The Heart of Decision Superiority

Evolve or Lose – Why Your Next War May Be Won or Lost in Seconds

By Colonel (ret.) Anthony Bellione, US Air Force

> *'The question is not whether NATO will need to evolve and develop its C4ISR capabilities but whether it can do so in time to meet the gathering threats to the Alliance.'*
>
> General James Cartwright,
> Former Vice Chairman of the Joint Chiefs of Staff

Vignette

Imagine you are a leader in a high-stakes operation where every decision matters and time is of the essence. Your eyes in the sky, a long-endurance RQ4 Unmanned Aerial Vehicle (UAV) meticulously scans the vast battlefield providing real-time, high-resolution imagery while maintaining persistent surveillance. Meanwhile, an Unmanned Underwater Vehicle (UUV) vigilantly patrols beneath the waves. Its advanced sonar, and Artificial Intelligence (AI) algorithms autonomously identify and neutralize treacherous sea mines. Up in the stratosphere, a Zephyr high-altitude platform station maps the ground below, meticulously tracking moving objects and providing unparalleled situational awareness, while small movable CubeSats satellites in low Earth orbit provide remote areas secure 5G internet via ground transceivers, allowing instant communication between soldiers, vehicles, planes, and ships. Close to the ground, the V-BAT Future Tactical Unmanned Aircraft System offers another set of vigilant eyes equipped for persistent aerial reconnaissance for ground combat and special forces teams. Behind the scenes, advanced AI systems process and analyse the avalanche of data from these advanced Intelligence, Surveillance, and Reconnaissance (ISR) systems turning data

into action-able intelligence. At the same time, a multi-domain, battle management network fuses the data and connects the right sensors to the right shooter regardless of the domain. In seconds, the X-47B unmanned combat air vehicle, serving as a loyal wingman to a B-21 bomber on another mission, receives a new tasking derived from the critical information provided by the network – mission accomplished.

What once took days or weeks of meticulous planning is now accomplished in seconds. Each advanced ISR system draws out patterns and offers predictions, cutting through the noise and emphasizing critical information allowing quicker, more precise decisions, and highlights why decision superiority is essential. Achieving military decision superiority relies heavily on the ability to make swift and informed decisions that outmatch those of the enemy. A crucial element in this process is having exceptional ISR capabilities.

Why Decision Superiority?

Decision superiority is achieved when a military force has better situational awareness, a more efficient decision-making process, and greater adaptability allowing for faster decisions than its opponent can react. Decision superiority means military forces own the decision advantage, allowing them to outwit and outmanoeuvre their adversaries and improve battlefield performance. Decision superiority melds advanced technology with cutting-edge sensors, platforms, and communication systems to efficiently collect, process, and precisely transmit data. You achieve decision superiority when you take advantage of superior information and convert it into knowledge that can be acted on by the right decision-makers. However, too much data is a liability too. Militaries that do not learn to integrate and fuse disparate data sources will become victims to information overload, decreasing operational effectiveness. Those who avoid this mistake will successfully prevent disruptions and enhance their mission-critical systems' overall performance.

Advanced ISR systems grant militaries a competitive advantage by enabling a force to outperform its opponents in decision-making by exponentially increasing situational awareness. Cutting-edge air, land, sea, space, and cyberspace ISR systems provide intelligence about an adversary's capabilities and activities, allowing users to prioritize and take prompt action. Advanced surveillance systems, like the NATO AGS (Alliance Ground Surveillance), greatly enhance troop deployment, enemy engagement, and friendly force protection.[1] Military forces can ensure decision superiority by leveraging innovative sensor technologies and embracing advanced Battle Management Command, Control, Communications, and Intelligence (BMC3I) concepts, thereby effectively closing the OODA (Observe, Orient, Decide, Act) loop. This approach significantly enhances multi-domain ISR warfighting and mission success.[2]

Leveraging Advanced ISR

One of the hallmarks of decision superiority is situational awareness and clarity. Decision superiority requires current, accurate information from multiple verified sources, risk-taking, and failure-learning. Commanders must act quickly to seize opportunities and counter threats while being flexible in their plans and decision-making. To stay ahead of an adversary's evolving technology and tactics, ISR systems must be adaptable to add value to the decision-making process.

