Coming to a Theater near You

Evolving Air Combat to Counter Anti-Access and Area-Denial

Maj Tom "Banger" Lawrence, Royal Canadian Air Force

With a measure of suspense in 2015, the UK completed its Strategic Defense and Security Review (SDSR) and began to signal a broad defense policy shift among Western nations. SDSR was one of the first policies to note a general decline of international cooperation. Coupled with increasingly capable state-based threats, SDSR raised concern for the future of the existing rules-based international order.[1] This signal reverberated within the defense communities of Western nations. Australia published similar conclusions in its 2016 Defense White Paper. Being geographically isolated, Australia fundamentally relies on the international order for its continued security and prosperity.[2] "Strong, Secure, Engaged (SSE)," Canada's Defence Policy, speaks to Canada being a beneficiary of the international rules-based order and acknowledges that such an environment underpins the country's strategic interests. SSE also speaks to the re-emergence of major-power competition and the need to balance the interests of our alliances with the emergence of China.[3] The latest US *National Defense Strategy* prioritizes building the US's military advantage over its explicitly stated rivals of Russia and China.[4] New Zealand has echoed similar conclusions, and the North Atlantic Treaty Organization (NATO) has fallen in step as well, intending to adapt the alliance to address challenges to the rules-based international order and geopolitical competition while monitoring the shift in the global balance of power as a result of China's rise.[5]

China's defense policy, "National Defense in the New Era," denounces the growing threat to global stability. China, however, sees US hegemony as the source of increased competition among states and reproaches NATO for the alliance's increased deployments to Eastern Europe.[6] Lastly, Russia's defense policy warily noted what it saw as the West's destabilization efforts in the Eurasian region and NATO's growing global military capability with its positioning of forces to Russia's near-abroad.[7]

One need not look further for a better example of diplomatic posturing on the international stage. The message communicated is that lines are being drawn, and the stage is being set. As policy guides from above, so commanders below make fast their preparations. The fundamental change in underlying assumptions is that operations are no longer conducted from a position of advantage and may instead be from one of disadvantage. As such, this article will show that for the Royal Canadian Air Force (RCAF) and Western air forces to succeed in a contested operating environment, they must shift to an operational command and control (C2) model that is more resilient, flexible, and capitalizes on emerging technologies. This article focuses on how and why the distribution of control of forces in theater is necessary, and the current and future shifts occurring as autonomous vehicles begin to augment existing force structures.

The Modern Operating Environment

The general trend of economic advancement and diffusion of military technology will increase Western nations' power projection costs and erode the tactical advantage of forces in the field. As some countries acquire advanced military capabilities and the means to control access to their regions, other nations face the dilemma of continual defense investments versus assuring access to the global commons for all.[8]

The major adversaries to the Western powers are both capable and credible within their sphere of influence and in more domains than those occupied by traditional military forces. Encapsulating this idea is the current concept of anti-access/area denial (A2/AD).[9] Simply put, A2/AD means that the act of entry into a theater will be contested, and if successful, the adversary will challenge a friendly force's freedom of movement within. A concept like this should not seem new because it is not. The term does have utility as a rallying point and is a reminder to academics and officers of how war with a major power could appear. After 20 years of low-intensity conflict, a reminder may be sorely needed.

Nontraditional and traditional means of power will be enhanced by real-time, multispectral surveillance. Space-based, cyber, and enhanced conventional weapon systems will challenge the freedom of movement. Machine learning and artificial intelligence will simultaneously stress legacy decision-making structures and empower those with the requisite agility to harness the coming speed of action. Overcoming these challenges in the past required more capable equipment, leading to higher levels of defense spending. For most Western nations, this higher cost has traditionally been offset by a shrinking force structure. This offset has resulted in small, capable, but irreplaceable forces that increased the implicit risk to operations.[10] Additionally, A2/AD increases these risks. In this environment, a further challenge may be to prepare future commanders capable of conducting high-intensity combat operations from a corps that has been accustomed to everything but.[11]

A2/AD signifies an environment where the adversary can employ advanced capabilities on a sufficient scale across the physical and virtual domains and the resiliency to maintain operational effectiveness while suffering attrition. Examples of antiaccess capabilities are cruise and ballistic missiles, surveillance systems (satellites, aircraft, and surface or ship-based radar), antisatellite weapons, submarines, and cyber-attack methods. Examples of area denial capabilities include integrated air defense systems (air and surface-based systems, both fixed and mobile), cruise and ballistic missiles, antiship missiles, antiarmor systems, longer-range man-portable air defense systems, precision-guided munitions, autonomous weapon systems, unmanned aircraft and underwater vehicles, and swarm tactics.[12]

In the Eastern European theater, Russian surface-based weapon systems represent a significant layer of their A2/AD posture. This layer consists primarily of the S-300/400 surface-to-air missiles (SAM), Iskander-M ballistic missiles, and K300P Bastion antiship missiles.[13] Additionally, frontline fighters mainly consisting of Sukhoi Flanker variants present a complementary layer of air defense.

