's Long Telegram was emphasised, with participants suggesting that the Integrated Review was too broad to allow effective prioritisation of national activity. Subsequent publications must fill the gap.

Three priorities for delivering integration emerged: dependence on partners; pace; and the importance of people.

Partners

Integration is relational, and depends on effective relationships with partners based on bringing value to all parties; a joint venture rather than a takeover. The IOpC envisages the UK armed forces integrating across the five operational domains[5] at the tactical, operational and strategic levels. This multi-domain integration is more profound than a mere coordination of inputs. The armed forces must also work seamlessly across government and enhance interoperability with international allies and partners.

Military capabilities will be persistently engaged around the world, coming together when needed (reminiscent of Corbett's 'Fleet in Being'[6]). Multi-domain integration goes beyond coordinating activity across stovepipes, and requires the development of integrated outcomes developed from the start of the planning process, with Strategic Command at its heart. This goes beyond Jointery, where coordination is too often an afterthought. It requires trust created through positive experiences of working together, the right concepts and doctrine, and appropriate processes and reward mechanisms.

Four areas for development were identified:

1. **Influence in the cognitive domain**. The UK should identify strategic areas of interest and act more boldly in support of a national narrative. This requires the capacity and will to conduct information operations, including the selective use of information and better understanding of audiences, both friendly and adversary. Understanding and shaping activity in particular takes time, and influence activity needs to be built into mission planning from the outset, not merely sprinkled on at the end of an operational plan as a force multiplier. Testing and developing this through exercises is essential. It also requires the ability to identify and attribute actions, for example, the response to the Novichok poisoning in Salisbury or the WannaCry cyber attack. More work is required to understand the risks and opportunities in information operations, and greater authorities are needed. A 'Defence only' approach is insufficient; it requires coordination with others, including the intelligence agencies and the National Cyber Security Centre.

5. The five operational domains are maritime, land, air, space and cyberspace. See MoD, 'Introducing the Integrated Operating Concept', p. 10.
6. Julian Corbett, *Some Principles of Maritime Strategy* (London: Longmans, Green and Co., 1911).

2. **Multi-domain command and control**. Command and control needs to be more dispersed, flatter and connected, while current approval processes are too slow. Improved data feeds that combine open-source and classified data and secure cloud capacity to pass data securely to the field and back to headquarters are crucial. So is the ability to pass information across partners. The US Joint All Domain Command and Control programme attempts this but is expensive. To help prioritisation and focus on solving operational problems, command and control needs to work from the frontline back to garrisons. With adversaries targeting command and control capabilities, however, developing redundancy and reversionary methods will be essential. Technology may help in some areas, but decision-making will continue to involve people who need to be prepared for and able to thrive in the new, and reversionary, environments.
3. **Full-spectrum targeting**. Defence must get better at looking at adversaries as a system, and then identifying and targeting vulnerable points. Target systems analysis is a crucial function and needs to take account of the electromagnetic environment. Defence also needs to mature the capacity to orchestrate full-spectrum effects so work done in individual domains can be integrated, and then connected with wider government action. As with information operations, considerable time needs to be invested up front to be ready for when action is needed. This requires expertise that is not always compatible with military career paths or posting cycles. It also requires legal permissions, for example, to engineer failure in supply lines or other elements essential to, but not directly engaged in, hostilities.
4. **Operating in the electromagnetic environment**. This includes cyber, but extends to other areas, including resilience throughout the supply chain and into operational use. Understanding cyber as a civilian and transformational space, as well as an operational domain, is important. Being artificial, it is different to the natural domains of maritime, land, air and space, and can be shaped and reshaped. As well as the criminal, intelligence and military uses of cyberspace, policy is also a contested area and the UK needs to be engaged at a national and international level to shape the environment, including educating its citizens to understand its opportunities and risks.

Working with government partners poses challenges, including clarity on the role defence should play and trust-building through training and exercising. Language itself is important; not only must it be understandable to others, but describe what they recognise. Criminal threats on the internet do not make cyberspace a war zone, and labelling it 'war' may make it harder for countries to respond appropriately. Self-awareness is also essential; considerably larger than most other parts of government and better resourced, working with Defence can be difficult for smaller departments.

Civilian services and infrastructure remain crucial; adversaries know this and target them. Consequently, integration needs to extend to the whole of society. Sweden's 'Total Defence' concept brings the whole country into national security. This includes collective resilience that goes beyond the military or even wider government. The population is engaged, including sharing intelligence and information, to create a high level of understanding in society. Industry is also aligned with the threats. All of this reduces system mismatches and vulnerabilities.

Internationally, responses will involve allies and partners, requiring the ability to integrate politically, geographically, temporally and in terms of data sharing and action. The ability to shape the security environment and work together seamlessly when needed is important. NATO plays a central role, and its 30 member states provide political and military credibility for action, but challenges exist. A multitude of weapon types, systems and C4ISTAR mechanisms complicates integration. Compromise is a central feature of working in NATO, and there is a need to examine how to speed up NATO responses, in particular to hybrid attacks. This is made more challenging as many civilian levers are within the competence of the EU, requiring close NATO–EU cooperation. The strategic dilemmas can be mitigated by having common goals, standards and values, and strong human and technical networks that foster better decision-making.

