ROYAL AUSTRALIAN AIR FORCE
AIR POWER DEVELOPMENT CENTRE

Working Paper
43

Fifth Generation Air Warfare

by Dr Peter Layton

FOREWORD

For over two decades the Australian Defence Force has been engaged in continuous operations. During much of this period, operations have occurred in a range of theatres across the globe. At times there has been significant concurrency with single force elements engaged simultaneously at varying tempo and scale, across diverse terrain, operating environments and threat. The Maritime Patrol capability, for example, has been engaged in anti-piracy, irregular arrivals operations, overland reconnaissance and targeting, as well as fisheries patrols and survival assistance from the Middle East to the South-West Pacific.

However, as we look toward the next two decades, an even more complex and challenging strategic environment faces us. Not only is our geopolitical environment becoming more complex, but so too is warfare. The introduction of fifth-generation capabilities is likely to see potential combat spread across all the domains of land, sea, air, space and cyber.

As we increasingly depend upon networks and access to the electromagnetic spectrum, we see both threat and opportunity in the cyber domain. Networks will form and disappear in a combat cloud to deliver an effect in support of an operation. Access to space-based systems will become increasingly a dependency and a target. No single line of operation will occur that does not spread across most if not all the domains.

Availability of data, data assurance, accuracy, deception and denial will become critical to future operations and will involve both military and commercial as we become increasingly dependent upon commercial support for mounting and sustaining operations. These dependencies and the associated risk are both targeting opportunities and our Achilles' heel of fifth-generation capability.

The one thing we can be assured of is that by the very nature of networks and cyber, fifth-generation operations will be fast paced, and the time available for decision-making will be compressed. Dr Layton's paper challenges us to expand our consideration of how a fifth-generation force will be employed and challenged.

GPCAPT David Millar
DAPDC
June 2017

ABOUT THE AUTHOR

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

INTRODUCTION

Fifth-generation air warfare is a beguiling concept. It offers the promise of making the use of air power in future wars significantly more effective and efficient. And this is not some inward-looking perspective. Chinese and Russian military thinkers also consider fifth-generation ideas offer real promise.

Even so, fifth-generation air warfare concepts push the boundaries of current technology. This is a remarkably complicated way to make war with real engineering challenges both in hardware and software. Moreover this incredibly intricate way of war is meant to function to a high efficiency within an environment where adversaries are trying very hard to defeat it. It is understandable that some may have doubts about the compatibility of fifth-generation air warfare with war—a violent act waged in a chaotic environment where friction, ambiguity and uncertainty are endemic.

Some may also ask about the preceding generations of warfare that makes this the fifth. Many authors have attempted to simplify humanity's long history of making war down into well-defined epochs but none of these constructs are widely accepted. Furthermore, it is true that the term 'fifth-generation air warfare' originated as an aerospace company marketing slogan. This all might suggest that 'fifth-generation air warfare' is a somewhat vacuous term. Taking this position though would be a grave error of judgment.

As this paper shows, there is now a great deal to the concept of fifth-generation air warfare. The term has come to encompass and combine several important ideas, in particular: network-centric thinking, the combat cloud operational construct, multi-domain battle and fusion warfare. Fifth-generation air warfare is now a multifaceted concept with real underpinnings.

This paper initially explores the ideas on which fifth-generation air warfare is based with the second chapter extending this to discuss some of the practical difficulties in actually implementing these enticing visions. Chapter three looks at the application of fifth-generation air warfare to battle network and hybrid wars. Together the two types of conflict illuminate some of the fundamental warfighting issues associated with fifth-generation air warfare. Chapter four considers how China and Russia approach fifth-generation air warfare. Their particular strategic cultures and national requirements mean the two countries have adopted unique approaches to fifth-generation air warfare but in this there are insights potentially useful to others. The short conclusion then brings this complicated story together.