China's A2/AD layers are equally complex. Its air defense is anchored on a network of early warning radars along its coast, complemented with Russian SA-20 and domestically produced CSA-9 surface-to-air missile systems. Further augmenting these SAM systems will be the Russian SA-21 and indigenous HQ-19 systems. The People's Liberation Army Air Force employs a mix of fourth and fifth-generation aircraft and continues to develop longer-range air-to-air missiles.[14] The ability to forward-base these forces on outposts in the South China Sea will further extend China's A2/AD umbrella.[15]

The People's Liberation Army Navy (PLAN) continues to be fundamental to China's A2/AD ambitions. Its efforts to develop a multicarrier navy with modern nuclear-powered submarines and escorts like the Type 055 stealth-guided missile destroyer will allow it to credibly intervene in the South China Sea and project its power beyond the first island chain.[16] Equipped with modern cruise missiles and SAM systems and an increasing ability to sustain operations beyond the first island chain, the PLAN is effectively expanding China's A2/AD eastward while consolidating its strength closer to home.[17]

China fields a wide range of conventional and nuclear-capable ballistic missiles capable of precision strikes versus land targets and surface vessels. Counterspace capabilities include ground-based lasers, orbiting space robots, and antisatellite missiles.[18] The People's Liberation Army cyberwarfare strategy advocates targeting C2 and logistics networks to dissuade military responses to crisis situations and hinder effectiveness from the outset of hostilities.[19]

These developments do not go unnoticed. The Future Air Operating Concept acknowledged the challenge that A2/AD brought to RCAF operations and described the imperative to be able to operate in contested and degraded environments. This challenge means achieving freedom of maneuver in the air domain and across the electromagnetic (EM) spectrum. To meet operational objectives, the RCAF sees low-observability and stand-off weapons and sensors as advantageous qualities to possess.[20]

Countering A2/AD Conceptually: Evolving Doctrine

One concept proposed to address the A2/AD challenge was cross-domain synergy.[21] The idea was not only of fighting jointly but integrating advantageous service-specific capabilities to create windows of superiority in supporting domains and enabling freedom of force movement in another domain. This concept also envisions the integration of capabilities at lower levels to maintain an operational tempo in the face of denied communications and a degraded EM spectrum.[22] An example of this type of integration would be to utilize cyber capabilities to degrade an adversary's air defense systems sufficiently to allow strike and suppression of enemy air defense (SEAD) assets to ingress, destroy their targets, and egress. One challenge of any integration-based concept is having the relevant expertise at the tactical and operational level to plan operations and execute missions. Special capabilities and the reluctance to share technical information between services and nations are not new operational problems and may be aggravated under this concept. These problems are partially mitigated by the participation in recurring multinational air exercises at different tiers of classification and allied information sharing agreements. These agreements cannot be taken for granted though and continued organizational security modernization should be done concurrently.[23]

Another concept to counter A2/AD is the distributed control of operations. Its hypothesis is that the tenet of centralized control and decentralized execution is itself incomplete if applied to a modern A2/AD environment. Recent conflicts that Western nations have been party to have not challenged the resiliency of the information network that underpins much of the C2 capability of its forces. In a major power conflict, offensive cyber and antisatellite attacks may be the primary means of accomplishing this.[24] The threat to forward-deployed air assets from air and missile attacks cannot be discounted either.[25] Therefore, believing that a capable adversary will deny our information sharing networks, control can no longer be rigidly centralized if air forces are to be effective. Authorities and control must at times devolve to ensure continued integration of combat capability and maintain operational tempo. As a result, an isolated combined forces air component commander (CFACC) cannot inhibit lower operations centers and C2 units from assuming control authority to organize, task, and manage combat missions without imperiling operational objectives.[26]

One major difficulty, however, is that forces and combat capabilities tend to be geographically dispersed within a theater to mitigate the risk of loss to forward bases already within an A2/AD environment.[27] Distributed control must be able to join dispersed forces, and the "key to this process is establishing and practicing detailed protocols for when and how to assume control authorities as well as clear guidance as to commander's intent." Cross-domain synergy reiterates the obvious in that advantageous capabilities that reside in other domains must be integrated into the force package where and when they are needed. Cross-domain synergy does not provide the how, which is where the concept of distributed control should fill the gap.

Unfortunately, academic literature on distributed control hesitates to bridge that gap in detail. For example, Larry Broadwell Jr. and Gilmary Hostage III correctly suggest that distributed control could be exercised in degrees. The CFACC or the combined air operations center (CAOC) could reallocate resources from a relatively inactive portion of the theater to more intense areas and delegate authorities for a set period, or subordinate C2 elements could assume additional control activities after a period of lost communications.[28] Generally, these control authorities are already delegated, and the authors only tangentially address the heart of the matter (what they refer to as self-organization). What so few who write on distributed control acknowledge bluntly is its central idea of the transfer of operational control (OPCON) from the CAOC to a lower level. It is the idea that under specific circumstances, the tactical level will assume OPCON over itself and plan and execute on the last-known intent and orders to maintain operational tempo. In other words, keep fighting.

A blend consisting of cross-domain synergy as the solute and distributed control as the solvent may be the conceptual solution to countering A2/AD. United States Air Force (USAF) doctrine seems to be trending in this direction.

