OCTAVE

WHITE PAPER

Beyond boundaries: Unleash the power of multi-domain operations



Introduction

Within NATO, there are five domains of operation: maritime, land, air, space and cyberspace. These are duplicated across 32 member nations and over 40 partner countries and international organisations. Given the speed of information, data flows and adversarial capabilities, orchestrating military activities across all domains, all members and partners as a single force is crucial for long-term defence and deterrence initiatives within NATO.

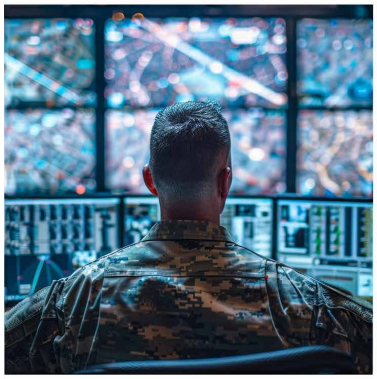
For many years, member nations have run joint operations – planned, prepared and executed by a variety of centres and commands, but now, the push is for multi-domain operations (MDO).

- **Joint operations** involve multiple nations and military services
- **MDO** includes military and nonmilitary assets, with a holistic approach to operations across multiple domains (land, air, sea, sea, space and cyberspace)

In order to be successful in MDO, organisations need to embrace digital transformation and have the right technology in place, the latter of which will be outlined in this white paper.











What is MDO?

At its core, MDO refers to the push for NATO to orchestrate military activities across all operating domains and environments. These actions are synchronised with nonmilitary activities and enable the Alliance to create desired outcomes at the right time and place. This allows NATO's Military Instrument of Power to prepare, plan, orchestrate and execute coordinated activities in collaboration with other stakeholders and actors associated with the Alliance.

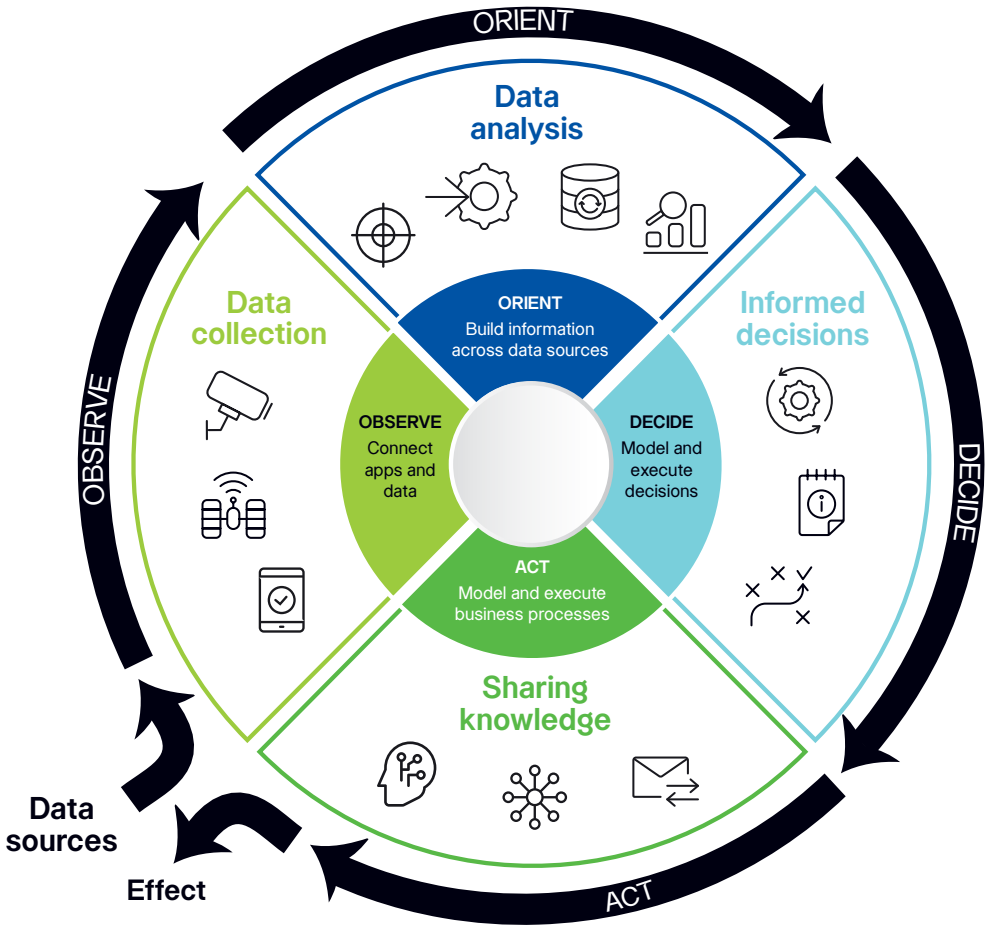
The stakeholders in defence agencies and nonmilitary organisations are part of MDO in differing ways.