This paper covers many aspects but by no means all. An important gap that the paper's approach may unintentionally conceal is that concerned with human cognitive processes. This paper focuses principally on *what* people should think about when using advanced digital networks to fight fifth-generation air wars rather than on *how* they should think. This distinction may seem abstract however, the decisions we make to address complex problems are significantly influenced by how we structure the way we think about such problems—not simply by the nature of the problems themselves. This paper then, in focusing on the nature of fifth-generation air warfare only opens the discussion.

2. FIFTH-GENERATION AIR WARFARE THINKING

The fifth-generation air warfare concept is a powerful one but to be best applied needs to be understood. Fifth-generation air warfare may be conceived 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 been incorporated into the idea of fifth-generation air warfare. The concept has progressively evolved and this evolution continues.

The Network

The fifth-generation air warfare concept is based on the idea that military forces are systems, and in particular 'systems of systems'. Military forces 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 world-wide 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'. By 1999, the US Joint Staff's papers were asserting that: 'the primary mechanism for generating increased combat power in 2010 will be networks of sensors, command and control, and shooters'. This proved prescient.

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

1. **An Information Grid**. The entry requirement for fifth-generation air warfare is a high performance information grid. It is the fundamental building block, which provides the infrastructure for receiving, processing, transporting, storing, and protecting information. 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. The information grid can consist of both military and commercial communication capabilities and transmit multiple information types in multiple modes at multiple data rates. Voice, data, and video can be transmitted via point-to-point or direct broadcast.

2. **A Sensing Grid**. Sensing grids are composed of individual nodes that scan the battlespace to detect, track and identify targets. The elements compromising the sensing grids can include dedicated sensors, sensors based on weapons platforms, and sensors employed by individuals, as well as embedded logistic support sensors. The information from the sensing grid is distributed across a force through the connectivity and computing capabilities of the information grid. The size, composition and complexity of the sensing grid required to support a specific mission is a function of the level of battlespace awareness required to prosecute the mission. A few wide area sensors may suffice for sea surveillance over a large area, but in an urban environment a large number of local area sensors will be needed.

3. **An Effects Grid**. 'Shooters' form the effects grid. They engage targets based on sensor grid information distributed across the communications grid. The 'shooters' aim to create desired effects and can be quite diverse in type 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, problem-solving skills and cognition (thinking processes). This grid though could also include knowledge-based, artificial intelligence, software applications that act as command

advisers able to recommend courses of actions. In this grid construct, the control function relates to the passing of instructions from the commanders to subordinate elements and accordingly is part of the information grid.

Conceptually, the information, sensing, effect and command virtual grids overlay the operational theatre. The various force elements, from individuals and 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 well-known Boyd loop of Observe, Orient, Decide, Act (OODA). 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.

The grids, being virtual, can be standing or created on order to meet the operational situation as the commander requires. Even from an established grid system, different quality services can be provided to meet the needs of different users. A strategic-level commander may only need broad positional information on friendly and hostile force location but across the whole theatre. Conversely, an air defence commander may need highly precise hostile aircraft track data, but only covering the small area in which the engagement is taking place.

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'. 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'. This is not just exchanging radar track data but also electronic surveillance data, allowing targets to be detected and identified with a high degree of confidence. All involved will know where the hostile aircraft and systems across the battlespace are located, their type and mission profile. This extends not just to air targets but also to the electronic battlespace where emitters can be geo-located and identified. Moreover this is all-round; the view from the cockpit is not as in older platforms that in front of the aircraft but instead a 360- degree view extending hundreds of kilometres. All on the grid whether airborne or surface-based can greatly benefit from a wide-area, integrated surface and air picture.

Secondly, the combat cloud makes long-range engagements more practical. Implicit in the combat cloud concept is that the multi-sensor 'big picture' transmitted to all friendly aircraft will provide an accurate identification of distant aircraft well outside visual range. In earlier eras, electronic identification was somewhat erratic and in many cases the fighters needed to close with the target and visually verify that it was a hostile aircraft before engaging. 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 and 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 and retain a significant tactical advantage.