> During these operations, forward based airpower can conduct air operations based on a standing "integrated tasking order" (ITO). In this air equivalent of mission command, forward based air expeditionary wings or task forces receive conditions-based authorities with standing orders and commander's intent on the ITO. This empowers subordinate commanders with the flexibility to provide coverage of key defensive counterair combat air patrols (CAPs); air interdiction kill boxes; suppression of enemy air defense CAPs; close air support; or intelligence, surveillance, and reconnaissance in support of surface forces. This decentralized execution model enables local commanders to maintain pressure on the enemy even when disconnected from communications with higher headquarters due to a contested environment against a peer or near-peer adversary.[29]

A new candidate for that solution may be joint all-domain operations (JADO)—an operational statement that discards freedoms and assumptions previously taken for granted. It positions the USAF and willing allies to reimagine C2 to allow for conditions-based authorities supported by broad access to information; converge fires from all domains to achieve mass; emphasize cooperative information sharing on resilient, dispersed networks; automatically synthesize and share intelligence; and to disaggregate and disperse supply to enable resiliency and maintain operational tempo through limited self-sustainment. Given the trends in international relations, the refinement of JADO should proceed with vigor.[30]

Influencing Operations

Several operational factors should be considered when designing a system that would allow the distribution of control (delegation of authority) within an air campaign. Broadly speaking, a survivable C2 network must be established through distribution of tasks, information, and responsibilities. Geographically dividing the joint operating area (JOA) into regions with tactical commanders dual-hatting as regional air component commanders (RACC) may be one method. If so, RACCs must have organic subject-matter expertise and support, limited it may be, to integrate capabilities from other domains to achieve those windows of advantage where they are needed.[31] As a further contingency, control should be distributed to individual squadrons in the event they become isolated from the RACC. By establishing a preplanned system of marshal points and combat air patrol locations with coordination timings throughout the JOA, what emerges may be a crudely effective method of allowing forces to self-organize into strike packages or counterair formations. Lastly, the commander's intent must be drafted in a manner that can be used as a stand-alone by tactical commanders and subordinate units all the way down to individual formations to organize, plan, and execute missions to achieve operational objectives.

The CFACC must clearly define what the transition events to and from distributed control are if C2 systems are denied or become unreliable. This definition includes the loss of satellite communications, cut fiber optic cables, or a cyberattack on communications infrastructure. It could also arise from the retrograde of personnel due to the risk of a strike on the CAOC or its complete loss due to enemy action. An event may also be triggered by allied forces adopting a passive employment/emissions control (EMCON) posture for a predetermined period.[32] Further, a description of the control authority to be delegated, and to whom, should be clear. Consideration should be given to delegating control of missions to airborne early warning assets (preferably fifth-generation platforms such as E-7 Wedgetail), control and reporting centers, or mission commander-qualified aircrew in fifth-generation fighters for *ad hoc* airborne packages.[33]

The CFACC, or the designated airspace control authority should publish a contingency airspace control plan that supports the required operational tempo in a communications-denied environment. A plan of this nature should rely heavily on procedural control and permit the unhindered flow of passive/EMCON assets into, within, and from the JOA.[34]

The CFACC, or the designated area air defense commander, should publish a contingency area air defense plan that supports the identification and engagement requirements in a communications-denied environment with friendly assets operating passively/EMCON. Additionally, the plan should include considerations for additional defensive air patrols if forward deployed assets are destroyed. Complicating this will be the multinational nature of operations, specifically establishing friendly identification criteria that can be met by different aircraft from different countries.[35] Despite the universal recognition of the importance of interoperability, this is an area where willing nations may be denied participation because identification (ID) capabilities have not been modernized.[36]

Rules of engagement (ROE) should always be drafted in such a manner to permit the targeting of adversary forces and infrastructure regardless of the functional status of theater C2. What enables the application of ROE are ID criteria that are practical and balance the risk of fratricide and collateral damage with mission objectives and tactical game plans. ID criteria must be coordinated at all levels to ensure that safe-passage transit corridors, altitudes, and electronic indications of friendly and enemy aircraft used to fulfill the ID matrix are achievable and operationally effective. Exacerbating this issue is the probability of coalition air forces operating passively from time to time.[37] As described previously, what will challenge the coalition force's ability to establish positive ID are participating nations' combat identification system capabilities. Fighter aircraft that do not employ modern cooperative and noncooperative methods of determining positive ID of adversary air, land, and surface weapon systems may be relegated to support rear areas of the JOA.

Effective positive ID criteria will also enable the continuity of dynamic targeting. Such criteria must account for semi and autonomous air vehicle operations, as will be discussed later. To account for periods where reach-back and intratheater support are lacking, target engagement authority should be delegated to the cockpit to the maximum extent practicable, along with acceptable noncombatant casualty values for time-sensitive and high-payoff targets. To ensure the continuity of deliberate targeting, preapproved target folders drawn from the joint integrated prioritized target list should be allocated to different RACCs or squadrons and updated regularly. Achievable intelligence, surveillance, and reconnaissance (ISR) requirements should be articulated to support joint targeting coordination boards at the tactical level. An unhindered target approval mechanism is needed to maintain the required flexibility and tempo for air interdiction and strategic attack missions.