Advanced ISR systems can enhance freedom of manoeuvre and resource allocation for commanders by providing a comprehensive battlespace understanding. For instance, persistent high-altitude ISR systems, like the RQ4 UAV, operate in potentially hazardous or inaccessible areas enabling the identification and tracking of enemy forces over extended durations. The RQ4 can also evaluate friendly fire efficacy and offers real-time updates to intelligence analysts. For future-minded military organizations, it is crucial to maintain focus on investing in and developing innovative ISR systems. This forward leaning approach will help maintain a decision advantage, improve situational awareness, and enhance operational efficiency.

Leveraging innovations such as a Multi-Domain Command and Control (MDC2) or BMC3I concepts, the alliance can forcefully disrupt adversaries across all domains, creating unrelenting dilemmas and empowering the leadership to dominate the battlespace decisively. Utilizing MDC2, BMC3I, and ISR, the alliance does not just respond to but exploits an adversary's actions. This proactive strategy reshapes the conflict's landscape, putting an alliance firmly in command.

The Kratos XQ-58 Valkyrie UCAV designed by Kratos.

Innovate Training to Win

To effectively adapt to modern warfare and utilize advanced ISR systems, military forces must foster a culture of innovation and invest in comprehensive training programmes. Additionally, military forces must prioritize innovation and calculated risk-taking to adjust to the ever-changing nature of warfare. A culture of innovation means leaders must resource and encourage creative thinking, reward initiative, and provide opportunities for ISR professionals to experiment with new tactics, techniques, and procedures.

By embracing a culture of innovation for ISR, military forces can develop novel approaches to leverage ISR capabilities and outmanoeuvre their adversaries. Instilling a culture of risk-taking also requires risk tolerance, accepting that some actions may not pay off. Calculated risks are a trade-off of risk-reward and avoidance of a catastrophic error. The best way to instil a risk-taking and risk-tolerance culture is to start from the top. Senior leaders must be willing to take risks by creating an environment where forces feel comfortable taking calculated risks, considering the potential for failure. One way to do this is to create a 'learning environment' where everyone is encouraged to learn from mistakes. In such a learning environment, failures should be viewed as opportunities to learn and improve. In support, tailored training programmes are required to educate staff members on the complexities of advanced ISR systems, to learn and master the use, interpretation, and analyses of the vast amounts of data that these systems provide. As US General Stanley McChrystal, former commander of forces in Afghanistan, stated 'Information is only of value if you give it to people who can do something with it'.[3]

Just as computers profoundly impacted our lives, changing how we work, learn, and communicate, ubiquitous advanced ISR systems with the data they provide will change how militaries will fight the next conflict. For advanced ISR systems to be effective, training must include understanding the capabilities

and limitations of integrating data into a comprehensive operational picture. If not, seams and gaps may be exploited by the enemy, reducing, or eliminating the advantage altogether. History is rife with stories of military technology failures.

Learning from ISR History

Early ISR was instrumental in achieving decision superiority in several previous conflicts. During the Battle of Britain in World War II, the United Kingdom's Royal Air Force (RAF) used a network of radar systems called the Chain Home System to detect incoming German aircraft. The RAF's early warning system provided information on enemy aircraft's location and altitude, directing the RAF to effectively deploy their fighter squadrons to intercept and engage the German Luftwaffe. Although the system effectively detected targets during the day, the Germans Luftwaffe shifted to night attacks to minimize losses. The importance of ISR in military conflicts cannot be overstated. By providing commanders with crucial information about the movements of enemies, they gain an unparalleled decision-making advantage over their adversaries.[4]

In 2011, after exhaustive practice and intelligence gathering, the US Naval Special Warfare Development Group, also known as SEAL Team Six, carried out Operation Neptune Spear. ISR played a critical role in the success this operation by aiding in locating Osama bin Laden. The Central Intelligence Agency utilized human intelligence, signals intelligence, and satellite imagery to identify and confirm the presence of bin Laden in a compound in Pakistan, which led to a successful raid. Without sophisticated ISR activities, locating Osama bin Laden and accomplishing a successful mission would have been challenging, if not impossible.[5]

These examples highlight the importance of innovating to maintain a competitive advantage. However, it is essential to note that there is always a potential for unforeseen challenges, limitations, or errors in any

military operation, including those involving ISR, which underscores the reason intelligence methodologies and decision superiority must continue to evolve.

