Ones and Zeros: Creating an AI-Driven, Data-centric Approach for All-Domain Operational-Level Simulations

Matt J. Martin
2200 Arlington Downs Rd
Arlington, TX 76011
USA

Matthew.Martin@caemilusa.com

ABSTRACT

As NATO and the member nations prepare for the highly-contested, near-peer potential conflicts of the future, the all-domain, data-intensive nature of these operations quickly outstrip the capabilities of legacy approaches to training, testing, and concept development. It is simply not possible to present sophisticated, multi-domain threat representations—with integrated effects from space, cyber, electronic warfare, and sophisticated red force tactics—on live-fly ranges or using legacy M&S tools. CAE has been developing a high-fidelity, all-domain, M&S environment, with red forces controlled by behavior graph-enabled generative AI, and tools to generate synthetically all the Command & Control Intelligence / Surveillance / Reconnaissance data, to enable training, testing, and concept development for near-peer, highly contested Battlespaces at scale. This capability has been tested at multiple large-force exercises. Initial results indicate that the process of multi-domain command and control, as well as intelligence exploitation, targeting, and planning can be improved in terms of speed and accuracy in executing the targeting process. This paper will review the development of these capabilities and the results of our testing. We propose the expansion of this capability to NATO operational C2 hubs such as Combined Air and Space Operations Centers (CAOCs) and Joint Task Force (JTF) components.

1.0 THE DATA ENVIRONMENT OF THE PEER THREAT

The emerging threat scenario faced by NATO and her allies is the high-end, sophisticated, threat-contested environment where you would expect sophisticated air defense systems, electronic warfare, and rapid targeting of all-domain blue forces. In the past, the NATO intelligence and targeting apparatus was focused on the lower-end of the spectrum of conflict: the counterterrorism, counterinsurgency fight where the intelligence analysts support special operations or other small task forces to hunt down specific high-value targets. Training was focused on the operational level of C2ISR: intelligence analysis, targeting, operational command and control.[1] Centralized intelligence centers called Distributed Common Ground Stations (DCGSs), received data from many ISR platforms and sensors. Through a process of exploitation that fuses the data, assessments are made, and intelligence products are produced to support their different customers.

In the past, this type of intelligence exploitation, as well as targeting, and operational command and control was primarily learned through on-the-job training[2] along with the occasional Large Force Exercise (LFE). This was partly because there was always a need to get people into action, to start assessing these huge quantities of data. But also because the capability to replicate that type of data-immersive environment did not exist.[3] The best training was on-the-job training with an instructor over the shoulder.

It's a different threat environment now. The military power of the NATO Alliance is eroding in the face of

[1] Arndt Freytag von Loringhoven, "A New Era for NATO Intelligence," *NATO Review: Opinion, Analysis, and Debate on Security Issues*, 29 October 2019, https://www.nato.int/docu/review/articles/2019/10/29/a-new-era-for-nato-intelligence/index.html

[2] The Joint Warfighting Center Joint Training Division, "Focus Paper 8: Intelligence Operations at the Operational Level," *Insights & Best Practices*, United States Joint Forces Command, April 2011.

[3] Sten Rynning, "After Combat, the Perils of Partnership: NATO and Afghanistan beyond 2014," *Research Paper, No 80,* NATO Defense College, Research Division, Rome, July 2012, Page 2.

adversarial nations as they develop and acquire equivalent weapons to become peer threats. This makes training difficult because until conflict actually breaks out, there is no on-the-job training to be done. Live sensor data which could be used for OJT during operations in Iraq and Afghanistan is obviously not available for conflicts that have yet to break out. This is where Modelling & Simulation (M&S) driven by Artificial Intelligence (AI), can make a difference. These tools are able to generate the high-resolution synthetic data needed to stimulate C2ISR processes at the operational level, and also employ AI tools to increase the complexity and fidelity of simulations needed to prepare for these threats.

1.1 The Data-Centric Environment of 6th Generation Conflicts

6th generation combat aircraft are expected to eclipse current 5th-gen aircraft such as the F-22 and F-35 in one key area: the fusion of information in the battlespace to greatly increase the speed and accuracy of target identification and prosecution.[4] Not only will 6th-gen aircraft retain the key elements of speed, maneuverability, and stealth; but they must be survivable against highly-sophisticated air defense systems. This drives the need not only for multi-spectrum stealth—the ability to evade detection by a broad range of sensor systems beyond radar (infrared, signals, electro-optical, etc.), but a need for rapid and automated processing of data from sensors and communications systems. Next-generation combat systems will need to be able to see first, make sense first, and rapidly engage targets—from beyond line-of-sight ranges—in order to act faster than an enemy's decision-making process and achieve the initiative in targeting.[5]

The future of conflict will therefore be dominated by a need to collect vast amounts of data, from all-domain sensors (space, air, ground, maritime, and cyber), make sense of that data, and make decisions quickly. The NATO Alliance has set the goal of developing concepts and tactics for Multi-Domain Operations (MDO) in order to plan, synchronize, and execute military operations across all domains and environments at speed and scale.[6] In fact, NATO's newest Strategic Concept puts "cognitive superiority," "integrated multi-domain defence," and "Cross-Domain Command" at the center of NATO's approach to achieve both an effective deterrence as well as an ability to prevail in a conflict should deterrence fail.[7]

This means that not only will intelligence analysts, C2 operators, and targeteers supporting NATO operations need to be able to rapidly collect, process, and comprehend the vast quantities of data that will be streaming from next-gen ISR sensors during a conflict, but they must achieve proficiency in targeting at the operational level prior to any crises. This is the only way that a NATO deterrence posture can be considered credible enough to prevent large-scale conflict from breaking out.

But with no existing dedicated training capability to achieve this level of complexity, no opportunity for on-the-job-training, and few opportunities to participate in complex LFEs, M&S must be brought to bear. But how to achieve both data-immersion and peer-level complexity via M&S?

1.2 Intelligence Exploitation and the Need for Data

On any given day, at several of the world's hotspots, national and NATO reconnaissance units are conducting missions in support of NATO operations. These may be MQ-9s belonging to the US or another NATO member. They may be the NATO Alliance Ground Surveillance RQ-4 platform. They may even be ground troops with tactical sensors tasked to perform operational Intelligence, Surveillance, and Reconnaissance (ISR). But in all these cases the operations crews carrying out those missions would be conducting some level of intelligence exploitation and analysis of the ISR data they collect—a first level of ISR exploitation.

