Fifth-generation air warfare

Group Captain Peter Layton, Royal Australian Air Force

The Royal Australian Air Force (and Australia's Navy and Army) is embracing the vision of a fifth-generation future.[1] Originating as a company marketing slogan, the 'fifth generation' expression has evolved into a useful, catch-all term—a simple buzzword—encompassing several important concepts. At its core, 'fifth generation' is about how we conceive waging tomorrow's wars.

Fifth-generation warfare draws on the concepts of John Boyd, a fighter pilot turned strategic thinker, who developed his energy maneuverability theories of dogfighting into the so-called 'OODA loop'. For Boyd, winning at any level of war requires working the 'observation, orientation, decision and action' sequence faster than an adversary. With this, the adversary's reactions to friendly force initiatives will always lag, becoming less and less appropriate to the battle as it evolves.

While seemingly reminiscent of Liddell-Hart, Boyd went beyond such earlier thinking in stressing that the crucial aspect to attaining the requisite superiority in OODA loop speed is rapid orientation. Success lies in building an accurate image of the battlespace more rapidly than the opponent.[2] Situational awareness is the *sine qua non* of victory—a notion military aviators have turned into a mantra.

The process of converting Boyd's 1980s ideas into today's reality has been a somewhat protracted one. This article initially explores the principal approaches on which contemporary fifth-generation air warfare rests, with the second section extending this to discuss some of the practical difficulties in actually implementing this enticing vision. The final section looks at the application of fifth-generation air warfare to battle network and hybrid wars. Together, these two conflict types illuminate some of the

fundamental warfighting issues associated with fifth-generation air warfare.

Fifth-generation air warfare thinking

Fifth-generation air warfare may be considered as comprising four parts: a network, a 'combat cloud' operational concept, a multi-domain focus and a fusion warfare construct. In some respects, the order of these parts reflects the sequence in which they have developed and been incorporated into the overarching fifth-generation idea.

The network

In the fifth-generation air warfare concept, military forces are systems; they are not monolithic entities but are instead composed of many different, interacting parts. This notion of dynamic interaction is key as it means that the system as a whole is more than the sum of its parts. What the system does and how it performs cannot be understood by simply examining each part in isolation. The system can only be comprehended in its totality. This idea has been extended up and down the vertical axis so that complicated organisations like military forces are now seen as being composed of 'systems of systems'. Lower-level systems are embedded within progressively larger systems.

In the age of information technology, the system idea has been made tangible with the building of computer networks of varying scales and intricacy. Originally platform-centric, computing is now network-centric with the worldwide web and countless numbers of intranets and extranets. In the late 1990s, the US armed forces seized upon these developments in information technology, applied them to military operations and popularised the term 'network-centric warfare'.

Today's fifth-generation air warfare concepts incorporate network-centric thinking, with networks seen as comprising four generic elements:[3]

1. **An information grid.** The entry requirement for fifth-generation air warfare is a high-performance information grid. The information grid is a 'network of networks', consisting of communications paths, computational nodes, operating systems and information management applications which enable computing and communications across the battlespace.
2. **A sensing grid.** Sensing grids are composed of individual nodes that scan the battlespace to detect, track and identify targets. The information from the sensing grid is distributed across a force through the connectivity and computing capabilities of the information grid.
3. **An effects grid.** 'Shooters' form the effects grid, engaging targets based on sensor grid information distributed across the communications grid. The 'shooters' aim to create desired effects and can be quite diverse, including manned and unmanned aircraft, surface-to-air missile systems, electronic jammers and cyber systems.
4. **A command grid.** The command grid is principally the province of human decision-makers in involving their perceptions and problem-solving skills. This grid could also include knowledge-based, artificial intelligence software applications that act as command advisers able to recommend courses of actions.

Conceptually, the information, sensing, effect and command virtual grids overlay the operational theatre. The various force elements, from individuals to single platforms to battle groups, are then interacting nodes on the grids; each node can receive, act on, or pass forward data provided from the various grids as appropriate.