The maintenance of operational tempo, or that of an effective counterpunch, is key. To permit this, a flexible air tasking cycle is required. If operations transition to distributed control, a series of preplanned air tasking orders that cover a set time period could be used. Coupled with last-known mission orders and commander's intent, the isolated force commander can begin to plan, assign, and execute tasks in furtherance of the CFACC's objectives. This method must recognize that the destruction of friendly forces, integral or peripheral to the isolated commander, is a possibility and may impact what is achievable. Isolated regions or forces may find that the day-to-day capabilities for offensive or defensive missions may only be known once assets are airborne and the force package and weapon loads can be determined. Mission commanders should be prepared to rely on the intraflight datalink and standard procedural flow of aircraft within the JOA to coordinate while utilizing standardized tactics, techniques, and procedures to execute missions.[38]

As logistical chains represent high-value targets for the adversary, *in situ* weapon inventory levels at each operating location should be described in terms of operational effects to be achieved.[39] Tactical commanders and logistic officers should maintain war stocks at sufficient levels to achieve their primary mission for a predetermined time period should a reversion to distributed control occur as a result of enemy action. Disaggregating supply, sharing sustainment information, and empowering lower-echelon logistics officers in the same regard as operations officers to adapt and support operational tempo is fundamental to mission success.[40]

Addressing the human element, tactical commanders must be psychologically prepared to rule in favor of military necessity when confronted by concerns of proportionality or collateral damage. Likewise, legal advisors must be professionally prepared to support actions that favor military necessity. Mandatory adherence to a goal of zero civilian casualties is an unacceptable risk to mission success.

Finally, multinational air exercises must continue to evolve and present degraded operating environments to aircrew such as: denied or degraded space-based capabilities such as ISR, satellite communication, global positioning satellite (GPS), and launch detection and tracking; denial of key portions of the EM spectrum; effects resulting from cyberspace attacks; and passive/EMCON employment. Decision-support mechanisms should be degraded to a level where "imperfect knowledge including missing or degraded information, intelligence, and communications capabilities" challenge commanders' decision-making abilities.[41] These air exercises are the only arena where the RCAF Fighter Force can holistically test their combat capability. The RCAF Air Warfare Centre and the Fighter Standards and Evaluation Team, in partnership with the USAF's 561st Weapons Squadron, should further develop and refine tactics, techniques, and procedures for such environments.

Cross-domain synergy and other similarly sounding concepts may be rightly criticized as simply jointness on steroids. Distributed control could be criticized as a modern regurgitation of the concept of tasking by exception,[42] or something that harkens back to the day when the business of war fighting did not have access to the luxury of communications at the speed of light. Some ideas are ahead of their time, such as Gen Merrill A. McPeak's vision of a composite air wing, now practical (ironically requiring fewer types of fighters) with truly multimission aircraft such as the F-22 and F-35.[43] Actually, what lies before us are concepts that have been slowly forged over time. All we must do is decide when to stop folding steel and quench the blade.

Moving from the Conceptual to the Concrete

The targeting of C2 and communications infrastructure of a forward deployed force will isolate and expose it to attack and reduce its operational effectiveness. A2/AD will invite the attrition of friendly weapon systems—systems that cannot be regenerated in a manner achieved in previous major conflicts. While this last point was raised in the discussion of the future operating environment, it should be acknowledged that this implication will be negatively weighted toward the forward deployed force. The solution to these problems for air forces will lie in adopting the conceptual shift described previously, coupled with the fielding of "attritable,"[44] autonomous, combat vehicles. The technology emerging includes unmanned combat air vehicles (UCAV) with advanced communications and information technology, and software algorithms to enable autonomous operations. Complementary to and controlled by manned fighters initially, UCAV usage will mature to fully autonomous operations utilizing swarming-type tactics. In addition to nature, history has shown many examples of swarm tactics employed in the land domain,[45] and thanks to advanced technologies, the exigencies of defense budgets, and supportive policy, its potential in the air domain may be showcased in the next major war.[46]

While the path forward may be classified, the one leading to our present location is unobscured. BAE's Taranis UCAV demonstrator, coupled with Defense Secretary Gavin Williamson's recent announcement in favor of "swarm squadrons of network-enabled drones capable of confusing and overwhelming enemy air defenses,"[47] indicates the British intent. These drones will form a squadron meant to complement and enhance existing F-35 and Typhoon capabilities.[48] After Northrup Grumman developed the X-47B demonstrator for the US Navy (USN), Boeing was awarded a contract under the carrier-based aerial refueling system project to build the MQ-25 Stingray that will give the USN an autonomous, unmanned refueler with an option to develop an ISR capability.[49] The USAF's science and technology strategy includes Skyborg, a recently announced Vanguard research program that will develop an "autonomy-focused. . . low-cost teamed aircraft that can thwart adversaries with quick, decisive actions in contested environments."[50] Under the Air Force Research Laboratory's Low-Cost Attritable Aircraft Technology portfolio, the XQ-58 Valkyrie is in development to meet Skyborg's requirements.[51] The Royal Australian Air Force (RAAF) and Boeing announced in early 2019 the Airpower Teaming system, affectionately referred to as the "loyal wingman" project, to equip the RAAF with low-cost, unmanned fighters.[52]

In the near term, semiautonomous UCAVs will present several benefits and challenges. The political level will be challenged to continue investment in national military capabilities fulfilled with legacy technology. At the strategic level, low-cost, attritable, and easily repairable drones will lower the risk calculus. Previously considered high-risk operations will become tenable, at least for as long as the edge is maintained. Lowering the risk and cost of military operations for Western nations may cause an adversary to lower their estimation of the threshold of war, resulting in a measure of deterrence. Operationally, with UCAVs supplementing the mass of fighter assets in theater, manned fighters could be increasingly dispersed to increase their survivability in the event of hostile action. The replenishment of UCAVs lost in combat could arrive by airlift, thereby quickly regenerating a location's combat capability. Tactically, operations with UCAVs will upend concepts such as an acceptable level of risk, force ratio, and fighter mutual support. Passive, or a blend of active and passive, target engagement offers new shooter-sensor support employment methods. Lastly, combining observable and low-observable platforms into formations will offer new tactical options to flow forces in relation to the threat, sowing doubt and confusion along the way.