[4] Jon Harper, "What to Expect from Sixth-Gen Aircraft," *National Defense,* 16 Sep 2019, https://www.nationaldefensemagazine.org/articles/2019/9/16/what-to-expect-from-sixth-gen-aircraft

[5] Tate Nurkin and Julia Siegel, "Battlefield Applications for Human-Machine Teaming: Demonstrating Value, Experimenting with New Capabilities, and Accelerating Adoption," *Atlantic Council Report,* August 2023, Page 2.

[6] NATO Allied Command for Transformation, "Multi-Domain Operations Conference—What We are Learning, 08 Apr 2022, https://www.act.nato.int/article/multi-domains-operations-conference-what-we-are-learning/

[7] Colonel Thomas Schroll, GE AF, "Enhancing NATO Air and Space Power in an Age of Global Competition," *The Journal of the JAPCC,* Edition 35, Winter 2022/2023, Page 80.

But in most NATO ISR operations, there is a second level of exploitation—a team of intelligence analysts receiving that ISR data in real-time or near-real-time and fusing multiple streams of data from multiple sources to provide a more detailed and actionable intelligence assessment of potential targets, threats, and other entities in the battlespace. This analysis and production of intelligence products would likely be part of a "Federated" Processing, Exploitation, and Dissemination (PED) operation whereby any of the PED cells allocated to the NATO Joint Task Force (JTF) by member nations can be tasked to exploit data from any ISR sensor—regardless of nation or domain.[8] And beyond the intelligence assessment, the data would move downstream to drive a targeting decision, and then provide operational and tactical Command and Control (C2) guidance to the tactical units that will ultimately act on the decision—whether it is to engage with weapons, non-kinetic action, or continued ISR collection.

The ability to exploit the data from any sensor—in any domain—and drive a joint targeting decision at the operational level, is at the heart of the Joint All-Domain Command and Control (JADC2) problem. And while the technical means to collect and distribute that data is one aspect of the problem, the deployment and employment of a ready C2 team proficient in the Tactics, Techniques, and Procedures (TTPs) to conduct rapid targeting is perhaps a more significant aspect. NATO expects this problem to be solved by the nations. It expects that contributing nations will provide C2ISR personnel who are trained by the nations—in accordance with NATO standards—who are ready to commence operations on the first day they are tasked.[9]

While there have been a number of NATO Standardization Agreements on C2ISR training tasks and standards—and in stark contrast to other training problems such as that for aircrew or ground forces training—there is no standard NATO or member nation JADC2-oriented training capability identified to achieve this state of readiness. In fact, across the Alliance, C2ISR training is characterized by a lack of any dedicated training capability at all.

1.3 Intelligence Exploitation and the Need for Data

A fundamental premise of NATO operations is that forces contributed by member nations comply with the agreed-upon NATO standards and that those forces will not require extensive support, training, or other enablers to carry out their assigned missions. And to a point, the NATO allies have been successful at contributing trained intelligence analysts, targeteers, and planners to NATO operations—either in the form of augmenting personnel for NATO headquarters and command centers, or entire C2ISR units allocated to NATO operations. In the cases of NATO combat operations in the last twenty years—from Kosovo, to Libya, to Afghanistan—NATO targeting has been sufficiently effective to achieve operational and tactical objectives. The tactical success of the operations being the main evidence.

However there continues to be gaps in C2ISR manning and skill sets. For example, during Operational Allied Force in Kosovo, it typically took the joint team 3-4 hours to prosecute a target from initial detection to weapons delivery—due to both a slow target identification and approval process as well as a lack of proficiency in the coalition targeting process. As noted by a RAND study after the conflict, "One realization driven home by these and other shortcomings was the need for planners in the targeting cell to train together routinely in peacetime before a contingency requires them to react at peak efficiency from the very start."[10]

Thirteen years later, during Operation Unified Protector, challenges remained. Participants in that operation noted that to carry effective targeting inside the Combined Air and Space Operations Center (CAOC) in Italy—a C2 center intended to provide a standing capability to conduct operations—required "…major augmentation of US personnel—specifically targeting specialists…"[11] Another participant observed that NATO personnel

[8] R. D. Thiele, "Towards integrated C4I—NATO experience in building C4I systems," *ISPSW Strategy Series: Focus on Defense and International Security,* Issue No. 531, Jan 2018, Page 7.

[9] Major A. Haider et. al., *NATO / Multinational Joint Intelligence, Surveillance, and Reconnaissance Unit: A Feasibility Study,* The Joint Air Power Competency Centre, October 2015, Page 48.

[10] Benjamin S. Lambeth, *NATO's Air War for Kosovo: A Strategic and Operational Assessment,* RAND, 2001

[11] Joint and Coalition Operational Analysis, *Libya: Operation Odyssey Dawn (OOD): A Case Study in Command and Control,* Suffolk, VA, 4 October 2011

working the CAOC targeting functions "…had no experience, training, or qualifications to do so."[12]

To provide additional intelligence, analysis, and targeting expertise to member nations, NATO has set up training courses at different venues. These courses, such as the N2-02 NATO Intelligence Course, or the N3-17 NATO Joint Targeting Staff Course—both at the NATO School in Oberammergau, Germany—provide a combination of classroom and simulation-based training to develop core intelligence skills. However, courses like this are limited in scope, duration, and capacity (courses are typically one week long), and cannot provide the entirety of skills need, knowledge, and experience for an individual analyst or targeteer to function effectively at a NATO-supporting intelligence or C2 center. That burden still falls on the member nations.

Within those member nations, skills development for intelligence analysis and targeting to support tactical operations is still done mostly via on-the-job training—even for those nations with the largest intelligence enterprises. For example, in the US, despite an extensive course at the Intelligence Technical school to provide the initial intelligence skill set, the United States Air Force (USAF) relies extensively on On-the-Job Training (OJT) to bring an analyst student from apprentice status to full qualification. Likewise, inexperienced analysts have very few opportunities to participate in Large Force Exercises (LFEs) to gain the experience needed.

To further examine the USAF as an example, there are 22 intelligence positions in a USAF Distributed Common Ground Station (DCGS), each with their own position-specific training tasks applicable across the entire spectrum of conflict. But since the USAF or NATO as a whole lacks an intelligence-dedicated mission training simulator akin to aircrew simulators for all airborne platforms, there is no specific technology dedicated to training each of those 22 positions.