The operation of the grids can be visualised using the OODA loop. The sensing grid observes, the information grid orients (through disseminating information), the command grid decides, and the effects grid acts. To achieve a mission, the four grids must all interact and exchange information.

'Combat cloud'

The grid construct is simply an abstraction until turned into a meaningful operational concept. In this, the grid enhances distributed air operations in a particular manner that has been termed the 'combat cloud'.[4] The term derives

from commercially developed 'cloud' computing, where users can exchange information with a virtual cloud, pulling down data and applications as necessary, and adding information others may find useful. A combat cloud created by advanced information technology can bring several tactical benefits.

Firstly, situational awareness is considerably improved. With all aircraft and surface-based systems connected through data-links and able to exchange real-time information, all involved will have the 'big picture'. All involved will know where the hostile aircraft and systems across the battlespace are located, as well as their type and mission profile.

Secondly, the combat cloud makes long-range engagements more practical. Using the data pulled from the combat cloud, friendly aircraft will be able to engage hostile aircraft at extended ranges, well before they near friendly forces, enhancing own force survivability. Greater situational awareness will also allow long-range surprise engagements of hostile aircraft from unexpected directions, allowing friendly forces to gain significant tactical advantages.

Thirdly, with a high-quality distributed air picture, no single aircraft or surface-based system is critical to mission success and so the loss of one input is not catastrophic. The more numerous the aircraft involved, the more detailed, comprehensive and wide-area the air picture developed, and the greater the overall redundancy.

Lastly, the cloud concept allows good use to be made of the different capabilities offered by different platforms. The cloud should be conceived as comprising multiple diverse elements, not simply identical elements; it is heterogeneous not homogeneous. In some respects, the information grid then allows all elements involved to possess the capabilities of all the participants—not just their own individual platform capabilities.

Multi-domain battle

The network-centric idea and the combat cloud construct can be extended beyond the air domain into the other domains of land, sea, air, space and cyber. The resultant multi-domain battle concept then breaks the battlespace up into domains, rather than into Service components as some joint doctrines do.[5]

The key idea animating multi-domain battle is cross-domain synergy; the use of armed force across two or more domains to achieve an operational advantage. The synergy comes when the employment of different domain capabilities produces an effect greater than the sum of their individual effects. Acting in a complementary manner—rather than an additive one—each capability enhances the effectiveness of the whole while lessening the vulnerabilities of each platform individually.[6] Importantly, in using closely synchronised cross-domain synergy, the multi-domain battle concept aims to create and then exploit limited duration windows of opportunity, where friendly forces have the operational advantage and can manoeuvre freely.

In air-land operations in Europe during the Second World War, all sides tried to use air domain forces to pin the enemy down while land domain forces attacked on narrow fronts, aiming to drive deep into hostile territory. Without air domain pressure, an adversary could easily reposition forces to counter the friendly force thrusts but, with air pressure, as soon as adversary forces broke cover and tried to move they became subject to air attack. The enemy was on the horns of a dilemma: remain hidden from air attack and survive but then be destroyed by land attack. The importance of friendly force close synchronisation is manifest.

Fusion warfare

With the creation of large cross-domain networks with diverse sensors, there are concerns that there is now a greater volume of information collected on the battlefield than can be analysed. The solution is seen as fusion warfare. The 'fusion' adjective relates to using improved analytics that fuse data from numerous disparate sensors into a single common picture for decision-makers at the tactical and operational levels of war. The data is not just overlaid but rather carefully combined to give weapons quality tracking information and combat identification—attributes critical to the combat cloud construct.[7]

The fusion process though is just a means to the warfighting end. Future adversaries will also fight using sophisticated multi-domain networks. The fusion warfare idea is to make friendly force decision-making faster so that it stays within the

enemy's OODA loop cycle. In the OODA loop, time is the key variable that determines success or failure. Fusion warfare seeks to compress the time needed to analyse the considerable amount of data continuously collected so friendly forces can have an asymmetric advantage through making well-informed decisions faster.