Semiautonomy represents only a precursor. Achieving full autonomy will enhance both the benefits and risks. Instead of loyal wingmen, one has loyal swarms. With autonomous, low-observable UCAVs conducting aerial refueling from autonomous, low-observable aerial refuelers, a given theater could be infested with friendly swarms. Initial contested entry operations could task UCAV-only missions to achieve control of the air until the airspace is sanitized of threats. The swarm could then transition to a direct support role, enmeshed with manned fighter operations. An infestation could be easily sequenced, staggering arrivals of UCAVs into theater such that relief sorties could be scheduled in a predictable manner. Unpredictability arising from losses in combat and expended weapon states could be discounted by maintaining a reserve force on ground alert at forward air bases to replenish the swarm where needed. As such, the word infest may find a suitable home in the lexicon of air forces as a tactical condition of the air domain, a task to achieve, and a situation to leverage in the planning and execution of strike, SEAD, close air support, counterair, or countersea missions.

UCAV swarms sharing multispectral sensor information will employ network-enabled weapons capable of being retargeted midflight. Efforts to employ networked weapons collaboratively is another USAF Vanguard project, aptly named Golden Horde. Planned initial demonstrators are the Collaborative Small Diameter Bomb 1 and the Collaborative Miniature Air-Launched Decoy, both modified versions of what is currently in US inventory.[53] With networks able self-organize, converge, act, and disperse as required to achieve their objectives, the doctrine of the BattleSwarm, proposed by John Arquilla and David Ronfeldt, may be coming to a theater near you.[54]

The controlling function of an autonomous swarm would most certainly be given to an advanced algorithm or AI. Vehicle and weapon type, task, target, and threat could be the determining factors in deciding swarm behavior, just as they are determining factors in planning large-force employments of traditional air forces.[55] In the face of A2/AD, overcoming adversary defenses may suggest the use of stand-off weapons and vehicles, ideally networked in such a way as to produce cooperative actions. Arquilla and Ronfeldt refer to this practice as "swarming by fire." In this case, a hive-type mentality, where the swarm is treated as one amorphous body working in concert, may be an appropriate organizational method. An analogy can be drawn from bees, whose omni-directional approach culminates with a singular sting, consuming the life of the bee. This type of approach might be more suitable for expendable, or single-use vehicles. For example, future air-launched decoys could be programmed and employed in a cooperative, responsive manner to confuse, divert, or deceive adversary defenses. The Golden Horde, at least initially, will rely on collaborative behavior or a set of predetermined "plays" decided upon during the mission planning process. A "playbook" will be loaded into the weapons before flight. Once airborne, the optimal play will be selected and executed, as determined by the task and the conditions of the operating environment. "Golden Horde does not use artificial intelligence or machine learning to make determinations independently regarding which targets to strike. The system only selects from set plays and cannot violate defined Rules of Engagement."[56] Even lacking a sophisticated swarm behavior model, a simple linear approach of weapons flying to the target area could achieve the effect of saturating adversary air defenses with the necessary quantity of weapons at their desired points of impact. Where the encirclement of a target or target area may be more appropriate, smaller, microdrones may be the answer. Recently divulged tests with the Perdix system in 2017 saw 103 microdrones launched from pylon-mounted canisters carried by two USN Super Hornets. These microdrones were externally controlled to accomplish basic formations and maneuvers relative to different points on the ground. Target vulnerability analysis, coupled with live destructive testing, computer modeling, and simulation, may offer the capability of using microdrones carrying small quantities of explosives to attack specific adversary systems and their vulnerable points precisely and efficiently.[57]

The long-endurance and low-observable properties of UCAVs make the comparison to the tactical employment of German U-boats a natural one. Instead of a hive approach to organization, the swarm operates under a wolfpack mentality. The pack hunts while dispersed, and the detection of an enemy target triggers the convergence of the pack, or massing of the forces, at the desired target. Here, the low-probability of intercept/low-probability of detection radios, antennae, and waveforms would be of critical importance to incorporate offboard sensor information from other UCAVs and aerospace assets discreetly.[58] Coupled with onboard sensors, the assembly and distribution of battlespace information to network participants would result in offboard targeting information that could support passive weapon employment and passive weapon support. Ideally, the target under attack remains unaware that it is being employed against or from which direction the attack is coming. After the engagement is complete, the pack disperses or reorients itself for follow-on action. Adversary aircraft challenging friendly forces organized in such a manner would be inviting ambush.