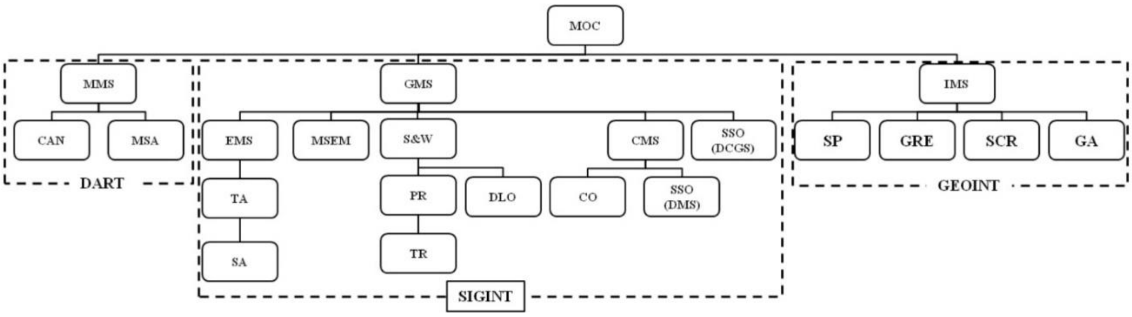


Figure 1: USAF DCGS Intelligence Crew Positions[13]

Considering the breadth and depth of the NATO Coalition ISR enterprise, and the current distributed nature of NATO ISR, creating new stand-alone training solution is not the answer. The USAF alone has 27 DCGSs and over 5,000 analysts assigned to them. The embedded and institutionalized nature of OJT would also make it difficult to change to a completely different approach to operational training.

1.4 Simulation Complexity to Drive C2ISR Processes

Assuming an M&S toolset is able to generate the C2ISR data needed to enable training and concept development in peer scenarios, the red and blue force entities in a simulation must behave in a highly complex and realistic manner. This has been a significant gap of M&S tools in the past.[14] Simulation entities must possess of number of capabilities to achieve the needed level of complexity:

- Qualitatively-valid and doctrinally-correct behaviors as judged by Subject Matter Experts (SMEs)
- Ease of constructing behaviors by non-technical personnel
- Ability to increase number of entities as needed to represent large-scale operations
- Automation of entity behavior to obviate the need for "white cell" personnel to control the scenario

[12] Major J. R. Greenleaf, "The Air War in Libya," *Air & Space Power Journal,* March-April 2013, Page 54.

[13] Air Force ISR Agency Instruction 14-153 Volume 3, 05 Feb 2014, Page 23.

[14] Brian Hart et. al., "Dante Agent Architecture for Force-on-Force Wargame Simulation and Training," Sandia National Laboratories, Albuquerque, NM, 2017.

In short, what is missing from current battlespace simulations is the modeling of the weapons system operators inside the platforms. This lack of human modeling limits the realism of battlespace simulations. Platform operators communicate with each other in natural language, learn through experience to perform tasks more quickly with less conscious effort, and aren't limited to decisions based on scripted behaviors. It has been convention to exclude these kinds of details in simulations as the computational power was barely adequate to model the physical behaviors of platforms, weapons, and sensors—let alone the decision-making process of platform operators—was often not available. However, now that Artificial Intelligence (AI) is improving, so are the prospects for the rise of more realistic intelligent agents that leverage AI technology. What is needed are M&S tools that use intelligent synthetic agents having operator tactical characteristics (anthropomorphic) that can take the place of real operators to facilitate training and analysis.[15]

1.5 The Limitations of Live Training

The needed complexity and scale for MDO is difficult to achieve in the real world. An expected large force, peer military conflict would involve thousands of tactical military units across all domains. It would involve not only the use of highly destructive weapons, but also involve electronic warfare, communications spoofing and jamming, deception tactics, contested logistics, long range fires, gaps in intelligence, collateral damage concerns, and highly complex and fragile command and control systems. These types of operations would extend for days, weeks, and months, through all types of weather and across all types of terrain. These types of conditions are very difficult to replicate on live ranges.

Add to that the cost and difficulty assembling large live forces in one location, the limitations of ranges in terms of size and content, and the need to avoid unnecessary risk during training, and the prospect of achieving the needed level of scale and fidelity via live training operations to prepare for peer conflicts becomes all but impossible. This type of training can only be achieved through a Live-Virtual-Constructive (LVC) approach.[16] M&S tools must therefore enable data immersion, red force realism, and represent the true size, scope, and scale of anticipated peer operations.

2.0 M&S CAPABILITIES FOR THE PEER THREAT TRAINING CHALLENGE

Since 2016, CAE has been developing a data-centric virtual environment to enable training to the peer threat for C2ISR operators. We have tested and refined this capability in testing environments such as the NATO Coalition Warrior Interoperability Exercises (CWIX). The toolset, known as the Virtual ISR Training Application (VISTA) can create essentially any C2ISR platform in the virtual space in any domain. High-fidelity, high-resolution models of virtual sensors can be attached to those platforms, as well as emitters, radios, and weapons, which synthetically generate the same type of data that would be coming from live ISR assets if there was an actual operation. Data can be streamed onto operational networks, stimulate the targeting processes, along with the software tools, to allow C2ISR operators to do their jobs as if they were in a live operations in peer threat environment. This means they can create whatever scenarios and threats they want and present a level of complexity that is hard to achieve through any type of live training.

VISTA also incorporates an approach to AI-driven scenario development named Joint All-Domain AI (JAD-AI). Through the use of this generative AI framework, powered by behavior graphs and deep reinforcement learning, VISTA is able to add highly-complex, doctrinally correct, behaviors to both blue and red forces in the simulation. This combines the data immersion of synthetic C2ISR data with the complexity of scenarios needed to stimulate operational activity to train for the peer threat. Figure 2 below provides an operational view of the VISTA concept.

[15] Brian Mills and Robert Ducharme, "High-Level Orders for Intelligent Agents to Rapidly Generate a Realistic Battlespace," *I/ITSEC 2022 Paper No. 22351.*

[16] Stacey Geiger, "AFRL Demonstrates LVC Capabilities During Red Flag Rescue Visit," 88th Air Base Wing Public Affairs, 05 Dec 2019, https://www.wpafb.af.mil/News/Article-Display/Article/2031849/afrl-demonstrates-lvc-capabilities-during-red-flag-rescue-visit/