- **Commanders** receive intelligence from wider sources, giving a more comprehensive view for better-informed decisions; however, there could be timing, assurance and trust concerns
- **Deployed troops or response personnel** collect data to be shared beyond their usual networks. This should be with no extra effort on their parts; likewise, they receive information or commands from multiple sources
- **Defence system architects** want to open up compartmentalised information and data silos, to enable data sharing with trusted parties
- **Solution providers** need to design around standards and bake interoperability and integration into their solutions

MDO delivers tailored options that build an advantage in shaping, contesting and fighting and presents dilemmas that decisively influence the attitudes and behaviours of adversaries.[1] MDO is not unique to NATO; it can be envisaged and employed by any military force, ranging from two artillery battalions operating together to multinational military and nonmilitary agencies operating in a natural disaster or countering grey warfare.

The aim of MDO, or any military operation doctrine, is to be quicker in your Observe, Orient, Decide, Act (OODA) loop than your adversaries. The OODA loop is a decision-making model used for quick and effective outcomes. When you are quickest, you can outmanoeuvre your opponent and come to your chosen outcome of events. MDO is intended to combine and collate all observers (sensors, systems, etc.), commanders making decisions (strategic, operational and tactical) and methods of action for the common desired outcome through the instruments of power most suitable and as available (military, political, national, etc.)

[1] www.act.nato.int/article/mdo-in-nato-explained



OODA loop

Achieving success in MDO depends on several factors. These include:

- Digital transformation
- Combination of processes and technology
- Engagement of people
- Having standards in place
- Ease of interoperability
- Ability to integrate technology
- Implementation of a digital backbone
- Controlled data sharing

MDO is a system of systems that includes command and control (C2), a common operating picture (COP), data analysis and cataloguing, etc. Collaboration amongst system integrators, NATO, partners, nations' forces, etc. in all geographical areas will be required to enable MDO.

Digital transformation and MDO are two of the main things defence organisations (NATO, European Defence Agency, etc.) are focusing on. Others include innovation, speed of change, core defence and deterrence. Plus, as MDO also involves nonmilitary agencies, it overlaps with other processes, people and technology in public safety and government agencies – which are transforming at different paces.

Benefits of MDO

Interoperability

Data and processes can be stored and shared in standardised formats, making interoperability possible and much easier between systems – standards include NATO STANAGs and commercial Open Geospatial Consortium (OGC) and International Standards Organisation (ISO)

Easier sharing

Data and processes can be shared much more easily and quickly with necessary entities

Security

Conversely, shared data can be controlled much more easily with, for example, certain user groups for a certain amount of time

Resilience

Data can be replicated/backed up to different physical locations; when combined with data-centric security, it is more resilient than hard copy data

Quicker processes

Automation transforms processes, making them faster and enabling, for example, built-in quality checks, attribution and the ability for them to be triggered when new data is received

Collaboration

Speed and ease of working with other agencies, departments or nations to share current information

Trust

Data assurance is paramount for commanders to trust data and information from third parties as though they had captured and processed it themselves

The key areas impacted by MDO and necessary for digital transformation to support MDO, are people, processes and technology. This paper will focus on some of the technology aspects related to these areas.

Technology aspects of MDO

Enabling interaction

With agencies coming together to respond ad-hoc to incidents, they will need quick, known methods to connect their systems or share data. Adhering to defence standards is a traditional approach to interoperability (see more on this later). Geospatial defence standards are set by OGC, STANAGs, DGIWG, nations, etc. and these change over time. Defence procurement often requires standards to be used; however, these standards should be baked into solutions from conception rather than tacked on to meet a requirement. They should be fit for purpose and, indeed, "standard," – not adapted for NATO use.

Octave is very strong in building its products around standards and implementing those standards thoroughly. By adopting standards from various domains including maritime, aviation, geospatial, cartography, building information modelling (BIM), etc, Octave's software can be used to fuse, analyse, view and manage data from all domains. An example would be the Octave Alto (formerly Luciad) SDK, already used in numerous defence applications on land, sea, in the air and space.



