Te Matataua

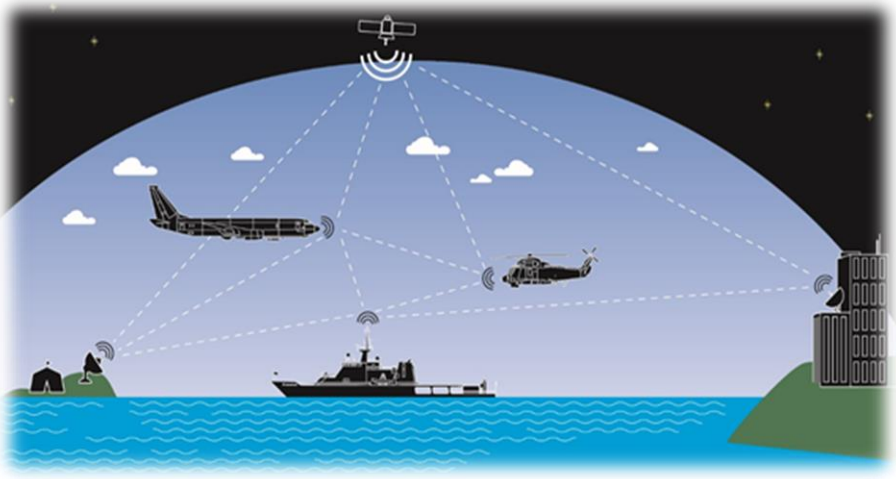
The Scouting Party of Air Power

RNZAF Air Power Development Centre Bulletin

Issue 27, December 2018

Operational Agility in a Multi-Domain Operating Environment?

The latest phrase to join the ever expanding lexicon of military jargon is, ***Operational Agility (in a) Multi-Domain Operating Environment***; so what does it mean? Let's start with Multi-Domain Operating Environment (MDOE) as this is straightforward. Multi-Domain (MD) is simply military operations that take place in, or utilise, two or more of the: cyberspace, land, air, sea, or space (CLASS) domains. To illustrate the term by way of an example, imagine an RNZAF P-8 carrying out a maritime patrol in conjunction with an RNZN Off-shore Patrol Vessel (OPV) around the Pacific Islands. The P-8 is operating in and from the air in the maritime domain, and is operating out to 200nm (≈370km) from the OPV. It is using Satellite Communications (SATCOM) to upload secure real-time data to the OPV, as does the ship's embarked Seasprite. The OPV filters the information and sends, again via encrypted SATCOM, the local maritime picture to HQJFNZ. At the same time, the NZ Army is manning a satellite ground station feeding supplementary material back to HQJFNZ. Additionally, each element is communicating directly with each other via encrypted and/or unencrypted radio communications whenever in range. The combined imagery and data is used by HQJFNZ to form a user defined operating picture (UDOP) that can be disseminated to other military units or government departments that require it.



Example of Multi-Domain Operating Environment

So, a simple maritime operation may require the use of all domains. While multi-domain operations are a reality now, we do not think of them as such, and consequently we do not think in terms of Multi-Domain Command and Control (MDC2). Adjusting to the newly realised MD environment will require a new way of thinking and operating. Currently sailors, soldiers and airmen rarely think outside of their own domain and consequently their cognitive approach will have to expand to become MD aware. Therefore, those in C2 roles and structures will require a robust working knowledge of each domain.

The current Air Operating Centre (AOC) model for exercising Air C2 is unlikely to cope with the complexities of MDC2 and consequently we will need to shift to a Multi-Domain Operating Centre (MDOC) model that is capable of integrating MD operations by fusing, analysing and distributing data to those who need it. Survivability of the MDOC will also demand smaller, agile, distributed and dispersed C2 nodes. MDOC airmen will ideally be career C2 professionals (Battle Managers) who are trained to consider and appreciate the full range of domain capabilities, and understand their effects and limitations. MDOC airmen will need to be supported by tactical specialist Liaison Officers who provide operational advice. The MDOC will provide a dynamic sourcing, tasking and execution cycle that

seeks to operate inside an adversary's OODA loop[1]. And if one domain loses superiority, then the MDOC will use the other domains to achieve objectives.