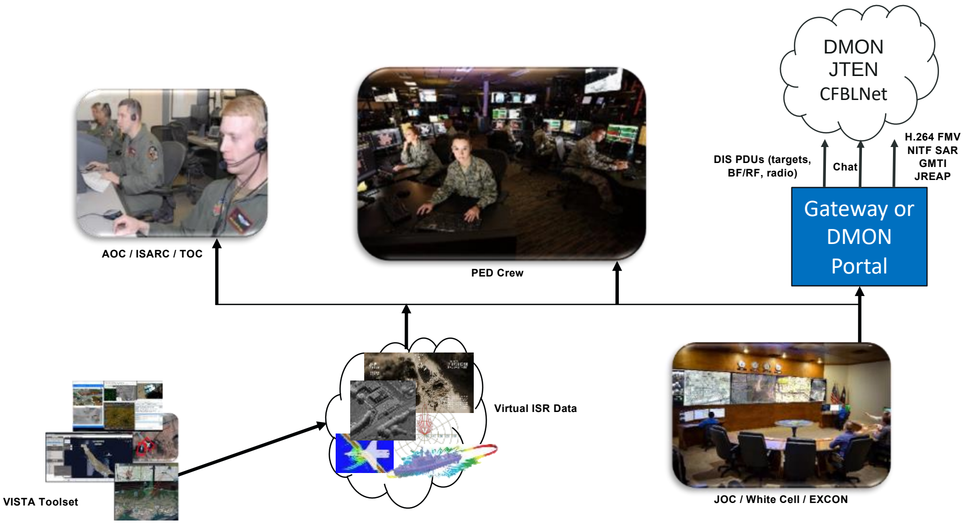


Figure 2: Operational View of the Virtual C2ISR Training Concept

2.1 Synthetic Data for C2ISR Immersion

The CAE team had significant virtual training capability available to address the problem. Over the years, large investments have been made in developing high-fidelity ISR sensor simulation capability as part of aircraft tactical flight and mission training. The MQ-9 Mission Training System (MTS) is a primary example.

In the MQ-9 cockpit, the Pilot and the Sensor Operator must work together to not only manoeuvre and position the aircraft, but to employ the sensors on board the aircraft to achieve the desired effects and collect the required ISR data. Typical MQ-9 sensor flown by NATO members include Electro-Optical, Infrared (both near- and short-wave), low light, Synthetic Aperture Radar, Ground Moving Target Indication, and even some signals intelligence. To effectively employ these sensors, the Sensor Operator of the MQ-9 must be able to train to full manual control of each sensor and be able to maximize the quality of ISR data. To replicate that, it was necessary to develop a series of high-fidelity sensor simulation modules to incorporate them into the MQ-9 mission simulation. Figure 3 below provides some examples.[17]

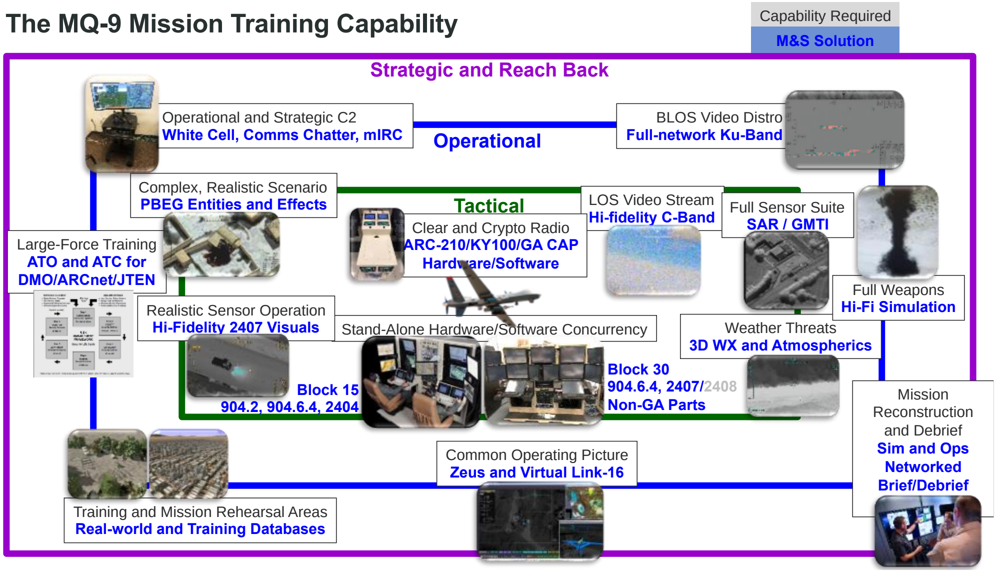


Figure 3: M&S Capability to Leverage from the MQ-9 Mission Training System

In addition to the sensor models, CAE also drew upon both internally-developed and commercially available tools to create both the physics based virtual environment for tactical training events, but the joint and coalition forces as

[17] Matt Martin, "Fake Data—Real Operations," *MODSIM World 2022,* Page 4.

well as the targets that could be represented in simulations. The idea was to enable ISR instructors to create the same dynamic scenarios—to be scripted ahead of time or adjusted dynamically in real time—that aircrew have taken for granted for many years. Rather than be dependent on live mission data flowing into their network from live ISR collection platforms—and therefore being limited to the missions those assets happen to be flying—C2ISR students and instructors should be able to create their own complex scenarios to meet their own training objectives.

To do this, the CAE team incorporated existing imagery/scene generation tools as wells as a Semi-Automated Forces system capability of creating whatever ISR collection platforms, red and blue forces, targets, weather conditions, and terrain needed for any training scenario. This technology also provides a high level of terrain and atmospheric fidelity so that Infrared, Synthetic-Aperture Radar (SAR), and highly level imagery would appear correct and realistic so that students can train to target recognition and analysis as they would with live imagery.

2.2 Streaming Data from C2ISR Sensors

To capture the full range of NATO operations and produce constructive representations of possible C2ISR assets that could become part of NATO operations, it was necessary to identify all needed STANAG-compliant data types and add them as VISTA sensor models. VISTA is able to represent up to 6 ISR assets with imagery streams, of Full Motion Video (FMV), still imagery, and SAR images. VISTA is also able to create up to 6 ISR platforms producing Electronic Intelligence (ELINT) data, GMTI, and JREAP targeting messages. The key to the simulation is in the sensor models. Different kinds of sensors require dramatically different models and the data must comply with NATO standards (Standardization Agreements – STANAGs) for format and presentation. For example, video sensors, be they sensitive to visible or infrared energy, must comply with NATO STANAG 4609. While these STANAGs often refer to legacy capabilities, future XML versions of the data formats using common data elements may be developed and can then be incorporated into synthetic data production.

A number of sensors provide data in a streaming format. That defines sensors that have no defined end to the data. The data can continue as long as the sensor is operating. Streaming sensors have different data formats based on the nature of the sensor. Some sensors use a framing format, often due to the volume of the data collected in a short period of time or other system limitations. Images from the U-2 and satellites, for example are produced in a frame. In addition, MASINT sensors also produce frames due to the restricted bandwidth of the connectivity links. Framing sensors produce images in STANAG 4545 format. Formats are as follows:

1. Full Motion Video: These sensors produce data in accordance with STANAG 4609, which is based on the commercial digital video standards with enhanced metadata to meet military requirements.