Fusion warfare allows command and control systems to more effectively manage the increasing volume of information. However, there are growing concerns that adversaries may physically attack the centralised command centres involved or isolate them from the battlefield using cyber and electronic warfare means. The centralised command centre has become a worrying single point of failure.

Fusion warfare offers a partial solution in allowing a move away from the tenet of centralised control and decentralised execution that has long guided air operations. New technologies now make possible a 'centralised command, distributed control, and decentralised execution' construct. Control of air assets could be passed to lower-level commanders as part of making a more agile, flexible and survivable command and control system. Distributed control is seen as allowing collaboration between commanders and operational units in near-real time, leading to a greater focus on solving tactical problems rather than platform tasking.[8]

The fifth-generation air warfare concept involves the combination of network-centric thinking, the combat cloud, multi-domain battle and fusion warfare. As such, this is an intrinsically complicated way of war. Getting the concept to work either in peacetime or operationally is no easy task.

Making fifth-generation air warfare happen

Undertaking fifth-generation air warfare requires moving data around 'system of systems' networks. There are accordingly two crucial elements: data and connectivity. In terms of data, this must be of an adequate quality that decision-makers can use to take action. In terms of connectivity, this must both connect large numbers of diverse nodes and be sufficiently robust to function during stressful military operations. Neither are simple tasks.

Data

Fifth-generation air warfare is data hungry. The 'hunger' of command centres for useful data is readily apparent when considering multi-domain battle and fusion warfare. Less apparent perhaps is that individual fifth-generation air warfare platforms are also heavily data reliant. Major General Jeff Harrigian, when director of the US Air Force's F-35 Integration Office, noted that modern stealth aircraft are 'some of the most data-dependent machines in the US inventory, and require significant amounts of information in order to operate at their best'.[9]

Such aircraft need electronic order of battle data that includes the characteristics and electronic signatures of systems likely to be encountered while on operations. This data is used both to allow mission planning that optimises aircraft survivability, as well as to allow aircraft systems to be able to identify friendly, neutral and adversary systems when airborne.

Without this data, the 'big picture' of the battlespace provided to the aircrew may be inaccurate, incomplete and dangerously misleading. The aircraft can detect targets but, without accurate data, the identity of the targets will remain uncertain, making using beyond-visual range air-to-air missiles risky. If mission data files do not reflect the real world accurately on every sortie, aircrews may launch long-range weapons against incorrectly identified electronic blips, meaning that friendly, neutral or civilian aircraft may be endangered.

Ideally, mission data files should be updated before each sortie to ensure optimum combat effectiveness and aircraft survivability, albeit this is inherently complicated. In broad terms, the process involves extensive support by advanced in-theatre intelligence, surveillance and reconnaissance systems that collect the electronic order of battle data necessary, teams of skilled analysts to make sense of and filter this raw data, unimpeded communication links to carry this information back to the distant software support laboratories, on-call skilled software teams able to quickly translate the evolving tactical circumstances into mission data files and then retransmission to the operational area to load onto each stealth aircraft before every sortie.

Several implications arise from this cycle. Firstly, it is important to have highly specialised electronic data collector systems in-service, albeit these are expensive to acquire and maintain. Secondly, building up a detailed electronic order of battle across a region takes considerable time. Collector systems may be gathering data for years before an operational need arises, as many military emitters may only transmit at rare times for short periods.

Thirdly, the inherent difficulties of collecting data across all potential operational areas suggest that electronic order of battle sharing arrangements with allies takes on a new importance. Fourthly, the faster paced the conflict being waged, the more problematic meeting the mission data file cycle's time updating requirements may become. Lastly, in the most difficult conflicts—those that involve a peer adversary—the whole mission data file cycle may be attacked both physically and virtually.