So where did MDOE come from? The pervasive manner in which cyberspace and space have come to influence military operations over the last 50 years or so has now evolved to the point where they are now recognised as domains in their own right; and each has its vulnerabilities and advantages.

Cyberspace and space are different to the traditional land, sea, and air domains, in that while they are domains in a broad sense (an area where military operations are carried out), they are not environments within which a person operates. Military forces do not physically deploy people into cyber-space or space, not yet anyway, so cyber-space and space are unique in that aspect. And while space in the future will become a deployed military operating environment, no one will be deployed 'in' cyber-space. Cyber-space can be considered an enabler of the other four domains.

To operate as part of an 'integrated' force in the future, MDOE is going to require a new approach; this is **Operational Agility**. The concept of an 'agile' military is not new, and surfaced around 20 years ago as an enabler of information warfare; and while it was more or less to do with speeding up the decision making cycle, no consensus was ever reached over what it meant. The concept of agility though has evolved, in a similar way that security has (which has widened considerably from the idea of physical security), and now cuts across many aspects of military activities. There are now a number of agilities, such as; organisational; tactical; conceptual; acquisition etc., and now, somewhat inevitably, it is being applying to logistics and C2.

Operational agility is the ability to rapidly generate – and shift among – multiple solutions for a given challenge.[2] It is being able to adapt rapidly and precisely, and being able to exploit any change in circumstance along the way. In large part it is a measure of our resilience. Operational agility has a number of drivers, not the least of which is shrinking defence budgets. Budgets that won't easily sustain the status quo or enable growth, together with threats that won't permit doing less, means militaries must be agile in the ways they use their means. As systems and platforms become more complex and interdependent, a major test of agility is how rapidly new capability can be successfully introduced and transitioned to.

The size or funding of an organisation does not automatically indicate how agile that organisation is. One belief is that limited resources may limit agility as consensus appears to be that the bigger the organisation the greater the agility; based on the bigger the toolbox the more tools you have. However, a small specialist niche force can be positioned to respond quickly and with a light footprint, being more nimble, though a single platform or capability is also a single point of failure. One doesn't have to be the biggest, fastest or strongest; just big enough, fast enough and strong enough to do the job.

The key to agility is being the first to know something. The 'West' can no longer rely on a qualitative edge to win the fight, and being the first to know is where the advantage is gained. Advantages are transient, perhaps only minutes or seconds long, and as the human element is often the dominant factor in delays, Artificial Intelligence (AI) sorting through big data sets will be required to prevent information overload, thereby allowing decision making to keep pace. This will require an agile C2 system with flatter C2 networks, and greater delegation of authority, which also aids in recovery after cyber or physical attack.

The cognitive abilities of our Battle Managers will be paramount, with humans and computers working in harmony, analysing, developing plans; running simulations and directing operations just in time. One thing will never change though - no amount of technology will ever remove the fog and friction of war, though we will get a better look at it.

Key Points

- Operational agility will require us to think multi-domain.
- Complexity will demand C2 professionals.
- Space and cyberspace will be as integral as air ops in the Air Force's approach to MD ops.

Further Reading

- Jacoby and Shaw, Strategic Agility: Theory and Practice, *JFQ* 81 (2nd Quarter, April 2016).
- Anthony H Dekker, Measuring the Agility of Networked Military Forces, *Journal of Battlefield Technology*, Vol 9, No 1, Mar 2006

[1] The Observe, Orient, Decide, and Act loop, or OODA loop is a method of gaining situational awareness so you can anticipate, and provide effects to counter your opponent before they act.

[2] USAF, *Air Force Future Operating Concept: A View of the Air Force in 2035,* September 2015.

E-mail: ohapdc@nzdf.mil.nz