2. Ground Moving Target Indications: GMTI data is produced usually by radar systems, but in a few cases, optical systems have been adapted to produce the GMTI information. The output stream is formatted in accordance with STANAG 4607. If the data is processed into tracking data with tracks for discrete targets, the ISR ground tracking data is in accordance with STANAG 4676.

3. LINK-16 targets: Air data is generally passed between aircraft and the ground, as well as aircraft to aircraft using STANAG 5516. This data includes many different operational messages, but air tracking is one of the many messages and is used for many purposes.

4. GMTI: GMTI sensors produce detections of moving objects on the surface and output a stream of “dots” – individual target detections in the form of metadata including the location, radial velocity return signal strength, and with some sensors additional information such as double doppler as received from tracked vehicles, or high doppler such as would be received from helicopter rotor blades. The data should conform to STANAG 4607, and for sensors that process the data beyond basic detections, JREAP messages.

5. ELINT: Signals intelligence sensor detections are distributed using LINK-16 messages, but the current concept for cooperative SIGINT collection is called Cooperative Electronic Support Measures (ESM) Operations (CESMO). This involves the sensor data from multiple sensors being collected in a single processor which uses the multiple lines of bearing to refine the error ellipses associated with SIGINT detections to much greater precision. This data is also disseminated and uses STANAG 4658. (Note that the single processing node can easily be shifted from node to node within the SIGINT network.)

2.3 Intelligent Agents for Complex Entity Behavior

Our approach to AI is a *hybrid* one for Intelligent Agents based on the Kahneman Decision Making Model.[18] In this model, decision making is broken down into *System-1* and *System-2* thinking. System-1 thinking represents the fast brain which uses associative thinking based on experience and intuition. Driving a car, catching a ball, and making a gut decision all use System-1 thinking, and are based on repeated training, association, or heuristics. We can think of System-1 as being roughly analogous to how Machine Learning (ML) models operate and arrive at decisions. In contrast, System-2 thinking represents the slow brain which relies upon on rules and logic and is comparatively slow and deliberate. Symbolic logic as found in traditional AI is representative of this type of reasoning. By leveraging both systems together, operators can learn new tasks more quickly and offload these learned tasks from the slow brain to the fast brain.

AI in M&S products derive primarily from Kahneman System-2 thinking. This is commonly represented in IAs using rules, scripts, finite-state machines, and behavior graphs that are collectively often regarded as Generative AI (GAI). In such a system, the GAI will communicate with both the M&S models and the simulation environment– first to *model* intelligent (tactical behavior) entities & processes, and then to *play* within a simulated battlespace. The agent receives asynchronous events from entities in the synthetic environment and can query to get additional information necessary to make good decisions based on its training and engagement rules. A suitable battlespace Computer-Generated Forces (GCF) may already exist, and the GAI system will need to connect with it through an Application Programming Interface (API). The GAI communicates with the M&S system through analogous means. Open Standards make interfacing tasks relatively straightforward for experienced teams once a set of common semantics between M&S/CGF, GAI and models is agreed upon.

2.4 AI and the Modeling of Entities within Scenarios

A common approach to creating entity behaviors in simulations is that they typically don't model platform operators as separate and distinct entities from the platforms they control. Also, they typically lack any natural language communication capability which makes intuitive interaction with them difficult.[19] Thus, our approach has led us to modeling the platform operators by using intelligent synthetic agents that are separate from the platforms in the simulation, and that can be directed by issuing them high-level orders with natural language commands as well as military-specific brevity language commands. This research has resulted in the creation of a standalone AI software framework that communicates with battlespace simulations using different GCF tools. This AI software is responsible for modeling the operator decision-making and communication networks that are critical to achieving realism and leaves the battlespace simulations to handle the physics of the platforms and environment.

Thus, our goal is the creation of intelligent synthetic agents using AI to model the operators in the platform. For our purposes, we define AI as the study and design of intelligent agents that can perceive their environment and take autonomous actions. To properly model operators, other disciplines of science have been considered to better understand how they think and make decisions. Additional techniques such as Path Finding, pattern-of-life capture, and tactically-accurate target tracking provide great perception and optimization of the agents.

It was also necessary to give them the ability to communicate with understandable language, including brevity codes or other shorthand. The modeling of operators is the intersection of neuroscience, cognitive science, and AI. This view has defined our approach to the modeling of tactical entities to achieve truly complex and doctrinally-correct red and blue force behaviors for C2ISR.

[18] Daniel Kahneman, *Thinking, Fast and Slow,* Straus & Giroux, New York, NY, 2011.

[19] Brian Mills and Robert Ducharme, "High-Level Orders for Intelligent Agents to Rapidly Generate a Realistic Battlespace," *I/ITSEC 2022 Paper No. 22351, Page 4.*

2.5 Communicating with Intelligent Agents

Intelligent agents require a means of communication that is understandable by the Warfighter to maximize the agent's flexibility and utility. Thus, we have chosen to focus much of our AI efforts on the use of Natural Language Understanding (NLU) in our intelligent agents to give them a means of communicating. By taking this approach, we believe the following can be achieved:

1. Facilitate natural communication between intelligent synthetic agents and Warfighters .
2. Build Command, Control, and Communication (C3) networks within the simulation.
3. Rapidly generate complex, multi-domain scenarios.

Using the hybrid AI, an analyst or C2 operator can send orders to intelligent synthetic operators using tactical language. These orders are processed by an Automated Speech Recognition (ASR) engine where they are broken down into structured language, which flows down a command chain populated by other intelligent agents, who communicate with each other using the same structured language. A simple example is ordering an attack on a portion of an enemy Integrated Air Defense System (IADS). This order is given in layperson language and is directed to the theatre commander "Blue Boss" (Figure 4). The system's ASR engine processes the command and generates the correct structured language which is passed on to the next agent in the command chain. As orders flow down the command chain, each intelligent agent issues orders to a subordinate via structured language. This structured language can be translated back to the correct natural language or brevity language based on the identity of the sender and receiver as well as their location in the command hierarchy.