The problems in the mission data file updating cycle mainly apply to what might be called 'background information' that details the electronic environment within which a military force is operating. There is also another kind of information required. Military command and control systems need to have timely information on the activities within the background environment that friendly, neutral and adversary civil and military entities are undertaking. As noted in multi-domain warfare, this information is needed across the land, sea, air, space and cyber domains.

Unlike parametric data, which might be important at the individual item of equipment level, 'activity information' is most important at the group level. Accordingly, for command and control systems, the information desired is more 'pattern of activity' data. Such activity information might be termed 'foreground data' and, for this, 'big data' is becoming increasingly important.[10]

Big data is defined as 'extremely large data sets that may be analysed computationally to reveal patterns, trends, and associations, especially relating to human behaviour and interactions'.[11] Big data's elements, colloquially termed 'the three Vs', are ever-larger Volumes of data; a growing Variety of sources (old, new and open source) and increasing Velocity with continually greater data flows.

Given these factors, the analytic approach of intelligence organisations has shifted from looking for specific kinds of adversary activity to looking for changes in the normal pattern of activity. The big data analytic approach can be visualised in four phases.

In the initial phase, a high volume and variety of data from multiple diverse sources across time and space is collected, meta-tagged and placed into an information 'cloud'. In the second phase, analysts use software applications to manipulate, visualise and synthesise the data in the cloud, leveraging the relationships between the different data elements.

The third phase involves building situation-specific software tools that can use the filtered pattern data to clarify the kind of activity underway and what this means in terms of future adversary actions. The fourth phase involves a partnership between the data analysts, the collection systems and the operational users. Operational users are no longer just consumers of intelligence information but rather collaborators in its creation.

The concepts of combat cloud, multi-domain warfare and fusion warfare all drive towards being able to make decisions faster than an adversary—to get inside the adversary OODA loop across multiple domains. The big data analytic framework offers a potential way to achieve this.

Connectivity

Without adequate connectivity between the various network nodes, fifth-generation air warfare would fail. Fused sensor information needs to flow at high speed across and between the various platforms and command and control nodes involved, often via intricate communication architectures featuring voice, video, data and imagery transmissions. In this, the key issues are building the network and—given this is a military network—its robustness.

Fifth-generation air warfare requires all the participating nodes to be connected via data-links of varying capacities and capabilities. The archetypal data-link for airborne application is Link 16, fitted to many ADF aircraft, ships and command and control centres. Link 16 has some shortcomings, including in providing only

line-of-sight linkages, and so is used in conjunction with several other types of data-links. The different data-links connect and exchange digital information through optimised gateways, albeit this introduces complications, vulnerabilities and inefficiencies.

Modern stealth aircraft have been developed in a manner that creates data-link connectivity problems. Such aircraft have Link 16 but, when emitting the transmissions, may be detectable by hostile electronic surveillance systems and the aircraft targeted. Accordingly, stealth aircraft use special low probability of intercept (LPI) data-links that, at the moment, are much harder to detect.

These LPI data-links are proprietary systems and cannot link with those used by most other types of aircraft, including other different types of stealth aircraft. To overcome this, special gateways are being developed that can connect the LPI data-links (and other data-link types) to the Link 16 network. In Exercise Jericho Dawn 16-3, undertaken at Puckapunyal in 2016, a gateway hosted on a Grumman Gulfstream business jet successfully linked RAAF fighters, combat support aircraft and Army helicopters.[12]

Sharing data-linked information has some implications during coalition operations. The combat cloud construct involves everybody on the network contributing to the 'big picture' and making tactical decisions based on it. In this, there is an implicit assumption that the picture is accurate. If, however, one nation's forces engage a civilian target because the data provided to the combat cloud by another country's sensors was in error, who is responsible? Will governments be comfortable authorising their nation's forces to launch weapons based on multi-domain network data of uncertain origin and veracity?