Combining sensor feeds for improved situational awareness

Interoperability refers to the ability of different systems, devices or applications to work together and exchange information effectively. Whilst this is obviously related to standards – and for NATO the Federated Mission Network (FMN) – to be able to operate together, systems and people need awareness of respective capabilities, data holdings and shared outcomes. Even if data is delivered in a standard web service, how is that service "advertised" and accessed? Once accessed, to make use of the service the client needs to know what the data is capable of. Can it be used for change detection against another data source, for example? What is its temporal range, its ground sample distance, its band spectrum, its positional accuracy, etc.?

Having a "neutral" collaboration platform that can be used ad-hoc to respond to incidents and run operations will help MDO actors interact with ease. A hosted platform enables organisations to easily share and act on data in a secure environment to power real-time incident and operations centers.

Need to share

The digital backbone is simply infrastructure unless it has the lifeblood and nervous system carried along it – meaning data, communications and information in defence. The flow of data, information, workflows, commands, etc. needs to be uninterrupted and accessible. NATO talks about the NATO Digital Backbone (NDBB) being foundational in connecting the edge to decision-makers and effectors. As Octave's software is used from the edge to the HQ, it feeds and utilises the NDBB as needed, in addition to working standalone.

Data in silos is not fulfilling its potential. Whilst a lot of defence data is sensed and captured for a particular use, it could be and often should be utilised by more than one audience. This is particularly relevant for geospatial data, which often captures multiple aspects of the environment.

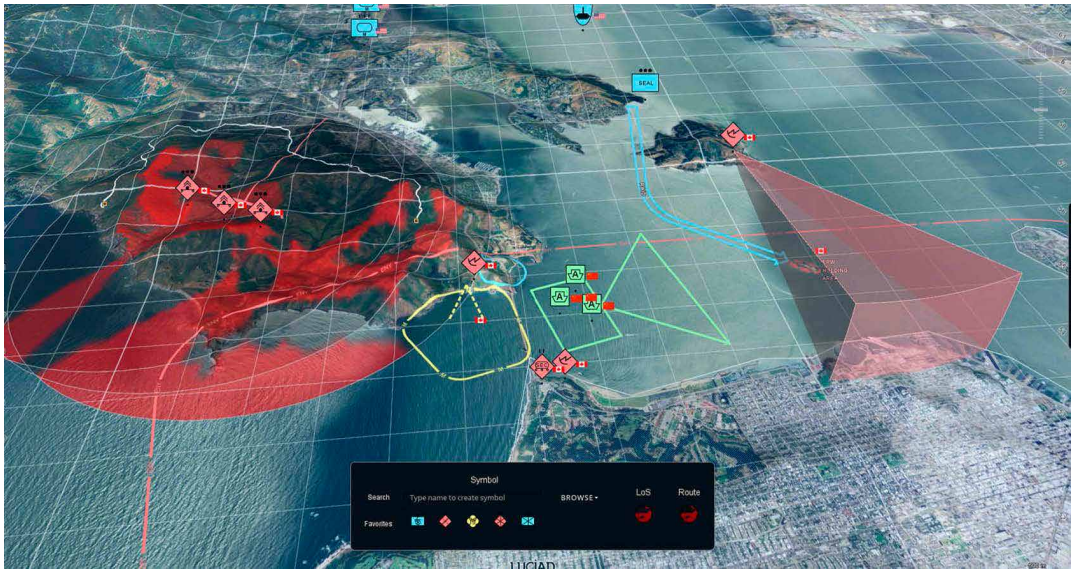
By making data visible - accessible - understandable - linked - trustworthy - interoperable – secure (VAULTIS) and findable - accessible - interoperable – reusable (FAIR), defence organisations will benefit and extract more intelligence.

MDO uses digital transformation to ensure traceability of data and changes made to data by systems or human operators. These are often recorded automatically in digital workflows and offer traceability as a valuable benefit for digitalisation. Cataloguing data records its properties, availability, etc., with software such as Octave Alto Data Management (formerly ERDAS APOLLO) recording numerous data formats, web services and database contents. Having federated data catalogues with standard metadata means all forces and systems know how to search for data in their areas and times of interest. There can easily be a Babylonian confusion – where different words having the same meaning and vice versa are unknown/ exchanged between data originators and users. So, the terminology used is important for international military operations, with semantics being a constant discussion point at NATO. Secure, selective sharing of data across (through) boundaries enables the right data to be accessible by the right people at the right time, leading to better contextualised decision-making.