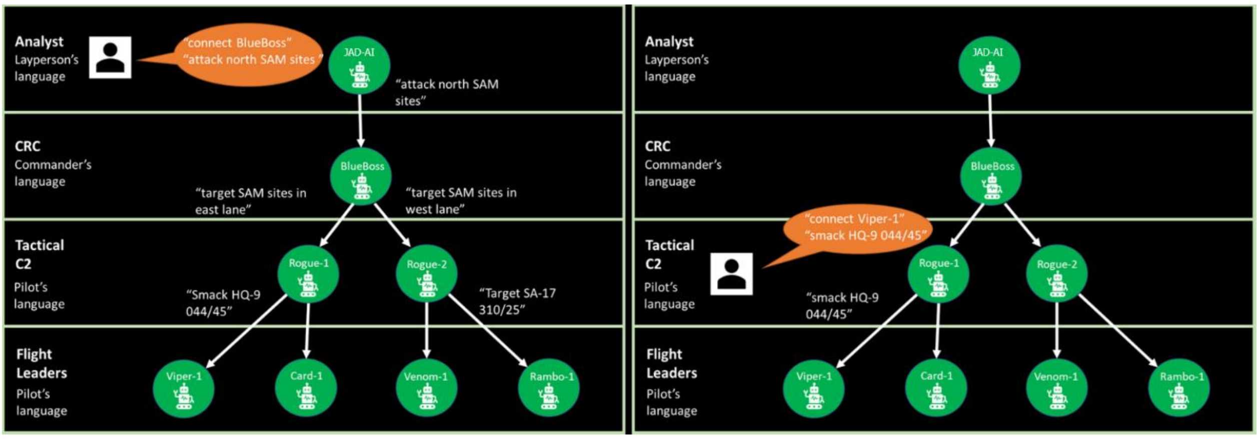


Figure 4: Orders given for a user playing the Analyst compared to a user playing "Rogue 1"

The high-level orders given to the intelligent synthetic agents result in specific tactics being carried out by platforms in the scenario, as well as the generation of scenarios containing formations of synthetic operators (and their platforms) along with their mission objectives. While the initial focus has primarily been in the air-domain, eventually we aim to map the same high-level orders command set across multiple domains and to expand the scenario generation capability, so that an analyst can rapidly generate a realistic scenario in multiple domains and issue the same commands (for example "destroy", "defend") to synthetic pilots as they can to synthetic ground vehicle operators and have the resulting behavior adhere to doctrine while contributing to a desired mission outcome.

2.6 Achieving All-Domain Complexity for C2ISR Training

A number of components are needed to achieve the level of M&S complexity to train to the peer threat:

- High-fidelity M&S environment to create constructive C2ISR platforms
- The ability to generate the entire range of NATO-standard C2ISR data on an operational network
- IAs that model not just the platform behavior but the doctrinally-correct tactical behavior of the operators of those platforms
- Natural-language interaction between the C2ISR training audience and the IAs

This is exemplified by one of our R&D test scenarios. In this case, a hypothetical scenario was constructed containing all the elements of highly contested operational environment between peer red and blue forces. For R&D purposes, all of the elements of both red and blue force Joint Task Forces (JTF) were modeled using publicly-available generic performance data for all the red and blue force platforms (air, ground, space, and maritime platforms, as well as weapons, sensors, and emitters). Red and blue forces were given high-level goals such as "defend the island you occupy" and "remove the adversary from the islands." Goals were further broken down to specific tactical units, such as "defend your airspace sector" for air defense units, or "defend your surface sector" for coastal defense cruise missiles.

But of note in the scenario was the need for different tactical units to share multi-domain data to achieve their goals. For example, in order for the blue force MQ-9 synthetic operator to achieve its goal of "neutralize the coastal defense cruise missiles on this island," it needed to receive targeting data from the blue force ground-based Signals Intelligence (SIGINT) unit on that same island. Which in turn needed to receive higher-level targeting data from the overhead space sensors detecting the missile launches. Likewise, the red force cruise missiles (composed of launchers, radars, and C2 nodes), had to share targeting and C2 guidance data with each other to achieve their goals of "prevent blue force maritime units from reaching the island."

The result is shown in Figure 5 below. The red force cruise missile battery is pursuing its goal of engaging blue force maritime units and producing exploitable signals and behaviors as a result. Meanwhile, the blue force synthetic operators are sharing data between the space platforms, the ground based SIGINT collector, and the MQ-9, to develop and refine a targeting solution against the red force missile launchers. While completely automated, a live player could be inserted as any of the blue force units to achieve their C2ISR training objectives. They would have the benefit of both the synthetic data to stimulate their tactical activity, as well as natural language interaction with the other blue force entities.

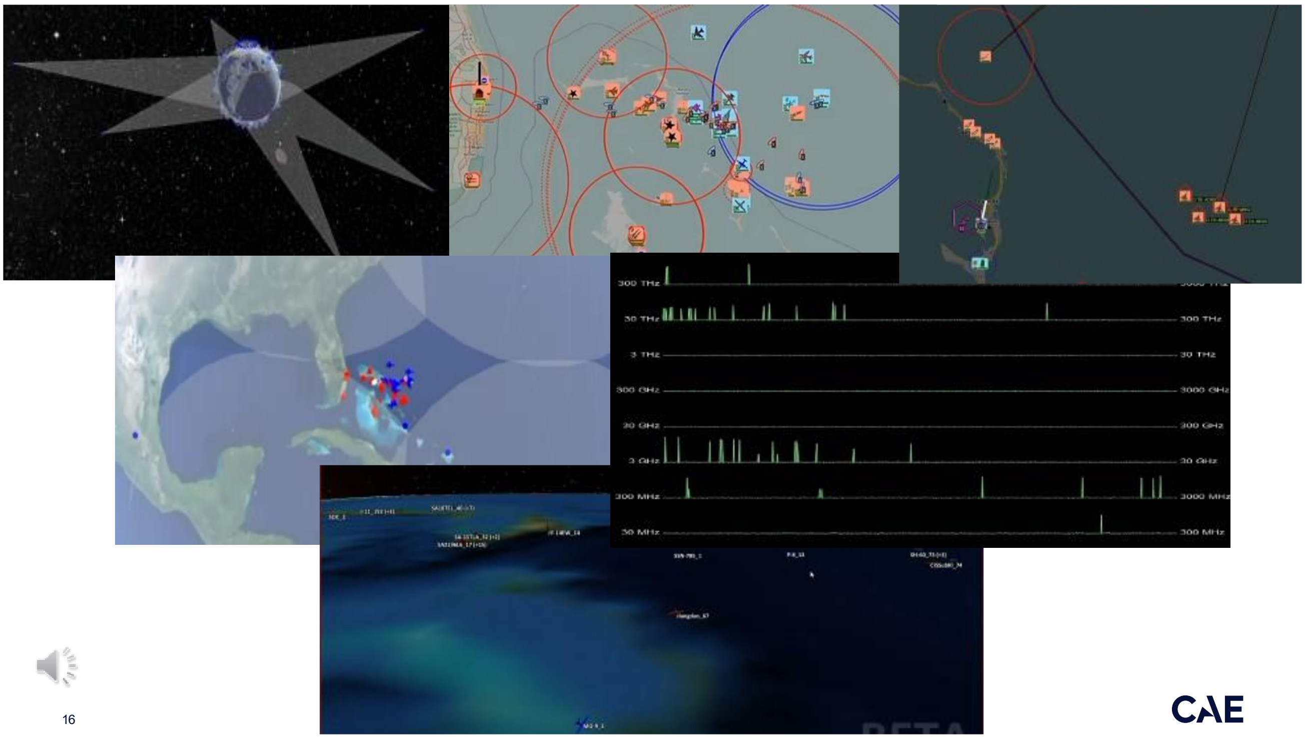


Figure 5: Multi-Domain M&S Scenario Employing Synthetic Data, IAs, and NLP Interaction