Thirdly, with a high-quality distributed air picture, no single aircraft or surface-based system is critical to mission success. In having multiple aircraft and surface systems with multiple sensors all contributing, the loss of one input is not catastrophic. An example might be a future offensive counter-air operation deep in hostile well-defended air space that limits Wedgetail AEW&C operations. Fast jets however, can operate in such air space and, if there are several of them, by exchanging data they can build up a useful, detailed wide-area air picture. The more numerous the aircraft involved the more detailed, comprehensive and wide-area the air picture, and the greater the overall redundancy.

Fourthly, each aircraft pushing data into the cloud can electronically designate targets for other aircraft pulling information from the cloud. In this way, an aircraft that is electronically quiet, that is whose radar is

not transmitting, could engage distant targets being accurately tracked by other friendly aircraft using their onboard radars. The tactical advantage is that the quiet aircraft may go undetected by an adversary, as it is not emitting a powerful radar signal. This allows the quiet aircraft's missile attack to be both unexpected and from an unexpected direction.

This idea has been extended to overcome two problems. Stealthy aircraft with their internal weapons carriage carry relatively few missiles and some future air operations may feature a mix of stealthy and less-stealthy aircraft. In this tactical construct, stealthy aircraft would retain their own weapons as long as possible and instead use the weapons carried by the less stealthy platforms. The stealthy aircraft with their greater survivability would operate further forward in hostile airspace and use the information grid to pass targeting data through the combat cloud to others. The less stealthy platforms would become distant missile trucks throwing forward various air-to-air and air-to-surface weapons as the stealthy aircraft advised. The combat cloud is perhaps better named a 'combat thunderstorm', hurling destructive lightning bolts from any part of the cumulonimbus.

Lastly, the cloud concept allows good use to be made of the different capabilities offered by different platforms. The cloud should not be thought of as comprising simply homogenous all-the-same elements but rather multiple diverse elements. Specialised aircraft for example may be able to build up a much more detailed electronic order of battle depiction than more general-purpose platforms. Once this depiction has been disseminated and fused into the big picture all involved can benefit. In some respects, the information grid then allows all parties involved to possess the capabilities of all the participants—not just their own individual platform capabilities.

Multi-Domain Battle

The network-centric ideas conceived multiple aircraft, platforms and systems as being integrated nodes on information, sensing, effects and command grids. The combat cloud construct took this idea and made it into an operational concept that envisioned disaggregated, distributed air operations across an ever-changing area of operations. The network-centric idea and the combat cloud construct can be further extended beyond the air domain into other domains including those of land, sea, space and cyber. This extension is termed the multi-domain battle.

Information technology advances principally drove the development of the network-centric idea and the combat cloud construct. In contrast, the multi-domain battle concept arose from operational demands. Potential adversaries have developed armed forces that exploit weaknesses in friendly joint force structures and might now be able to defeat them. Multi-domain battle counters this by moving from the joint force construct where the three separate services operated closely together under unified command arrangements to an integrated force where technology combines the three services into a single entity, albeit virtual. Modern warfare however involves more than just the three traditional services and moreover there are some functional overlaps between them. The multi-domain battle concept accordingly breaks the battlespace up into the land, sea, air, space and cyber domains rather than into service components as some joint doctrines do.

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. As an example, an air combat force penetrating a well-defended operational area can mount a more effective strike with greater survivability if land domain rocket systems simultaneously engage hostile surface-to-air missile sites while cyber attacks sever adversary command and control communication networks.

The example highlights that an important aspect of cross-domain synergy is being able to synchronise all the various actions being undertaken. The required close synchronisation is feasible principally because of the multi-domain battle concept's network-centric warfare foundation. Importantly, in using closely synchronised cross-domain synergy, the multi-domain battle concept aims to create and then exploit only limited duration windows of opportunity where friendly forces have the operational advantage and can manoeuvre freely. Cross-

domain synergy is an asymmetric way to create temporary tactical dilemmas for an adversary to which they have difficulty suitably responding.