The inherently complicated nature of fifth-generation air warfare, with its considerable data processing and information sharing, raises concerns about whether future kill chains can be clear, unambiguous and sovereign. Devising national rules of engagement appropriate to fifth-generation air warfare will present real difficulties.

Fifth-generation air warfare is an enticing vision but its practical implementation is not easy, especially in the face of adversary action. Considerable effort is required to create decision-quality data and then establish the robust connectivity needed to support combat cloud, multi-domain battle and fusion warfare concepts. Making sure that fifth-generation warfare is not overly fragile requires significant preparation before an operation commences, and substantial support during it.

Waging fifth-generation air wars

Fifth-generation air warfare is an operational employment concept rather than a strategy in the conventional understanding. A strategy aims to bring about a particular context-specific political outcome but the fifth-generation air warfare concept is instead a broad, generic 'way of war'. An understanding of its application to wars might be gained by discussing two different conflict types: battle-network wars and hybrid wars.

Battle-network wars

Battle-network wars involve two networks fighting each other.[13] Such wars might occur between near-peer adversaries that both employ advanced information technology and use similar military doctrines. In combat, both sides would try to maintain the integrity of their own network while attacking the hostile one. In this, the focus would not be on simply destroying individual force elements in attrition style battles but rather in attacking the interaction between the network nodes.

The aim would be to disrupt the network on which the adversary relies to wage war through fragmenting it. With mutual support through the network lost, individual hostile force elements could be defeated in detail as necessary. Friendly forces could mass through using the network while adversary forces could not.

One of the first battle networks was the British air defence system that defeated the Luftwaffe in the 1940 Battle of Britain. In retrospect, the Luftwaffe, in trying to gain air superiority to allow a seaborne invasion of Britain, should have concentrated its attack on the Royal Air Force's Chain Home radar stations, the network's sensing grid. Instead, the Luftwaffe attempted

to destroy the much more numerous fighter aircraft, the effects grid, for which the radar warning information was critical. The Luftwaffe focused on destroying platforms, rather than conceptualising the British multi-domain air defences as a network and designing an attack to prevent the interaction between the radars and fighters, and fragment the overall network.

A future air war with both sides using fifth-generation air warfare concepts would see two very complicated, opposing socio-technical structures being directed and fought by military commanders. At the operational level, the battle would probably not involve a series of discrete steps, with large force manoeuvres carefully choreographed and sequenced to progressively lead to the desired outcome. Instead, strategic results would be achieved through the steady accumulation of small tactical successes. The combined effect of these multiple actions occurring in time and space would ultimately fragment and defeat the opposing network.

This high-level outline suggests important considerations for commanders preparing their battle networks for conflict. The networks need to be of a sufficiently large scale appropriate to the commander's plan of attack. They should be designed to operate in a decentralised manner, with no single key node or critical points of failure. Across the envisaged operational area, the networks need to be robust, with an adequate level of redundancy built-in so they can continue functioning while being attacked.

This highlights an intrinsic weakness in that units that transmit as part of a battle network will probably quickly reveal their position to the opposing network, with an attack likely to follow, albeit it may take some time to mount. To counter this, readily deployable air units—able to access numerous permanent and transitory air bases—may be able to employ 'shell game' tactics and be hard to pin down.

Battle networks though are interactive and, as friendly forces take action, so the hostile network will respond. Historical analyses of earlier battle-network wars suggest that the pace of the move-countermove cycle progressively accelerates as each side learns and becomes more effective. Eventually, the pace gets so rapid that one side is either unable to keep up and fails, or instead tries to outflank the adversary attacks by manoeuvring cross domain and forcing the competition into a different regime.

A battle-network war though, as it speeds up, might turn into a war of rapid attrition with the losing side the one that runs out of equipment and skilled people first. Battle-network wars might be attrition 'slugfests'.