The Limitations of ISR

One of the most significant limitations of ISR is the volume of collected data. Modern ISR sensors can generate huge amounts of data, easily overwhelming collection managers, who must sift through a mountain of information for the most relevant data to meet the commander's needs.

The difficulty of identifying enemy locations in complex environments can be deadly. For example, history has shown that it can be difficult to distinguish between civilians and combatants in urban areas.[6] Civilian casualties during military operations can damage a military's reputation, hinder strategic goals, cause public outrage, damage trust, and lead to instability and insecurity in the region. Management of ISR data is equally tricky. The effective management of ISR data requires a deep understanding of the environment, the enemy, and commanders' priorities, which are critical for operational effectiveness.

ISR Collection Managers are military intelligence professionals responsible for managing ISR data. They ensure that ISR sensors' capabilities are tasked to effectively gather the information commanders need to make decisions. Collection managers must be highly knowledgeable about the environment, the enemy, and the commander's priorities. Additionally, collection managers make demands on scarce ISR resources. The shortcomings of ISR, like outmoded collection or inadequate battle management, can significantly impact the effectiveness of military operations. Armed forces must emphasize resourcing innovative technologies, refining personnel training, and establishing streamlined collection protocols to tackle most inherent limitations.

In the 2011 raid that led to Osama bin Laden's demise, US forces were able to identify his compound using ISR data. However, they were not able to identify the people present at the compound, and some of bin Laden's family members were able to escape.

The 'V-BAT', Tactical UAS, on the hunt. The V-BAT 128 can achieve 90 knots and altitudes of 20,000 feet.

Another instance is the 2014 occupation of Ukraine's Crimea peninsula when Russian forces made extensive use of Electronic Warfare (EW) to disrupt Ukrainian ISR operations. Effective EW made it difficult for the Ukrainian military to collect intelligence on Russian troop movements.[7]

The Future of ISR

One way to overcome data challenges is with AI and Machine Learning (ML). AI and ML technologies allow computers to learn and act without explicit programming. ML is a subset of AI that focuses on using data to train machines to learn how to perform tasks. ISR faces significant challenges due to the mounting volume of data and the growing complexity of the battlespace. To improve the quality of data, collection managers should capitalize on the power of AI and ML. Both AI and ML have the potential to revolutionize ISR by automating tasks, identifying patterns in data, and making predictions that would be difficult or impossible for humans to do. AI and ML technologies will also create new methods for processing and analysing ISR data, allowing commanders to make better decisions faster.

Innovations such as the MDC2 concept, which aims to connect all sensors and shooters across the land, air, sea, space, and cyberspace in real-time, and the related Alliance Future Surveillance and Control (AFSC) programme, which promises to provide real-time situational awareness and targeting information to warfighters, help to create decision superiority. Both MDC2 and AFSC need ISR for better situational awareness to boost operational efficiency and reduce casualties by providing commanders with an improved battlefield picture.

Information sharing is critical for decision-making, especially in complex and contested environments against peer-adversaries. Developers are advancing ISR technology, big data analytics, and cloud computing to combat the increasing complexity of the battlespace, while the Military Internet of Things (MIoT) technologies increase battlespace awareness but complicate information volume and velocity issues by the increased available data.[8] Additionally, electronic warfare

RQ-4D Phoenix NATO Alliance Ground Surveillance (AGS).

and cyber operations could soon incorporate ISR to develop a more comprehensive approach to modern warfare. All of these will enable a military force to disrupt enemy communications and other vital functions.

Military forces can garner more effective decision-making by leveraging advanced ISR capabilities, advanced data analytics tools, and ISR-enabled innovations like MDC2 and AFSC. As ISR capabilities continue to improve, commanders will have access to more and more information. This data deluge can overwhelm antiquated systems. However, bold leaders who invest early will be able to create new opportunities and develop innovative ways to process and prioritize information. However, as much as this concept promises, it does come with some risks.