In air-land operations in Europe during World War II, 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 become subject to air attack. The enemy was on the horns of a dilemma: remain hidden from air attack and survive but if so be destroyed by land attack. The importance of friendly force close synchronisation is manifest.

The multi-domain concept means that friendly forces do not need to dominate in all the domains—land, sea, air, space or cyber—to win a battle. Indeed, friendly forces may not dominate in any but can instead prevail by gaining localised, temporary superiority through cross-domain synergy at the right places at the right times. Friendly forces in being able to manoeuvre across physical and virtual domains can gain the operational advantage over larger forces. In an extension of this vision, linking across domains means that the overall integrated force can be self-healing in that destruction of any single node may be able to be compensated for by another node in a different domain. No individual node may then be critical to friendly force operations.

Fusion Warfare

In combining network-centric thinking, the combat cloud operational concept and multi-domain battle it is quickly apparent that this is a complicated mixture. Making the 'way of war' so complicated means there are additional cognitive burdens imposed on warfighters. Worryingly, these burdens will increase as new platforms and systems from different domains join the network. Even today there is a greater volume of information collected on the battlefield than can be analysed.

Moreover there are inherent problems involved when accessing digital information from many different sources, each of which generally uses incompatible proprietary software. The various data streams are intrinsically difficult to combine with problems compounding as the software evolves in each stream or new systems from national and international providers are bought online. The introduction of systems with millions of lines of code has further exacerbated this issue as testing deep software interoperability across all possible permutations and combinations is problematic.

The solution is seen as fusion warfare. The combination of the two dissimilar terms—one technical, one operational—may seem unusual. The 'fusion' adjective relates to being able to use improved analytics that fuses 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 a very high standard that gives weapons quality tracking information and combat ID—attributes critical to the combat cloud construct. Achieving this data quality standard requires a deep understanding of how each sensor functions and the detection and tracking algorithms they employ. Machine-to-machine automation at the algorithm level is integral to the process. Another part of the solution is not to process all data but only that which is useful for the problem at hand.

The fusion process is though 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 enemies 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.

There is a subtle twist, success may not necessarily go to the side with the quickest OODA Loop. Instead, the side that prevails may be the one that best harnesses the power of the multiple OODA loops running across the multiple domains. At any time, there are many different OODA loops running in the land, sea, air, space and cyber domains. Best exploiting these various loops in parallel or in sequence is a difficult challenge for which complex fusion software including machine-to-machine learning and machine-to-human teaming may be needed.

Warfare though involves intelligent adversaries continually seeking competitive advantage. The complicated multi-domain networks friendly forces are using are an obvious area to attack. The easiest paths are either to attack various nodes to shrink the network's coverage or to use some form of wide area jamming and take the information grid down. The first approach though is readily apparent and other friendly sensors can be swung into action to compensate and replace those lost. The second approach is also readily apparent and so can be quickly countered by the friendly information grid manoeuvring within the electromagnetic spectrum. If satellite communications links are denied through jamming then high frequency links or landlines might be used instead and data dissemination transferred to them.

More difficult to counter are techniques that try to deceive network users. Users tend to believe the information presented on their displays. Any incorrect information entered into the network will be quickly disseminated to all and when combined with other correct data can rapidly create an inaccurate common picture. The multi-domain network concept though envisages very large numbers of nodes from individuals to large warships all contributing information into a wireless communication grid. There are many physical and virtual paths adversaries can potentially exploit to get incorrect data into the friendly force network. The solution is to adopt a trust but verify approach that incorporates multiple sensors that can confirm the information displayed. This makes the fusion process more complicated again but is critical for information assurance.

