Integrating Information Manoeuvre
Nick Reynolds and Jack Watling
189 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 189 years.

The views expressed in this publication are those of the author, and do not reflect the views of RUSI or any other institution.

Published in 2020 by the Royal United Services Institute for Defence and Security Studies.

This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

RUSI Conference Report, April 2020.
Integrating Information Manoeuvre

On 10 March 2020, RUSI held a conference to bring together practitioners, policymakers, analysts and allies to discuss how the British Army is seeking to manage and exploit information on the future battlefield. The proceedings were off the record. This report is composed of observations by RUSI staff.

A consistent theme throughout the conference was that information manoeuvre – whether in terms of communications, intelligence, security, influence or cyber – centred on people. Cyber operations depend upon commanders being able to exploit opportunities created by interference with adversary networks, and appreciating how adversaries will respond. Influence operations must be premised on understanding how an audience consumes information – and their reference points for understanding it – and not those of the chain of command approving the activity. Security begins with an awareness of the risks across the force and appropriate management. Intelligence requires an understanding of the adversary and the ability of humans to accurately contextualise the information presented to them. Communications, while dependent upon technical systems, require clear procedures for what must be communicated and to whom. Education, training and realistic exercises that represent the contemporary operating environment including the virtual dimension are critical for successfully maintaining competitive capabilities against a diverse range of threats.

A second consistent theme was that the information domain is contested. The fact that data is increasingly agnostic of bearer network and may be fed into targeting via public channels, or distributed through internal systems, means that networks will be penetrated, corrupted, disrupted and denied by adversaries. Moreover, adversary attacks will target the physical infrastructure used to transmit and process data, intrinsically linking information manoeuvre to ground, air and littoral manoeuvre and other domains. In this environment, commanders will need to actively fight for access to data. They cannot simply expect the assurance of networks to be a line of effort, but must instead accept that adversaries will disrupt access. Thus, they must prioritise which links are vital, which are advantageous and which can be ceded. They must also consider when, given the application of their limited assets, ensuring connectivity or denying adversary connectivity is essential within the tempo of their operations and when it is not. Evidently, we must value our data as a critical commodity and develop associated resilience measures.

This again underscores how information manoeuvre must be linked to ground, littoral and air manoeuvre in the land domain. An information campaign may shape the environment so that physical effects have a disproportionate impact. Similarly, physical effects may create a window of opportunity for shaping narratives. Where these activities are not coordinated, they may conflict. Where one is applied without the other, they risk being ineffective, as physical effects cause negative political effects, or information operations lack an opening in the narrative to
Integrating Information Manoeuvre does not obviate the need for hard power, but manoeuvring for information advantage can act as a force multiplier for hard power, whether in deterrence or warfighting. The orchestration of effects across domains, and by deduction dimensions, remains a challenge, especially within coalitions, which is a high priority for resolution.

Over the past two decades, there has been a drastic increase in the volume of sensor data generated on the battlefield, and a corresponding expansion of efforts to capture, manage and exploit it. Much of this has evolved ad hoc, or in parallel silos. Maximising the benefit of this data today depends upon ensuring that it is mutually intelligible and transferable between systems. To that end, integration is a critical priority, and the purpose of a unifying concept such as information manoeuvre is in part to develop an agreed framework to best utilise and integrate several discrete strands within Defence, with a focus on operational outputs. While information manoeuvre as a concept allows the Army to better understand how it integrates data management with its traditional physical capabilities – and will help to determine how it wishes to employ data in the future – the development of cloud technologies to underpin information management must be a joint endeavour. If the Army is to access track data on targets from the RAF to conduct strikes, these systems must be compatible across the force. Putting in place the groundwork for future capability therefore needs integration under Strategic Command, and likely clear direction from the Integrated Review.

Finally, transformative capabilities in the information domain can be envisaged but are not yet realised. The precise timeframe for battlefield artificial intelligence (AI) is difficult to predict. Nevertheless, decision-makers in defence industry will need to set the groundwork today if they are to be in a position to exploit emerging capabilities. This will require the integration of industry, academia and allies as part of a broader innovation ecosystem. First, there is a need for an audit of existing data, alongside the development of standards for logging, mapping and harmonising it. Second, a common operating system must underpin future military capabilities so that all data within the system can be leveraged. Third, the capacity to upgrade sensor platforms to conduct more complex edge processing will be essential to avoid centralised headquarters being starved of relevant information or drowned in irrelevant data. Integrated innovation along these lines should be better positioned to generate application, data and analytics (including AI) capabilities at pace. In conjunction with this transformation, permissions and authorities require reviewing if fleeting opportunities are to be exploited.

The Integrated Review provides a further opportunity to address procurement agility. The conference suggested that getting innovation, procurement and permissions right was critical to advancing information manoeuvre capabilities to outpace adversaries.
About the Authors

**Nick Reynolds** is the Research Analyst for Land Warfare at RUSI. His research interests include land power, wargaming and simulation. Prior to joining RUSI he worked for Constellis. He holds a BA in War Studies and an MA in Conflict, Security & Development from King’s College London. During his time at KCL, he was Head of Operations of the KCL Crisis Team, which organises large-scale crisis simulation events.

**Jack Watling** is a Research Fellow at RUSI, responsible for the study of Land Warfare. Jack has recently published detailed studies of the British Army’s Strike Concept, achieving lethal effects with small UAVs, Iran’s strategic objectives and its capabilities, British training and assistance programmes in Yemen between 2004–2015, allied integration into Multi-Domain Operations, and Amphibious Operations, among other projects.