There is an even darker future possible. A network-battle war might have two phases. The initial phase might involve a fast and furious exchange of blows that expends the small number of high-technology platforms and systems immediately at hand. The second phase then may involve a drawn-out period of 'broken back' warfare, where warfighting regresses and simpler, more-quickly manufactured weapons are used to continue the clash. During this phase, both sides would be trying to reconstitute their battle-network forces as quickly as they can so as to win the war before the other side can similarly return to full operational capability. Such a battle-network war might be quite protracted and very costly in blood and treasure.

Hybrid wars

There are other types of conflicts that are not characterised by a symmetrical, network-on-network battle. Some of these modes of conflict may be chosen by adversaries so as to limit the effectiveness of the defender's high-technology battle network. One potential mode is hybrid wars.

Hybrid wars are waged using a variety of dissimilar actors: state, non-state, sub-state and highly-motivated individuals. The sensing grids of battle networks are usually designed to detect the signatures of conventional military forces. The grids will accordingly have difficulty discerning the other actors intermingled amongst the society in which the conflict is being waged.

Attributing specific actions to particular actors may become very difficult, inhibiting effective responses. Moreover, the effects grid is also usually designed to engage military units operating away from concentrations from civilians. Hybrid actors, even when detected, may be too close to civilians to be engaged in the manner the defending battle network has been designed for.

In recent years, hybrid wars have been waged using non-state and sub-state actors to quickly seize areas that can then be occupied by conventional military forces able to readily defend them. The advantage of using state and sub-state actors initially is to avoid detection, as battle-network sensing grids are usually looking for conventional military force movements. A prompt response by others is then prevented; they are simply presented with a fait accompli, shifting the onus to fire first onto the defenders.

In a hybrid conflict, the sensing grid would likely need to be restructured to make greater use of non-traditional information resources, such as social media and open sources. The use of non-state and sub-state forces is most likely to be discerned on these first. Broadening the sources in this way plays to a key fifth-generation strength: 'big data'.

As discussed earlier, big data techniques assess large volumes of information flowing at high velocities from various sources—the three 'Vs'—to determine changes in the normal pattern of activity. However, to find these changes, the friendly sensing grid needs to be collecting appropriate background information for a period of time before. In this, the data analytic software and applications in use will also need to be optimised to be able to use the detected changes to forecast the adversary force's future activity.

Hybrid war also impacts the information grid. Non-state and sub-state actors might generally be thought of as possessing inadequate technology or professional skills to exploit or interfere with the communications flowing across the information grid. In hybrid war, however, the state party may well supply its associated non-state and sub-state actors with processed exploited information and, at times, specialist equipment.

Such exploitation, for example, may allow the non-state and sub-state actors to use social media or mobile phones to contact the defending state forces at the individual level to threaten or coerce them immediately before attacks begin. In terms of interference, jammers or cyber assets safe from attack by virtue of being located in the distant homeland might degrade the information grid at critical times. Such interference may be made more effective by providing local non-state and sub-state actors with simple, optimised equipment able to be placed near battle-network nodes.

While there are numerous difficulties in fighting a hybrid war using battle networks, there are some advantages beyond that noted concerning big data. After the initial use of non-state and sub-state actors, the pace of the conflict is likely to slow. The initiative may then pass to the defenders. There may be time to arrange set-piece battles that realise cross-domain synergy and make best use of multi-domain manoeuvre. Multi-domain battle and fusion warfare may be complicated. However, the slower pace of hybrid war may assist making carefully sequenced multi-domain parallel attacks.

There are some further possible advantages. In a hybrid war, an adversary will be aware of the possibility of vertical escalation and will work to keep hidden some information about adversary military forces and, in particular, electronic signatures. Accordingly, friendly force mission data files and electronic order of battle information will probably remain valid significantly longer, easing reconnaissance and software reprogramming tasks. Moreover, non-state and sub-state units may make use of commercial equipment that can be readily jammed, exploited or have false data inserted. There may be significant opportunities for cyber-attacks.