Fusion warfare allows command and control systems to more effectively manage the increasing volume of information but there are growing concerns that adversaries may physically attack the centralised command centres 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. Shorter decision cycles should also be feasible given the reduced span of control in the distributed control structure; this reduced span will allow commanders to remain more immediately alert to quickly evolving tactical situations. Moreover, distributed control would allow missions to be undertaken with aircraft launching with minimal information but receiving en route updates via datalinks on targets, combat support assets and recovery airbases. Additionally, this form of control would permit operations to continue if the centralised command centre was offline. Adopting the 'centralised command, distributed control, and decentralised execution' construct would focus the centralised command centres more onto problem prioritisation and resource assignment rather than delving deep into solving tactical-level issues.

The fifth-generation air warfare concept involves the combination of network-centric thinking, the combat cloud, multi-domain battle and fusion warfare. As such, fifth-generation air warfare seems particularly complicated, giving rise to concerns that the concept could prove brittle when exposed to deliberate attack. This worry though goes deeper in that being a system of systems there are difficult issues with data collection and dissemination even without adversary interference. Getting the fifth-generation air warfare concept to work either in peacetime or operationally is no easy task.

3. 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 producing decision-making quality data, nor maintaining wide area connectivity across multiple dissimilar nodes, are simple tasks.

Data

Fifth-generation air warfare is data hungry. The 'hunger' of command centres for useful data is readily apparent when considering the concepts of multi-domain battle and fusion warfare. Less apparent perhaps is that in fifth-generation air warfare individual platforms are also heavily data reliant. Major General Harrigian when director of USAF's F-35 Integration Office noted that modern stealth aircraft like the F-22 and F-35 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'.

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—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. The files required are generally complied in mission data reprogramming laboratories. Given that such files contain highly sensitive intelligence data each nation usually prepares its own mission data files for its own aircraft. The F-35 follows this model with separate laboratories at NAS Point Mugu, California supporting Japan, South Korea and Israel while others at Eglin AFB Florida support the US services, Norway, Italy, Australia and the UK.

There is a further twist with each mission data file needing to be matched to the particular software block load that each nation's aircraft have installed. As noted earlier, the data available is not just overlaid but instead fused to give weapons quality tracking information and combat ID. Achieving this requires a deep understanding of the detection and tracking algorithms the aircraft's sensors employ and these algorithms may change as software blocks are progressively updated. Each nation's mission data files are accordingly unique.

The location in the Continental US of the various different mission data reprogramming laboratories brings advantages but means they are distant to the operating bases that the aircraft would use in combat. Appropriate and reliable communication paths need to be available between the laboratories and the aircraft operating locations on other continents. These paths are potentially vulnerable to disruption from physical attacks, electronic jamming and cyber attacks and so require suitable hardening.

Complicating the issue, the electronic order of battle continually evolves during conflicts as adversaries and allies tweak and modify their equipment and tactics to win tactical advantage. Adversary forces will try to keep such modifications hidden from friendly data collection sources as long as possible so as to gain and retain tactical surprise. As part of this, adversaries will also try to deceive, mislead and trick the friendly in-theatre collection systems.

All this makes the mission date file updating process inherently complicated. In broad terms, this 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 back to the US of this information, on-call skilled software teams

able to quickly translate the evolving tactical circumstances into mission data files and then retransmission to distant locations to load onto each stealth aircraft before every sortie.

There are some implications from this mission data file cycle. Firstly, it is important to have in service the collector systems able to be focussed on the operational area of interest. These systems will usually be highly specialised, single purpose and costly in acquisition and operating budgets. Secondly, building up a detailed electronic order of battle across a region takes considerable time. Collector systems may to 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 suggests that electronic order of battle sharing arrangements with allies take 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. Combined with the probably fast-paced nature of such a conflict timely mission data file updating may become unable to be relied upon.

The problems in the mission data file updating cycle mainly apply though to what might be called background information that details the electronic environment within which a military force is operating. This data is often quite technical and may include large amounts of parametric information. It is important to note that 'electronic data' is used here to mean data across the entire electromagnetic spectrum including ultraviolet, visible light, infra-red, microwave and gamma radiation. As discussed, modern combat platforms and systems require this data to operate but there is also another kind of information needed by military forces.