Although swarms of UCAVs employing hordes of weapons is a tantalizing, if not dystopian vision, of the future of air combat, the challenges of achieving this capability and its vulnerabilities cannot be discounted. In addition to the possibility of an adversary counterswarm, disrupting the flow of information should be considered the Achilles' heel, whether by an offensive cyber attack, electronic jamming, or deception.[59] The challenges of sharing sensitive information and technology among allies participating in coalition operations is ever-present and may only be compounded by this technology. Allies are not all equal, and this may be yet another fault line. Lastly, ROE may in fact be the most difficult hurdle to overcome. Logical arguments tend to fall flat in the face of collective fear and mistrust toward the idea of autonomous weapons, and only the foolhardy would blindly ignore the risks. Can the current laws of armed conflict support autonomous target identification, classification, and engagement, or do they need to be updated to reflect modern technological capabilities? If they can be applied, are there situations where the state might elect to relax a UCAV's programmed compliance measures in extremis to stave off defeat, or aggressively press a window of opportunity to achieve victory? To what extent must there be man-in-the-loop redundancy? These and other questions must be addressed in such a manner as to not reveal technical capabilities, if possible. Finally, are these technologies yet another case of over-promising and under-delivering, as air forces have often been criticized of? Time, certainly, will tell.

If the efforts to develop autonomous capabilities represent anything, it is the drive to maximize the economies and efficiencies of warfare. Complementing these future trends should be efforts to digitally twin the battlespace. Models that forecast terrestrial and space weather, EM propagation, and GPS accuracy should be integrated with enemy orders of battle, threat libraries complete with technical information, target capabilities, and vulnerabilities. Advanced surface, subsurface, air, and space sensors that can detect, localize, and classify electronic and infrared emissions can be integrated. Layered with blue force systems and capabilities, as well as logistic, supply chain, and force-generation models, the operational level can run AI-powered wargames. We may already be there, and if so, the next question is how to twin the battlespace in real-time such that operational-level commanders can make decisions supported by advice from an AI. Control, it turns out, may be distributed to the machines in the end. If, through our diligence and persistence, we completely digitize the environment of war, the last vestiges of an analog business may be the race to see who activates their system first.

Conclusion

Confronting and prevailing in the face of A2/AD systems requires advancements in doctrine and technology. Officers and politicians must become reacquainted with the probability of effective adversary attacks and the subsequent need of a resilient fighting force. These notions should inform discussions regarding the reorientation of our force structure. Centralized C2, highlighted by the last 20 years of counterinsurgency operations, may be ill-suited against a capable adversary. Distributing control to dispersed forces will cushion any blows, allow for effective responses, and enable the force to employ enhanced survivability tactics. Advanced fighters and UCAVs with advanced communication networks, sensors, and special capabilities will exercise greater lethality concomitant with a greater conditional latitude.

Networked-enabled weapons are here. Semiautonomous UCAVs will arrive shortly and eventually transition to fully autonomous modes of operation. The benefits of this type of weapon will fundamentally alter the risk calculus at all levels of conflict and help to maintain the edge that defends the international rules-based order. The challenges will be protecting the information tethers, overcoming organizational inertia, and gaining legal and social acceptance.

One of the 10 corporate risks identified in the *National Defense Strategic Planning Directive 2020–21* is that the "[Department of National Defense (DND)/ Canadian Armed Forces (CAF)] long term strategy doesn't accurately predict future capability requirements and concepts of operations to posture the CAF to provide required responses."[60] Canada's defense policy has reiterated its continued engagement in international affairs and its support for the international rules-based order. The level of airpower Canada wants to provide to that support is yet to be determined. The trajectory of air combat evidenced by our allies' initiatives may be unpalatable, deemed unaffordable, or assessed unachievable given Canada's byzantine defense procurement process. In any military acquisition, capability signals intent, and with strategic acquisitions such as the Canadian Surface Combatant and the Future Fighter Capability Project yet to be implemented, we would be well-advised to carefully consider the signals we are sending both to our adversaries and our allies. ✪

Maj Tom "Banger" Lawrence, RCAF

Major Lawrence (Advanced Diploma, Sault College; BS, Embry-Riddle Aeronautical University; MDS, Royal Military College of Canada) is a recent graduate of the Joint Command and Staff Program. He has completed the RCAF Fighter Weapons Instructor Course and has flown in Operations Unified Protector, Inherent Resolve, NATO Reassurance, and extensively under North American Aerospace Defense Command. He currently flies the CF-18 Hornet with the 433rd Tactical Fighter Squadron Tactical Fighter Squadron in Bagotville, Quebec.

Notes

1. Office of the Prime Minister of the United Kingdom, *National Security Strategy and Strategic Defence and Security Review 2015* (London: Controller of Her Majesty's Stationery Office, November 2015), 15, 20.

2. Australian Government Department of Defence, *2016 Defence White Paper* (Canberra, AUS: Department of Defence, February 2016), 44.

3. Canada Department of National Defence (DND), *Strong, Secure, Engaged: Canada's Defence Policy* (Ottawa: DND, 2017).

4. James N. Mattis, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Office of the Secretary of Defense (OSD), January 2018), https://dod.defense.gov/.

5. UK Ministry of Defence (MOD), *Strategic Defence Policy Statement* (Wellington, UK: MOD, 2018); and *NATO: Ready for the Future: Adapting the Alliance (2018-2019)* (Brussels: North Atlantic Treaty Organization, 2019), 2.

6. The State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, 2019).

7. Russian Federation, *Russian National Security Strategy* (Moscow: Kremlin, 2015).

8. Royal Canadian Air Force, *Future Concepts Directive Part 2: Future Air Operating Concept* (Ottawa: DND Canada, 2016).

