Picture credit: Getty

MISSION POSSIBLE

Brigham Bechtel *reports on the importance of optimising delivery of mission critical data*

Growing volumes of data and improvements in artificial intelligence (AI) and machine learning (ML) are disrupting the traditional ideas of the Observe-Orient-Decide-Act (OODA) loop and now require new means to deliver the information effectively. It is widely acknowledged in national security circles that big data is key to harnessing mission critical insights necessary for commanders and policymakers to prevail over adversaries. However, the OODA loop begins to look more reflexive than deliberative as time is compressed. Those with the ability to ingest the volumes of available data and orient faster could decide and act before an adversary. In the case of AI, it means human input into algorithms must precede potential scenarios well in advance. Therefore, new means to manage data must be employed in order to accelerate information used in the loop for vital decisions and actions.

Our understanding of the OODA loop is challenged from the outset by increases in the volume of data available. As more devices are able to connect to networks – vehicles, sensors, and equipment – more information is available to ingest and orient to inform key decisions. A vital advantage can be gained if one can make more accurate decisions, give precise instructions and launch calculated tactics faster than an opponent. The speed that's made possible with AI moves the emphasis away from the human calculus during such events.

Defence and intelligence organisations must find new ways to obtain real-time understanding for the "orient" portion of the loop from these huge volumes of data. In our systems now, algorithms represent the orient portion of the loop, which is where OODA's author, Colonel John Boyd, placed the emphasis on understanding the data ingested. 'Orient' takes account of culture, experience, and even genetic dispositions and biases. Here, analysis of potential outcomes moves to the 'decide' phase of the loop. For humans these factors represent years of training and education and some of it even becomes subconscious. For AI responses it requires humans training algorithms through neural networks well in advance of data input and then testing of the algorithm. The developers working with military professionals, or who are themselves operators, must train neural networks as they train themselves – making use of lessons learned, best practices, ethics and values – before deploying an algorithm to solve even the most mundane tasks.

The advantage that optimising data management provides can make the difference between success and failure

MANAGING THE DATA

The challenge now is to handle volumes of data at critical speeds to facilitate successful use of AI. Speed, volume, and variety of data – structured and unstructured – differentiate the AI process from previous methods of human analysis and response. In the information age, the broad spectrum of data sources – transmitted from distances, foreign language, different formats – arriving in massive volumes at near real-time speeds makes it harder to ingest and access all of the available reporting for use in decision processes. The data handling and availability must all occur at speed to respond defensively, or to intrude on an opponent's OODA loop. In conflict the adversary is likely to have AI-enabled systems too, which complicates efforts to disrupt their plans or defend your own.

Additional processing speed will not be enough for overloaded data systems to ensure the smooth ingestion and integrity of the data with context in order to support AI algorithms and thus complete the loop in time. Furthermore, the demands on AI are increasing for shorter response times in conflict scenarios as weapon systems and cyber weapons become faster. The problem is further complicated when an adversary's weapons are automated and enabled by similar algorithms. Faster responses are required of even seemingly mundane processes associated with things like supply chain management for loss replacement will be key in modern conflict.

In future, it may be that a general or admiral will not be part of a tactical response executed by an AI algorithm which could impact the success of his operation. Instead, a developer with some knowledge of military objectives, but an understanding of the mechanics of a system he writes for might have as great an impact on the outcome of an engagement as the officer who commands the forces employed. For example, a developer writing code for weapon systems to cope with a drone swarm effort to overwhelm a nation's air defences would write algorithms based on data from sensors, information about potential attacking drones, about the defensive weapons and about potential follow-on attacks. His calculations for algorithms would need to be vetted against the value of the drones, the targets, the follow-on forces, the defences in reserve and of course environments. All this would need to be accounted for in an algorithm well before any forces are employed by either side in the battle.

While OODA still has its relevant applications and remains widely taught in military circles, it may not be the most appropriate concept to apply when it comes to managing large and isolated data sets as the age of big data matures. The steps associated with OODA primarily described processes of how commanders or individual warriors won battles with the limited data available in the past. Is there still adequate time for a human to observe and orient or disrupt the adversary's OODA loop when the volume of data available grows exponentially? What happens when all the available data is not accessible to our human-machine teams?