Risks of AI-enabled ISR

One of the primary risks associated with adopting AI is tainted data and the difficulty in verifying and validating AI systems that learn. 'Bad data' is particularly concerning given that the military's current verification and validation processes may not be suitable for learning-capable AI systems. If tainted data, possibly from adversaries, is used to train such systems, the consequences could be fatal. Another risk associated with using AI in military applications is the lack of trust in and transparency of AI systems. Military personnel must trust the systems they are using to make informed decisions and carry out their duties effectively. To establish trust in AI-powered systems, leaders must have a solid understanding of how these systems reach decision recommendations.[9]

To ensure the prolific use of AI in military applications, it is crucial to establish a comprehensive risk management framework. AI risk management will help identify potential risks and hazards associated with using ISR-enabled AI and allows measures to mitigate them. This framework should include actions to ensure AI systems' reliability, transparency, and security. It should also have processes for verifying and validating systems that learn and measures to protect data from manipulation.

The use of AI by the military presents a range of risks that must be carefully considered and managed.

While AI systems can potentially improve military operations, they also come with their own challenges and risks. For the safe and effective deployment of AI systems within ISR systems, the military must establish a comprehensive risk management framework that deals with possible risks.

Conclusions

To maintain a competitive advantage, military leaders should embrace innovation to achieve and maintain decision superiority on the battlefield. Militaries can gain a competitive edge and enhance their decision-making processes by employing specialized ISR systems like NATO AGS, advanced battle management systems, and AI and ML technologies. However, the use of AI presents a range of risks that must be carefully considered and managed.

Military organizations should prioritize allocating resources to acquire and develop advanced ISR technologies, to include autonomous ISR, battle management systems, advanced data, and analytics tools. Simultaneously, military leaders must foster a culture of innovation, risk-taking, and critical thinking, as well as implement training programmes that emphasize decision-making under pressure. Prioritizing training in critical thinking and adaptability is crucial for success.

1. 'NATO Alliance Ground Surveillance (AGS)'. www.nato.int/cps/en/natohq/topics_48892.htm (accessed 7 July 2023).
2. 'Illuminating the Department of the Air Force Battle Network'. AFCEA International. www.afcea.org/signal-media/technology/illuminating-department-air-force-battle-network (accessed 4 July 2023).
3. 'Leadership Lessons for Health Care from General Stanley McChrystal'. www.ihi.org/communities/blogs/leadership-lessons-for-health-care-from-general-stanley-mcchrystal (accessed 6 July 2023).
4. Buderi, R., 'The invention that changed the world how a small group of radar pioneers won the Second World War and launched a technological revolution'. www.archive.org/details/inventionthatcha00bude (accessed 29 June 2023).
5. 'Operation Neptune Spear: The New Textbook for Special Operators', May 2012. https://nation.time.com/2012/05/02/operation-neptune-spear-the-new-textbook-for-special-operators/ (accessed 7 July 2023).
6. Khan, A., 'Hidden Pentagon Records Reveal Patterns of Failure in Deadly Airstrikes'. The New York Times, December 2021. www.nytimes.com/interactive/2021/12/18/us/airstrikes-pentagon-records-civilian-deaths.html (accessed 29 June 2023).
7. Withington, Dr T., 'Russia's Electronic Warfare Capabilities Have Had Mixed Results Against Ukraine', June 2022. www.thedrive.com/the-war-zone/this-is-whats-happened-so-far-in-ukraines-electronic-warfare-battle (accessed 7 July 2023).
8. Langleite, R. et al., 'Military Applications of Internet of Things: Operational Concerns Explored in Context of a Prototype Wearable', Norwegian Defence Research Establishment (FFI). https://ffipublikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/2993/1948731.pdf?sequence=1&isAllowed=y (accessed 13 July 2023).
9. Button and Robert, W., 'Artificial Intelligence and the Military'. www.rand.org/blog/2017/09/artificial-intelligence-and-the-military.html (accessed 4 July 2023).

ABOUT THE AUTHOR

Colonel (ret.) Anthony Bellione

US Air Force

Colonel (ret.) Bellione is an Intelligence, Surveillance, and Reconnaissance professional with a service record spanning the Navy, Army, and Air Force. His 32-year career culminated in his retirement from the USAF as a Colonel with expertise in Cyber, Intelligence, Aviation, Maintenance, and Unmanned operations. Bellione's assignments took him to Europe, where he forged ties with NATO. He also had the honour of commanding a global Reconnaissance Operations and Maintenance group. His operational experience includes serving in Bosnia (IFOR), Allied Force, OIF, OEF, and OUP. Anthony has experience in strategic planning, security assessments, and critical thinking. His educational foundation includes a bachelor's degree, two master's degrees, and several specialty certifications.