9. "Anti-access—action, activity, or capability, usually long-range, designed to prevent an advancing enemy force from entering an operational area. Also called A2; area denial - action, activity, or capability, usually short-range, designed to limit an enemy force's freedom of action within an operational area. Also called AD." Office of the Chairman of the Joint Chiefs of Staff (CJCS), *DOD Dictionary of Military and Associated Terms* (Washington, DC: CJCS, December 2020).

10. "A further critical issue to consider is the problem of increasingly sophisticated and expensive platforms and the inevitability of attrition. The issue is perhaps most acute with naval and aviation platforms which have become increasingly complicated, have a commensurately lengthy design, testing, and build phases, and require specialized technology (and skills) to operate. As a result, rising costs accompanied by reduced budgets have led many Western militaries to reduce many advanced platforms' overall fleet size. Reduced fleet sizes, however, mean that the loss of a single platform can have serious long-term effects." Department of National Defence, A-FD-005-001/AF-003, *The Future Security Environment 2013-2040* (Ottawa: DND Canada, 2014), 107.

11. UK MOD, *Future Operating Environment 2035* (Wellington, UK: MOD, 14 December 2015), 41–43; and MOD, *Global Strategic Trends: The Future Starts Today,* sixth ed. (Wellington, UK: MOD, 2 October 2018).

12. US Department of Defense (DOD), *Joint Operational Access Concept* (Washington, DC: DOD, 2012), 9–11; and UK MOD, *Future Operating Environment 2035*, 15–16.

13. Ian Williams, "The Russia—NATO A2AD Environment," *Center for Strategic & International Studies*, 3 January 2017, https://missilethreat.csis.org/.

14. OSD, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019* (Washington, DC: OSD, 2 May 2019), 58.

15. OSD, *Annual Report to Congress*, 62.

16. H. I. Sutton, "Chinese Increasing Nuclear Submarine Shipyard Capacity," *United States Naval Institute* (*USNI*) *News*, 12 October 2020, https://news.usni.org; and Andrew Tate, "Chinese

Navy's First Type 055-Class Destroyer Enters Service," *Jane's Defence Weekly*, 13 January 2020, https://customer-janes-com/.

17. Si-Fu Ou, "China's A2AD and Its Geographic Perspective," *Asia-Pacific Research Forum* 60 (2014): 81–124, accessed 8 November 2020, https://www.rchss.sinica.edu/.

18. OSD, *Annual Report to Congress*, 56.

19. "Additionally, targeted information could enable PLA cyber forces to build an operational picture of US defense networks, military disposition, logistics, and related military capabilities that could be exploited prior to or during a crisis." OSD, *Annual Report to Congress*, 64–65.

20. RCAF, "Future Concepts Directive Part 2," 20.

21. "The complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of the others." DOD, *Joint Operational Access Concept*, ii.

22. DOD, *Joint Operational Access Concept*, 16–17. While this concept and its name are continually evolving, the core ideas remain unchanged.

23. CJCS, *Cross-Domain Synergy in Joint Operations: Planner's Guide* (Washington, DC: CJCS, 14 January 2016), 8; and Canada DND, *Pan-Domain Force Employment Concept: Prevailing in an Uncertain World* (Ottawa: DND, 2019), 24.

24. DOD, *Joint Operational Access Concept*, 12–13.

25. "We reviewed a range of unclassified assessments to characterize the contested environment. We identified two broad types of disruptions that would have a major effect on air operations: air and missile attacks on air bases and disruptions to the communications links between Air Force operating locations." Miranda Priebe et al., *Distributed Operations in a Contested Environment: Implications for USAF Force Presentation* (Santa Monica, CA: RAND Corporation, 2019), 5.

26. "If the CFACC becomes isolated, the concept of distributed control empowers subordinate commanders, organizations, operations centers, and battle management command and control (BMC2) platforms to amalgamate otherwise disconnected units into teams of synchronized combat airpower." Larry Broadwell Jr. and Gilmary Hostage III, "Resilient Command and Control: The Need for Distributed Control," *Joint Forces Quarterly* 74 (3rd Quarter, 2014): 38–39, accessed 4 May 2020, https://ndupress.ndu.edu.

27. DOD, *Joint Operational Access Concept*, 20.

28. E.g., battle management C2, control and reporting centers, or airborne early warning and control aircraft.

29. Curtis E. LeMay Center for Doctrine Development and Education (LeMay Center), Annex 3-30: *Command and Control* (Maxwell AFB, AL: LeMay Center, 7 January 2020), 3, https://www.doctrine.af.mil/.

30. LeMay Center, Annex 3-99: *Department of the Air Force in Joint All-Domain Operations* (Maxwell AFB, AL: LeMay Center, 8 October 2020), https://www.doctrine.af.mil/.

31. M. Priebe et al., "Distributed Operations," 50.

32. "The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors; b. mutual interference among friendly systems; and/or c. enemy interference with the ability to execute a military deception plan." CJCS, *DOD Dictionary*.

33. "The Air Operations Directive may include the Joint Force Commander's (JFC) apportionment decision, the Joint Force Air Component Commander's intent, objectives, weight of effort, and other detailed planning guidance that includes priority of joint air support to JFC and

other component operations. . ." CJCS, Joint Publication (JP), *Joint Air Operations* (Washington, DC: CJCS, 25 July 2019), II-3.

34. CJCS, JP 3-30, II-6.

35. The unambiguous resolution of a track's status as either friendly, hostile, or neutral.

36. "Weapons control procedures and airspace control procedures for all air defense weapon systems and forces must be established. . . . Area Air Defense Plan should also be integrated with the Airspace Control Plan to ensure airspace control areas/sectors are synchronized with air defense regions/sectors." CJCS, JP 3-30, II-7.