3.0 TESTING AND RESULTS IN NATO OPERATIONAL ENVIRONMENTS

The CAE team has been fortunate to conduct testing, data collection, and capability refinement in NATO operational environments such as CWIX 2022 and 2023. The purpose of CWIX is to experiment, explore, examine, and to exercise interoperability through national test programs that have been coordinated between NATO and national C2 capability teams. This testing takes place within the overall context of Federated Mission Networking (FMN), which enables the distribution of C2ISR data and other data streams to various operational military activities such as Processing, Exploitation, and Dissemination (PED) of C2ISR data, multi-domain operational battle tracking, targeting, and operational C2.[20]

Sponsored by the USA national delegation to the CWIX exercise, the CAE team was able to integrate VISTA into various mission threads, such as Joint ISR, Live/Virtual/Constructive, Space, and Data-Centric Security. In 2023 CWIX included participants from every NATO nation plus the non-NATO nations of Sweden, Switzerland, Ukraine, Georgia, Azerbaijan, and the EU. Observers included New Zealand, Columbia, South Korea, Egypt, Moldova, Morocco, Tunisia, and Uzbekistan. There were 956 direct participants, with several hundred observers, visitors, and DVs. The Nations brought a total of 406 capabilities for testing with thousands of test cases and objectives. These cases were divided into 19 different focus areas.

3.1 VISTA Concept of Participation and Test Objectives

In order to provide an operationally relevant data environment, most of the testing took place on a classified network, with test events aligned with a “Joint Vignette”—a simulated scenario that would drive processes such as joint collection management, PED of ISR data, the production of a joint Common Operating Picture (COP), targeting, operational C2, and the coordination of joint fires. CWIX was also timed to coincide with NATO Unified Vision 2023—NATO’s primary ISR exercise. While CWIX had no live assets involved, UV23 had a handful air and maritime assets available. This did provide some live ISR data, but it was a very small amount. VISTA therefore was relied on to provide a significant amount of the data needed for collection management, targeting, and joint fires assessment.

Other LFEs such as the US Bold Quest exercise offer similar opportunities. The Bold Quest series exercises are specifically aimed to demonstrate Joint All-Domain C2 (JADC2) capability, with a focus on achieving data-centricity in the targeting process. According to Stuart Whitehead, Deputy Director-South, US Department of Defense Joint Staff J6 (the sponsors of Bold Quest), through LFEs like Bold Quest stakeholders have: “…learned quite a bit about data centricity through the practical activities…”[21] But it is typically difficult to assemble sufficient live C2ISR assets as such exercises to provide all the needed data to stimulate the targeting process of an entire NATO Joint Task Force.

The scenario-based, synthetic data capability can therefore be a key enabler to the development of JADC2 concepts and provide the C2ISR audience the opportunity to exercise the targeting cycle. For the Bold Quest 21.2 exercise, a VISTA system was brought to the Muscatatuck Urban Training Center, connected to the Bold Quest NATO-SECRET mission network, and configured to provide a number of virtual C2ISR platforms such E-3 AWACS, MQ-9, P-8, and RQ-4. Figure 6 shows the setup of the control terminal.

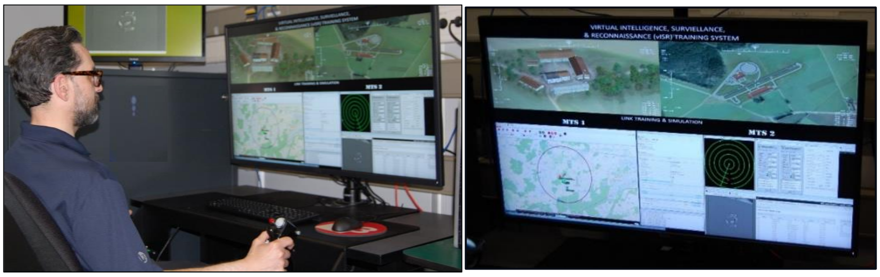

VIRTUAL INTELLIGENCE, SURVEILLANCE, & RECONNAISSANCE (vISR) TRAINING SYSTEM
MTS 1
LINK TRAINING & SIMULATION
MTS 2

Figure 6: VISTA Setup for Large Force Exercises

3.2 C2ISR Performance Improvements

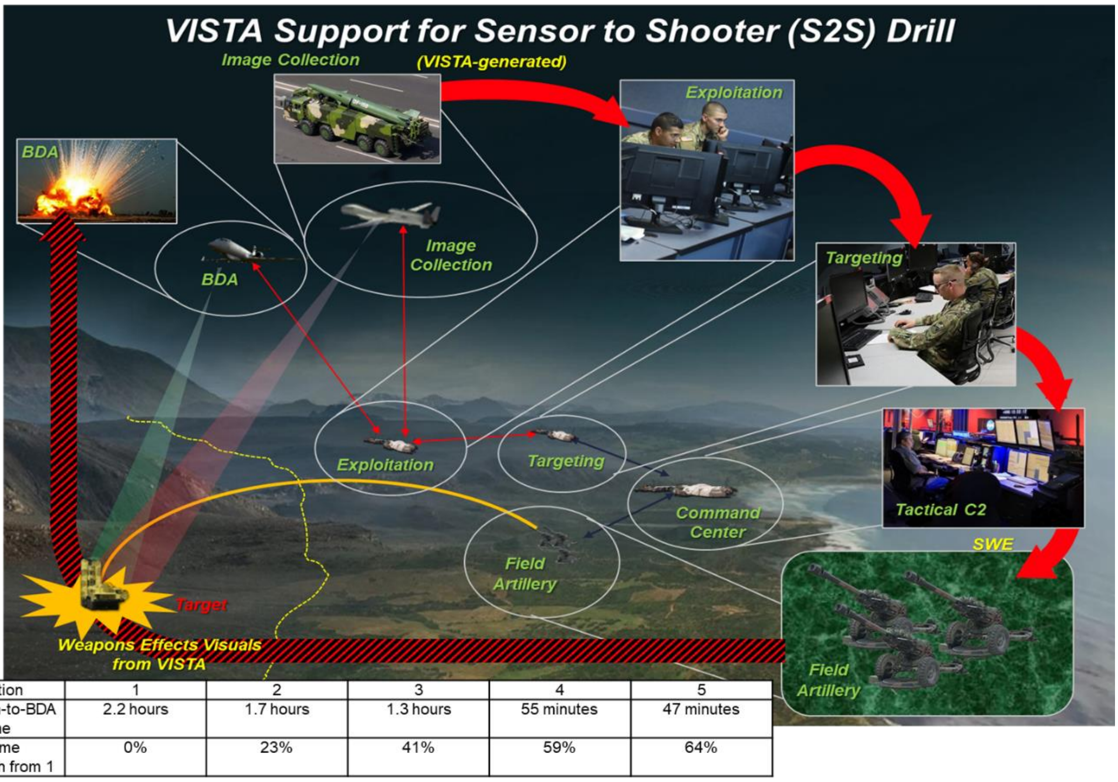
A key series of events in a recent Bold Quest involved a *Sensor-to-Shooter* Drill which ran through the entire targeting process to in order to develop streamlined TTPs for a faster response time. This included the integration of intelligence exploitation, operational targeting and decision-making, providing directions to a tactical layer of C2, cuing a tactical element such as artillery, and finally assessing the effectiveness of the engagement. This full targeting process however requires a number of elements to be conducted live—