The two different types of war help reveal the complexities in waging fifth-generation air warfare. Its network nature, in particular, influences the manner in which such wars can be undertaken. The symmetrical battle-network war is the most complicated and fastest paced. In contrast, the slower pace of symmetrical hybrid war type might allow friendly fifth-generation air warfare systems to progressively evolve to better meet emerging operational circumstances. This cuts both ways of course. The adversary hybrid forces also then have more time to adapt and introduce effective countermeasures.

Conclusion

From the discussion, it is apparent that the fifth-generation air warfare concept is a complicated one that is both a distinct way of warfighting and noticeably different to traditional approaches. In this, the concept's theory of

victory is clear: operational success is achieved through gaining relative superiority in battlespace understanding through the timely development and sharing of useful information across heterogeneous, geographically dispersed, digital networks.

This theory is unlikely to change. Rather, the fifth-generation air warfare idea is more likely to evolve through technological refinement than major conceptual shifts. In this, there are several caveats that should be borne in mind.

Firstly, the fifth-generation warfare idea relates to what Edward Luttwak termed 'the technical dimension of strategy'.[14] Technology influences how we fight wars, however, there is more to winning than technology. Leading-edge technology was insufficient in itself to prevail in the Vietnam, Iraq and Afghanistan wars—and fifth-generation warfare so far does not appear any different.

Secondly, the article generally neglects software—in terms of the code that makes digital technology function. Suffice to say, software matters make fifth-generation warfare even more complicated, possibly by an order of magnitude.[15]

Thirdly, in being inherently complicated, it may seem that the fifth-generation concept could be incompatible with the nature of war, a social activity dominated by chaos, uncertainty, friction and chance. At least in hybrid wars, it seems these worries are unjustified, if earlier comments about advanced technology being necessary but not in itself sufficient are accepted. Multi-domain battle and other fifth-generation warfare aspects are being combat proven in Iraq in operations against Islamic State.[16]

The concept's appropriateness to near-peer warfare, however, still needs confirmation. A very complicated approach to making war may prove too complicated if opposed by technologies optimised to defeat it. For example, if an adversary can cut most data-links for an extended period, would this invalidate the overall fifth-generation warfare concept?

Lastly, the whole fifth-generation idea rests on trust between all network participants. Within national armed forces, there may be some elements that would rather not share information. Submariners at times are an example of this; they prefer for their vessels to operate alone and not inform others of their presence. Trust also becomes a further issue when conducting coalition operations where concerns range from releasing sensitive tactical information to matters related to defence industrial base issues.

In reality, in most conflicts, the most common situation might be 'balkanised' networks, where some nodes are disregarded leaving others to potentially fight their own separate wars. Such an approach significantly undercuts the logic of fifth-generation warfare.

Fifth-generation warfare usefully integrates network-centric warfare, combat cloud, multi-domain battle and fusion warfare concepts. These are all important ideas that in fifth-generation warfare do not exist individually but rather function together as a 'system of systems', where the whole is greater than the parts. In this, fifth-generation warfare is an evolving way of war; new elements and novel innovations may yet be incorporated. It is an area that remains a work in progress.

Group Captain Peter Layton is a reservist with extensive aviation and defence experience. For his work at the Pentagon on force structure matters, he was awarded the US Secretary of Defense's Exceptional Public Service Medal. He has a doctorate from the University of NSW on grand strategy and has taught on the topic at Eisenhower College at the US National Defense University. For his academic work, he was awarded a Fellowship to the European University Institute. He is a Visiting Fellow at the Griffith Asia Institute at Griffith University.

Notes

1 Brendan Nicholson, 'F-35 will be regional game changer, says RAAF chief', *The Strategist* [website], 12 May 2017, available at <https://www.aspistrategist.org.au/f-35-will-regional-game-changer-says-raaf-chief/> accessed 7 December 2017; Tim Barrett, 'A 5th generation Royal Australian Navy', *The Strategist* [website], 26 November 2015, available at <https://www.aspistrategist.org.au/a-5th-generation-royal-australian-navy/> accessed 7 December 2017; and Brendan Nicholson, 'Angus Campbell: turning a 3rd generation Army into a 5th generation force', *The Strategist* [website], 30 June 2017, available at <https://www.aspistrategist.org.au/angus-campbell-turning-3rd-generation-army-5th-generation-force/> accessed 7 December 2017.