Analysing the deluge of data

As with any business trying to outperform its competitors, defence will benefit from automating tasks such as data analysis, cataloguing, sharing and so on. This will speed up tedious tasks and simplify complex procedures, meaning shortening the OODA loop and freeing up SMEs to work elsewhere. With data being received 24/7 from various sources, the automated workflow can ingest, analyse and summarise data to alert the human of points of interest. This avoids the human analyst having to look at all data in case there is something of interest in it. With imagery data this could be highlighting potential areas of terrain changes or a decrease in the number of ships in a harbour.

Automation can include validating data before a human operator even knows new data is received – preventing them from opening invalid data, perhaps because the point of interest was not captured in the image data.



Data from multiple domains – land, sea and air – in one view

Once data and workflows are digitised, they are easier to share with end users/systems. Rather than having to duplicate data or teach multiple users a workflow, they can be shared in a controlled manner via web services and APIs. This helps spread specialist capabilities to untrained users, removing training burden whilst helping increase the value extracted from data. It also helps assure processes are run in the same way every time, increasing trust in outputs.

As confidence and trust in AI grow, the introduction of agentic networks, with AI agents "roaming" across data with authentication to exploit data suitable for their allocated tasks, will work on data 24/7. These never sleeping data analysts will not necessarily give any results which a human analyst could not discover; however, they will work through data much more quickly. Defence is often keen to keep a human in the loop when it comes to processes, so AI agents can help by alerting the human operator to interesting, relevant and timely data.

People, processes and technology are in order of importance, yet it seems technology is ahead of the first two. Technology should be driven by processes as set by digitally literate people. Octave can assist defence organisations in at least two ways here – showing the art of the possible to alleviate data bottlenecks, etc. and helping set up configurations of software for customers/end users to maintain.

Whilst demographics of defence forces change overtime, the generational differences are affecting agencies. New recruits are used to having simple, focused, straightforward apps that run 24/7. Whilst Octave's geospatial software is function rich, it can be simplified through configuration, using Spatial Modeler and focusing on use cases. The user interface can be on the desktop, browser or via an app, enabling differing delivery methods depending on the audience and need.

Sustained technical edge

Technological obsolescence is often introduced during procurement by defence procedures. A shorter, quicker process is needed, with systems designed and targeted for tomorrow, not the next decade. With off-the-shelf offerings, commercial companies can help deliver solutions within their time of relevance and reduce the obsolescence burden. Defence is also shying away from bespoke, behemoth systems and preferring configurable, off-the-shelf software, often from commercial sources. Using dual-purpose commercial off-the-shelf (COTS) software will help defence work across MDO and deliver solutions faster.

This COTS software has various strengths and benefits, including the ability to adapt to technology changes, incorporate multiple-user feedback and have greater assurance through regular, frequent quality and security checks. Defence benefits from dual-use software to maintain interoperability and help integrate multiple workflows. Regular software updates with installers and support on-hand eases the maintenance of defence systems and helps optimise resource allocation. Plus, COTS software is certified for export, with standard export restrictions in adherence to U.S. Export Administration Regulations (EAR) and EU's Regulation 2021/821, for example.

As the intelligence, interconnectedness, decentralisation, digitalisation (I2D2)[2] of defence and defence data continues, creating a single pane of glass through which to look at the current situation will become harder. MDO will both increase the complexity of this and also aid the achievement of this, having means in place to share, collaborate, analyse, etc.

[2] www.nato.int/content/dam/nato/legacy-wcm/media_pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

Conclusion

Octave technology is widely used by defence agencies and nations, enabling forces to quickly and thoroughly interrogate data and extract information, streamlining the mission-critical decision-making process. With built-in cross-domain interoperability capabilities, our technology gives defence organisations the ability to digitally transform; produce, analyse and manage geospatial information; develop powerful solutions; and, ultimately, fully engage in MDO.

Discover how Octave can help your organisation embrace MDO

LEARN MORE

About Octave

Octave is a leader in enterprise software, turning data into decisive action and intelligence into your edge. Our software solves for and simplifies complexity, from the design and build to operations and protection of people, property and assets – for any scope, at any scale. For decades, we've partnered with customers to sharpen performance, elevate efficiency and amplify results. From factory floors to entire cities, our solutions are tuned to scale up what's possible from day one onward.

© 2026 Octave