[20] NATO CWIX 23 Visitor Flyer

[21] G. Seffers, “It’s Go Time for JADC2,” *SIGNAL*, 27 Oct 2021, https://www.afcea.org/content/it%E2%80%99s-go-time-jadc2

including live shooters and live targets. It also requires the integration of operational-level C2ISR assets to generate the ISR data needed to drive the process.[22] But in the case of Bold Quest, those assets were very limited. It was therefore necessary to generate those assets virtually via VISTA, and create the streaming synthetic data in lieu of live assets. For the LFE drills, the mission network was real. The intelligence exploitation crew, the targeteers, and the tactical C2 element, all consisted of live military players. Even the shooter was real—in the form of live artillery firing on the Muscatatuck range at the directed targets.

But the target, the ISR collection assets, and the data were virtual, generated by VISTA. This included a virtual ISR assets to generate the imagery of the virtual target. Both streaming and framing sensor data, as well as Link-16 and GMTI, were streamed onto the mission network for exploitation and targeting. Ultimately, the live artillery fired at the virtual target imposed on the live range. Then the effects of the target were verified via virtual Battle Damage Assessment (BDA) from those same virtual ISR assets.



Iteration	1	2	3	4	5
Detection-to-BDA Time	2.2 hours	1.7 hours	1.3 hours	55 minutes	47 minutes
% Time Reduction from 1	0%	23%	41%	59%	64%

Figure 7: A Data-Driven LFE Targeting Process

3.3 Synthetic Data Benefits

The most obvious result of VISTA integration in LFEs and the Sensor-to-Shooter drills was the ability to stimulate the entire JTF ISR Collection Management, targeting, and C2 network in absence of sufficient live fly capacity—to include the actual ISR data needed for intel analysts to perform their roles in a complex joint environment. The fact that the data could be streamed to all players with no limitations on capacity further enabled the exercise team to run multiple vignettes and TTPs tests, and ensure that all PED players were sufficiently engaged to gain value from the exercise. Other benefits observed included:

- The ability to change, in real time, the scenario inputs, virtual sensors, Red Force actions, target characteristics, and scenario pacing in a way that would be much more difficult using live assets
- The ability to represent a much larger and more variety Red Force order or battle than would be possible using live Red Force players

[22] C. Thatcher, "Back to Bold Quest," *Canadian Army Today*, 01 Dec 2021, https://canadianarmytoday.com/back-to-bold-quest/

- The ability to show both the positive of negative outcomes of Blue Force targeting decisions
- The ability to provide focused scenario inputs to each component, unit, and even individual to meet their specific training and testing objectives
- Greater situational awareness for the exercise management team to know the difference between “sim truth” and Blue Force perception of the tactical situation
- Integration with all three operational networks used in the exercise (Mission Network, BICES, and CFBLNet) which enabled proliferation of the data for all live players and also into the CSDs
- The potential to conduct distributed LFEs reducing the need for and cost of travel

3.4 Individual and Team Training Benefits

These exercises also demonstrated the potential for individualized intel analyst training when sufficient data capacity is provided. Figure 8 below shows an example of an intelligence product built by one of the analysts participating in the exercise to meet an individual training objective. Other examples include Intelligence Summaries built from multiple VISTA data streams, specific assessments made from VISTA full motion video and SAR images, as well as activity rollups from exploitation for multi-hour activity monitoring using the VISTA-generated virtual MQ-9s.

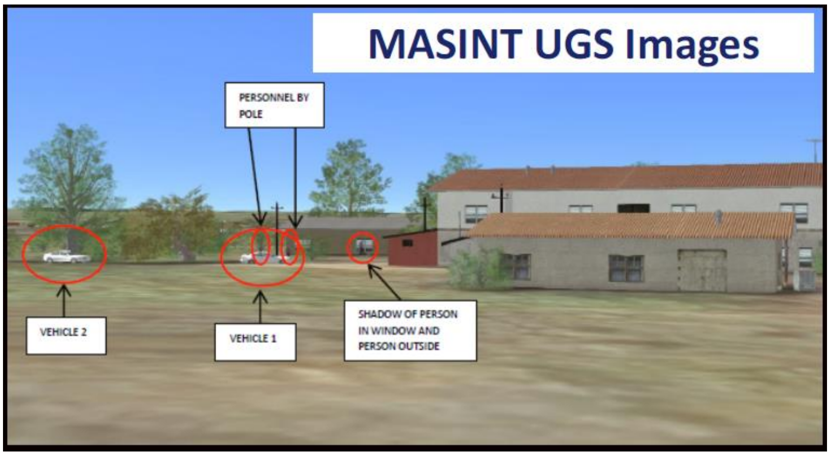


Figure 8: Example Intelligence Product Built for Individual Training Using VISTA data

This type of data-centric approach, with its ability to generate the full spectrum of synthetic C2ISR data and stimulate any needed software tools, provides for any training, mission rehearsal, or operational assessment experience needed by C2ISR operators. A full range of support can be provided for individualized training to meet specific training objectives, through LFE exercises as demonstrated in Bold Quest. Figure 8 above depicts an example individualized training experience for an intelligence analyst student.

4.0 CLOSING

Finally, the CAE VISTA team has also been invited by US Department of Defense Joint Staff to participate in additional LFEs next year. We invite all interested audiences to monitor the progress of these exercises and examine the results for further evidence of the potential for embedded and dedicated synthetic data capability on operational networks for the C2ISR professionals of NATO.