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.

Big data is defined by the OED as comprising 'extremely large data sets that may be analysed computationally to reveal patterns, trends, and associations, especially relating to human behaviour and interactions'. The elements of big data reflect the increasingly complicated environments within which military forces operate. 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, military intelligence organisations now have significantly more data than can be analysed quickly enough to readily support combat cloud, multi-domain warfare and fusion warfare concepts. The analytic approach has thus shifted from looking for specific kinds of adversary activity—looking for needles in a haystack without knowing what the important needles look like—to looking for changes in the normal pattern of activity. The big data analytic approach can be visualised in four phases.

In the initial big data phase, a high volume, velocity, and variety of data from multiple diverse sources across time and space are collected, metatagged and placed into an information 'cloud'. The key here is to structure incoming and already stored data in the particular way that the tools available to analyse the data require.

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. This phase involves forensic analysis to identity particular patterns. The data used for this can go back several years depending on the situation.

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. This forward-looking focus is in contrast to the second phase that is descriptive and looks backwards in time. The activity-forecasting third phase aims to develop decision-making quality information.

The fourth phase involves interactive collaboration between the data analysts, the collection systems and the operational users. The intention is that all can interact with the data analytics to help focus attention on the critical elements to collect, analyse and understand. Operational users are no longer just consumers of

intelligence information but rather collaborators in its creation. To allow this to happen, the analysts and users work in the cloud with their projects, queries and folders captured and added to the cloud as further metatagged data.

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 but requires having significant automation of the first phase—placing tagged data into the cloud—and having optimised applications and situation-specific software tools in the second and third phases respectively.

Importantly this framework in practice is dynamic and backwards flowing: the operational circumstances will determine the situation-specific software tools required and thence how the applications should be optimised to support them. With this information, the data entering the cloud can be structured in the manner the applications require. Accordingly, using big data involves not just data analytics but also data science.

A data analyst assesses data to make projections about future events, determines the data most useful to customers and which reporting approaches are the easiest for users to view and understand. The data scientist in contrast mines the cloud to discover new relevant data types, develops software that can transform these new types into user-friendly forms suitable for analysis, and statistically models the data to uncover correlations between data sets. The data scientist also structures the information in the cloud through metatagging protocols and other approaches, so as to allow the analysis software to be best employed. Such data structuring also ensures that what seems like valueless data now can be later located, retrieved and manipulated to create high value information when new requirements emerge or improved analysis methods are developed.

This 'big data' process like the mission data file process discussed earlier is inherently complicated. There are significant issues involved in having the organisations, processes and highly skilled personnel in place to be able to participate in newly emerging operations involving combat cloud concepts, multi-domain battle and fusion warfare. A key characteristic common to these concepts, and important to fifth-generation air warfare overall, is the need for speed.

Being able to provide pertinent information quickly enough to support fifth-generation air warfare decision-makers requires not just considerable preparation but also the ability to quickly evolve elements within the big data and mission data file processes to respond to adversary actions and a rapidly changing environment. Simply considering the need to be able to quickly optimise software to meet new situations highlights the challenges involved for those military organisations embracing fifth-generation air warfare.

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 complicated 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 datalinks of varying capacities and capabilities. The archetypal datalink for airborne application is Link 16, one of the digital services of the Joint Tactical Information Distribution System. Link 16 is fitted to many Australian and allied aircraft, ships and command and control centres albeit not all. Link 16 has some shortcomings including in providing only line-of-sight linkages and so is used in conjunction with several other types of datalinks. The different systems 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 datalink connectivity problems. The aircraft have Link 16 but when used the transmissions from this system may be detectable by hostile electronic surveillance systems. Accordingly, stealth aircraft use special low probability of intercept (LPI) datalinks that, at the moment, are much harder to detect. These LPI datalinks 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, the USAF has developed special gateways that can connect the LPI datalinks (and other datalink types) to the Link 16 datalink network. The specific manner these gateways are employed varies with the permissiveness of the air environment. If the environment features hostile air defences, the gateway system may be carried in external pods fitted to F-15 fighters. The use of the pod on fighters allows placing the gateway forward into hostile airspace if necessary to be able to reliably connect with distant stealth aircraft operating deep in enemy territory. Moreover, as Link 16 can be detected, an adversary may try to engage a Link 16 emitting aircraft making having self-defence capability important.