2 David S. Fafok, 'John Boyd and John Warden: airpower's quest for strategic paralysis', in Phillip S. Meilinger (ed.),

The Paths of Heaven: the evolution of airpower theory, Air University Press: Alabama, 1999, pp. 357-98.

3 Peter Layton, *Network-centric warfare: a place in our future?*, Air Power Studies Centre: Fairbairn, 1999.

4 David A. Deptula, *Evolving technologies and warfare in the 21st century: introducing the 'combat cloud'*, Mitchell Institute for Aerospace Studies: Arlington, 2016.

5 Future Joint Force Development, *Cross-domain synergy in joint operations: planners guide*, Department of Defense: Washington DC, 2016.

6 William O. Odom and Christopher D. Hayes, 'Cross-domain synergy: advancing jointness', *Joint Force Quarterly*, Issue 73, April 2014, pp. 123-8.

7 Hawk Carlisle, 'C2 and fusion warfare', *Air Force Association* [website], 2017, available at <http://secure.afa.org/events/AWS/2017/postOrlando/audio/3-2-17-Carlisle.asp> accessed 23 April 2017; and Lani Kass, 'Panel: C2 and fusion threats', *Air Force Association* [website], 2017, available at <http://secure.afa.org/events/AWS/2017/postOrlando/audio/3-2-17-C2Panel.asp> accessed 23 April 2017.

8 David A. Deptula, 'A new era for command and control of aerospace operations', *Air & Space Power Journal*, July-August 2014, pp. 5-16.

9 Jeff Harrigian and Max Marosko, *Fifth generation air combat: maintaining the joint force advantage*, Mitchell Institute for Aerospace Studies: Arlington, 2016.

10 Robert P. Otto, *Data science and the USAF ISR Enterprise*, Department of Defense: Washington DC, 2016; and Nicholas P. Cowan, 'Rethinking command and control of intelligence, surveillance, and reconnaissance', paper presented at the 20th International Command and Control Research and Technology Symposium, July 2015, available at <https://static1.squarespace.com/static/53bad224e4b013a11d687e40/t/55a64e86e4b0e88cf27dcc6d/1436962438969/094.pdf> accessed 23 January 2018.

11 *Oxford English Dictionary*, available at <https://en.oxforddictionaries.com/definition/big_data> accessed 12 December 2017.

12 Lara Seligman, 'Combat cloud', *Aviation Week and Space Technology*, 10-23 October 2016, pp. 40-1; and James Drew, 'Airborne gateway', *Aviation Week and Space Technology*, 10-23 October 2016, pp. 41-3.

13 John Stillion and Bryan Clark, *What it takes to win: succeeding in 21st century battle network competitions*, Center for Strategic and Budgetary Assessments: Washington DC, 2015; and Andrew F. Krepinevich, *Maritime warfare in a mature precision-strike regime*, Center for Strategic and Budgetary Assessments: Washington DC, 2014.

14 Edward N. Luttwak, *Strategy: the logic of war and peace*, The Belknap Press: Cambridge, 1987.

15 August Cole, 'Lesson learned from the next world war–integrated cyber and space operations in ghost fleet', in David Burns (ed.), *RAAF Air Power Conference 2016: Multi-Domain Integration*, Air Power Development Centre: Canberra, 2017, pp. 75-85.

16 Sydney J. Freedberg, 'Iraq: proving ground for multi-domain battle', *Breaking Defense* [website], 27 April 2017, available at <https://breakingdefense.com/2017/04/iraq-proving-ground-for-multi-domain-battle/> accessed 7 December 2017.