BIG DATA IS KEY TO HARNESSING CRITICAL INSIGHTS FOR PREVAILING OVER ADVERSARIES

What is evident is that a much more agile and streamlined way to process data is required for speed of mission. Legacy relational models and large data storage solutions are not fit for the ingestion, curation, and provision of massive amounts of data at a speed that would enable AI to respond effectively. Things that hamper those systems include: relational models require ETL processes that inhibit speed and governance; relational systems have difficulty scaling quickly to meet demands; they cannot handle unstructured data; and legacy systems require too much human review for quality control and rapid integration.

Crucial data can often be difficult to access which challenges both the observe-and-orient processes of the OODA loop. The information can be trapped in silos and exist in unstructured formats or file types, anything from geographical coordinates to a written letter. There is also no guarantee a report is accurate. Even when data is accessed and ingested, its integration with other important data sources is what leads to the most vital insights for the frontline use and can be the most difficult step. The combining of information from multiple sources enables examination, corroboration or verification of details that power AI algorithms. File formats, sizes and volumes of data cannot be allowed to prevent the integration so vital for the orient process.

The advantage that optimising data management provides can be the difference between success and failure. It is imperative that military organisations use the best data management tools to ingest reports in various formats and derive useful insights. Tools that offer an 'as is' alternative to inefficient ETL processes can help data integration so users do not have to curate and sort it manually before use. This integrated data resulting from proper tools enables humans, algorithms and machine learning to power autonomous decision making.

Once data is ingested, a range of technologies are now available to make use of it faster. Machine Learning can quickly detect patterns in data sets and artificial intelligence can take action automatically. Intelligent devices that are connected to networks are now

www.intersec.co.uk

operating on a two-way stream of information and can continuously make autonomous adjustments.

Consider an Unmanned Aerial Vehicle (UAV) tasked with surveillance on an enemy base, which can then fly autonomously based on pre-set flight plans combined with intercepted and triangulated transmissions. If the UAV receives data indicating a priority target is moving from a flight box, an algorithm can tell the drone to move to observe the target without waiting for pilot input or after a lengthy deliberative process. Instead of a slower command time going through the four steps of OODA, the machine can exploit the information because of the algorithm, speeding up responses to dynamic situations. This would not prevent command intervention to re-direct the drone, but it could save response time critical to maintaining coverage.

Another example could be sensors located on the aircraft that monitor its operating state and feed its maintenance algorithms. An automatic feedback loop could enable efficient ordering of replacement parts, which can feed a headquarters-based system to monitor supply chains. Crew chiefs can plan their workload based on AI, leading to higher readiness and availability of the airframe for more missions. Other benefits would be for the manufacturers knowing what is needed for a robust supply chain, more predictable supply requirements, and more efficient use of personnel and materials.

The importance of accessibility and quality data to support the processing capabilities of artificial intelligence in completing analysis is often overlooked. Professionals know artificial intelligence is only as powerful as the data it uses; it must be both accurate and complete because bad data leads to bad results. Many national security organisations pursue the promise of AI, but have difficulty solving the problems of data ingestion, governance and transmission with security and speed.

Artificial intelligence offers many advantages, but amidst the buzz, it is easy to neglect the importance of protecting the data. The connection of security to accuracy is ensuring the integrity of the information. Reports might be inaccurate from a source, but they cannot be inaccurate due to mishandling in the data management system. Secure means more than protection from theft; data must be incorruptible and safe from bad actors. Once data has been collected it must be stored with the capabilities for granular levels of control including who can access what data, when, and for how long. Analysts and data scientists tasked with assuring data quality must have systems that compliment their work.

Good data governance assures provenance and lineage while providing transparency into the movement of data and who edited it over time. Well-governed data also ensures the right people are accessing the right data as it moves and is transformed.

Having the correct technology in place to enable swift, secure processing of mission critical data can enable new technologies and replace some human OODA loop processes. This has the potential to provide commanders with a full intelligence picture in real time and enable AI when every second counts ●

Brigham Bechtel joined MarkLogic as a 31-year veteran of the United States intelligence community having served for more than 26 years in the Central Intelligence Agency with experience in leading operations, and in analysis. Mr. Bechtel has tours in field leadership with experience coordinating the work of the intelligence community, law enforcement and military partners.

In future, a tactical response may be executed by an AI algorithm rather than a general

Picture credit: Getty