In permissive air environments however, other gateway options become practical. Over Afghanistan and Iraq, the USAF uses modified business jets and Global Hawk unmanned aircraft fitted out as battlefield airborne communications nodes. In *Jericho Dawn 16-3* undertaken at Puckapunyal, a gateway hosted on a Grumman Gulfstream successfully linked RAAF fighters, combat support aircraft and Army helicopters.

Importantly while gateways have so far been discussed in terms of connecting stealthy and non-stealthy platforms, they are also useful in significantly expanding the network's area coverage. A high flying communications node can ensure data transmitted from a distant aircraft deep in hostile territory can be relayed backwards well into friendly territory to ground-based command and control systems. Airborne communications systems can overcome line-of-sight limitations in cases where satellite communications are not available or jammed. Airborne communications nodes may then remain useful even after stealth aircraft are equipped so as to directly link to non-stealthy platforms.

With airborne communications nodes there are several interacting issues. Survivability has been mentioned but the communication node needs to be reliable, flexible and persistent. Manned aircraft are flexible and allow networks to be quickly put in place and reoriented as necessary. Unmanned platforms can fly higher giving greater area coverage, and be persistent, but can be inflexible and at times have poor survivability. The solution may be to fly multiple platforms simultaneously so that if one node goes down others can quickly replace it.

For those air forces without such airborne gateways, the air network is split into two independent segments: firstly, the Link 16 segment that includes non-stealthy fighters, combat support aircraft (AEW&C and air-to-air refuelling aircraft), maritime patrol aircraft and naval warships; and secondly stealth aircraft operating in stealth mode. Having two separate segments is tactically constraining in preventing achieving many of the benefits of using the combat cloud construct.

Even with the gateway there are clear disadvantages in connecting the two networks. There is a single point of failure exploitable by hostile forces (or bad luck) while transferring data between the two different datalink types reduces data speed and quality. Using a gateway introduces unwanted complications.

Further issues arise when connecting networks to others outside of one's own air force. Military datalinks are encrypted and there are sometimes concerns giving other nations cryptographic information even if this is only valid for a short time period. With this released, there may be uncertainty as it who is accessing the data and their use of it to possibly glean sensitive friendly force operating data including concerning stealth aircraft. This issue becomes more prominent in considering multi-domain and fusion warfare concepts when not just track and identity data may be being exchanged but also more detailed intelligence and command and control information. Such concepts though will be much less operationally effective unless they are large scale, wide area and incorporate allied—and preferably partner—data.

There is another issue in sharing datalinked information in a coalition engaging in fifth-generation air warfare. 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 nations' 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.

Sharing data with other nations while balancing security and rules of engagement concerns will be a feature of fifth-generation air warfare. This may require multi-level security constructs operating both within and between the air forces involved. Such constructs will need to be developed, verified and practiced before a combined operation commences.

Looking to the future, most aircraft generally collect much more detailed information than is transmitted across current datalinks. Accessing this potentially crucial tactical information today can only be done after the aircraft lands and the information is manually downloaded and transferred to the network. Undertaking fifth-generation air warfare would be significantly enhanced in terms of reacting faster to new battlespace developments if better datalinks that allowed greater information flows could be installed.

Similarly, the inherent vulnerabilities that using networking involves need to be understood and compensated for tactically. Today's sophisticated electronic surveillance systems can build up comprehensive pictures of networks from detecting and geo-locating emitters. In the fast-paced air environment targeting airborne emitters is more difficult but technically possible. In the future, as electronic surveillance systems develop further, LPI datalink emitters will probably be able to be detected and tracked. Networks have a fundamental vulnerability through being built around discernible emitters. Fifth-generation air warfare in being built around actively transmitting networks has an Achilles heel.