The US–UK relationship is crucial, both bilaterally and to NATO, representing 75% of NATO defence spending in 2021.[7] President Joe Biden is putting huge effort into NATO. However, the US struggles with 'consultation', with many states feeling decisions are made without prior discussion. The US needs to rethink how it engages with allies, and how to get NATO to broaden its partnerships, including with Australia, India and Japan. While the US is keen to reduce its defence spending and get allies to take more military and financial responsibility, it also wants to maintain its technical edge. However, in doing so, maintaining integration with the US can be difficult for smaller countries, with concerns that the gap between the US and the rest may become untenable.

Integration's partnership component reflects a diversity and inclusion challenge. It can only work with trust: trust that different actors all have something to contribute that makes the complexity worthwhile; trust that actor differences will be valued; trust that it is a collaboration, not a takeover; and trust that the different voices will be considered in determining the approach(es) to be taken. It is not clear that trust is ready for integration's weight.

Pace

Concerns were expressed that Russia and China were outpacing the West, and greater speed was needed in acquisition, doctrine development and decision-making. The ability to act at pace was emphasised, because states that cannot (re)act in time are irrelevant. AI and machine learning were expected to speed up the processing of data to lead to swifter and better decision-making. While they offer the potential to process more data and present the most relevant information, decision-making in many cases will remain with humans, who need to work within and deliver the faster processes.

Current work to increase the pace of armed forces' transformation also focuses on acquisition and experimentation, including exploiting exercises to test capabilities, decision-making authorities and partnerships involving government, international and industry partners. Equipment experimentation was occurring more frequently with units being established to

7. *Ibid.*

spiral-develop existing, or test new, capabilities. Pace also needs to be injected into force development processes to shorten the time between need and solutions, involving all elements of a capability.[8]

Mission partners are crucial, but different rules, processes and permissions need to be geared. NATO's standards agreements offer important tools for interoperability and speed. Equally important is the need for partners to work together to understand each other; this is as true for cross-government working as it is for international militaries. Understanding should cover what can or cannot be done, and how different actors work.

The discussion on pace, particularly for information and cyber operations conducted at the speed of light, highlighted that the speed of delivery is built on a foundation that takes longer to develop. Defence needs to speed up what can be done fast, but also accept what takes longer. Adopting Daniel Kahneman's concept of 'thinking fast and slow',[9] it is crucial to be clear about what is sensible to do quickly and what needs to be done more deliberately. Heuristics that allow fast thinking and rapid action are often formed through activity that takes time to generate. Defence career paths and reward systems arguably do not support the slow generation of expertise necessary to support quick action.

People

Integration depends on people: their skills, knowledge and behaviours. It is also a matter of culture, and the ability to work across cultures, both national and organisational. A broader range of talents is needed, requiring a diverse workforce bringing different skills and different ways of looking at problems.

Accessing talent will continue to be a challenge as militaries seek skills required by commercial employers, including coders, cyber security, data engineers and information specialists, who in future may be as valuable as pilots today. But it is not just specialists who need to understand integration's enablers, and mainstream courses need to include these skills. Talent will increasingly reside across the whole force; regulars, reserves, civil servants and external partners in academia and industry. Talent management needs to become more fluid, including secondments into and out of Defence, with outcomes unconstrained by which part of whole force the person comes from. A trial for managing medical and cyber skills at a Defence level (Unified Career Management) sees these cohorts managed collectively by Strategic Command irrespective of the individual's parent service. Another change pioneered by Strategic Command is in Joint Professional Military Education (JPME). This seeks to improve the talent already in Defence through reform of the content, style of teaching and broadening and deepening access to JPME, including exposure earlier in a career.

---

8. In the UK, capability is described as comprising training, equipment, people, information, doctrine, organisation, infrastructure and logistics (TEPIDOIL). It is described as doctrine, organisation, training, materiel, leadership and education, personnel and facilities (DOTMLPF) in the US.
9. Daniel Kahneman, *Thinking, Fast and Slow* (London: Penguin, 2012).

Education is crucial, and the UK's Integrated Review repeats the 2015 Strategic Defence and Security Review's suggestion of a national security skills academy to teach strategy and create opportunities for national security professionals to interact.[10] If accepted, this should include opportunities for key industries to participate so relationships across Defence, government, allies and industry are strengthened.

Conclusion

Integration must enable fluidity in responding to the challenges posed by adversaries. It must draw on capabilities across all military domains, across government and in allies and partners. Strategic Command's role was likened to that of an orchestra conductor, harnessing the talent of experts towards a single end. This analogy works for national-level multi-domain integration, but may not neatly reflect the complexity of cross-government and international integration where the orchestra is likely to be playing under a different conductor. The orchestra and musicians must be able to play different kinds of music.

Adversaries will continually seek advantage in ways that test the West's ability to respond. Integration is an important part of responding to this, and Strategic Command has a key role to play in setting the tone, culture and appetite for risk and reward that allows the investment in experimentation, rehearsal and people that is crucial to success.

Paul O'Neill is a Senior Research Fellow in Military Sciences at RUSI.

10. HM Government, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, Cm 9161 (London: The Stationery Office, 2015).