37. For example, mission-essential equipment in quiet, or silent modes to mask electronic signatures.

38. Charles Bursi, "Centralized Command, Distributed Control, and Decentralized Execution—A Command and Control Solution to US Air Force A2/AD Challenges," (paper, Naval War College, Newport, RI, 28 April 2017), 15–18.

39. For example, sufficient stock of air-to-air missiles, at an assumed probability of kill-level representative of the operational employment method, to destroy 20 percent of the adversary's fighter aircraft; or enough air-to-surface munitions to achieve the desired effects on all regionally assigned targets from the prioritized target list.

40. LeMay Center, Annex 3-99, 23–24.

41. CJCS, *Joint Concept for Entry Operations* (Washington, DC: CJCS, 7 April 2014), 25.

42. "In the 1980s, the United States Air Forces in Europe examined the difficulty of centrally controlling daily combat flying operations during Soviet attack on the NATO command and control infrastructure. As a countermeasure, the directorate charged to find a solution to the problem recommended the issue of mission-type orders to combat wings and daily 'tasking by exception' as long as communications channels remained open. In this way, even if communications were disrupted with one or more wings, the air component commander would know what missions those wings would perform autonomously so he could plan the rest of the flying operation around them." Michael E. Fischer, "Mission-Type Orders in Joint Air Operations: The Empowerment of Air Leadership," (thesis, School of Advanced Airpower Studies, Maxwell, AFB, AL, May 1995), 2–3.

43. James W. Canan, "McPeak's Plan," *Air Force Magazine*, 1 February 1991, https://www.airforcemag.com/.

44. As opposed to expendable which has the characteristic of one-time use, *attritable* implies a design which accepts the probability of being lost in combat, at the same time not assuming every sortie will result in a loss. Further, its destruction may not have a detrimental operational effect, and replenishment may require a low-level of effort.

45. For examples, see Sean J. A. Edwards *Swarming on the Battlefield: Past, Present, and Future* (Santa Monica, CA: RAND Corporation, 2000), accessed 4 May 2020, https://www.rand.org/.

46. "The Department will invest broadly in military application of autonomy, artificial intelligence, and machine learning, including rapid application of commercial breakthroughs, to gain competitive military advantages." Mattis, *2018 National Defense Strategy*, 7.

47. Gavin Williamson "Transforming UK Defence to Meet the Global Threats of Tomorrow," Royal United Services Institute, RUSI Whitehall, London, UK, 11 February 2019, https://rusi.org/.

48. Gareth Jennings and William Lloyd, "RAF announces AEW&C, Space, 'Drone' Test Squadrons," *Jane's Defence Weekly*, 17 July 2019, https://www.janes.com/.

49. Megan Eckstein and Sam LaGrone, "Navy Picks Boeing to Build MQ-25A Stingray Carrier-Based Done," *USNI News*, 30 August 2018, https://news.usni.org/.

50. Air Force Research Laboratory (AFRL) "Skyborg," accessed 4 May 2020, https://afresearchlab.com/; "Skyborg is a vessel for AI technologies that could range from rather simple algorithms to fly the aircraft and control them in airspace to the introduction of more complicated levels of AI to accomplish certain tasks or subtasks of the mission." Bryan Ripple, "Skyborg Program Seeks Industry Input for Artificial Intelligence Initiative," AFRL, 27 March 2019, https://www.af.mil/.

51. Holly Jordan, "AFRL XQ-58A Valkyrie Expands Flight Envelope in Fourth Test," *Air Force Research Laboratory*, 24 January 2020, https://www.wpafb.af.mil/.

52. Gareth Jennings, "Boeing Australia Completes First 'Loyal Wingman' Fuselage," *Jane's Defence Weekly*, 10 February 2020, https://www.janes.com/.

53. Pat Host, "AFA Winter 2020: AFRL Plans Golden Horde Networked Collaborative Weapons Demo in 2020," *Jane's Missiles & Rockets*, 1 March 2020, https://www.janes.com/.

54. John Arquilla and David Ronfeldt, *Swarming & the Future of Conflict* (Santa Monica, CA: RAND Corporation, 2000).

55. Arquilla and Ronfeldt, "Future of Conflict," 22.

56. AFRL, "Golden Horde," accessed 4 May 2020, https://afresearchlab.com/.

57. Aaron Mehta, "Pentagon Launches 103 Unit Drone Swarm," *Defense News*, 10 January 2017, https://www.defensenews.com/.

58. Valerie Insinna, "The Air Force Tested its Advanced Battle Management System. Here's What Worked, and What Didn't," C4ISRNET, 22 January 2020, https://www.c4isrnet.com/. As one of its objectives, the USAF's Advanced Battle Management System seeks to allow platforms from different services to integrate their datalinks with each other and fully share their sensor information.

59. Scott Shane and David E. Sanger, "Drone Crash in Iran Reveals Secret U.S. Surveillance Effort," *New York Times*, 7 December 2011, https://www.nytimes.com/. As was reportedly the case of a US RQ-170 drone commandeered and directed to land in Iran in December of 2011.

60. Canada DND, *Strategic Planning Directive 2020–2021* (Ottawa: DND), 7.