Another inherent vulnerability relates to electronic jamming—both intentionally by hostile forces and unintentionally by friendly units. The USAF has concerns that hostile electronic countermeasures could degrade networks, slowing data transmissions, and possibly prevent networks being established in certain locations. Retired USAF Lieutenant General David Deptula considers that the USAF needs a robust datalink network much more than it needs a new fighter.

Datalinks can be made more robust to known jamming techniques but there will always be the possibility of technical surprise where the adversary introduces some novel approach. Having the capability to quickly understand evolving adversary electronic countermeasures aimed at network denial and then be able to counter them may be crucially important. Without this capability, network availability in times of conflict may be problematic particularly when the adversary is technologically advanced.

Importantly, in the age of multi-domain warfare, the network degradation and denial threat is not just from adversary jamming of the electromagnetic spectrum. There is also a considerable threat of cyber attacks that may insert false information into a network as well as simply deny its operation at all. Again having the capability to detect hostile cyber intrusions or attacks, quickly respond and re-establish secure networking is key.

There is also further concern over friendly transmissions interfering with own-force networks. The electromagnetic spectrum is crowded with numerous military and civilian transmissions and sometimes these unintentionally interfere with each other. In 2015 for example, the USAF determined that its satellite downlinks were jammed some 260 times by non-adversary transmissions.

The difficulty with understanding the robustness of military networks in a new operational situation is that each circumstance is unique and involves different mixes of emitters potentially from many various countries. From an electromagnetic spectrum management viewpoint, most modern battlefields are very complicated and hard to properly map. It is, therefore, impossible to fully determine before an operation commences how the various dissimilar transmissions will interfere with each other. Transmissions of concern include not just communication transmitters but also those from friendly force active electronic countermeasure systems. In the initial stages of an operation where combat cloud, multi-domain battle and fusion warfare are being undertaken it will be crucial to quickly start managing the electromagnetic spectrum to avoid 'own goal' interference.

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. Fifth-generation warfare may then be characterised as being a complicated way of war. Making sure it is not also overly fragile requires significant preparation before an operation commences and substantial support during it.

4. WAGING FIFTH-GENERATION AIR WAR

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'. To be adopted, the concept must be appropriate to the waging of future wars.

In discussing how fifth-generation air warfare may be applied to future wars, two specific types of conflict illuminate some of the concept's fundamental warfighting issues. These types are battle network wars, and hybrid/proxy wars.

Battle Network Wars

Battle network wars involve two networks fighting each other. 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. 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 upon 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.

The four-grid construct (described in Chapter 1) allows a hostile military system to be conceptually divided into constituent elements and the interactions examined to determine where force may be best applied to have the desired effect. In different situations, different grids or parts of grids will be the preferred place for the attack to focus on. If, for example, an adversary only has a few sensors but a large number of 'shooters' then the sensing grid may be the most profitable avenue of attack.

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 focussed 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 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.

This cumulative approach would involve a series of diverse and varied tactical actions that were in themselves independent events. The combined effect of these multiple actions occurring in time and space would however, ultimately fragment and defeat the opposing network. This defeat would not just be through attrition in a material sense but also through gaining a psychological edge over the opposing commander in terms of believing further tactical engagements will inevitably fail. Gaining decision superiority would enhance the likelihood of the success of each tactical action, as the opposing network would have difficulty responding in a timely manner.

Even so, gaining decision superiority would not in itself guarantee a network's survival wholly or in part in the face of hostile action. Battle networks have vulnerabilities that may be exploited through kinetic or non-kinetic attack. Continued operation over the course of a conflict would require the technical systems and organisations that comprise the network being able to readily evolve and adapt in a timely manner. As a result, the effects of some attacks may be limited in time and space as the networks repair, adopt work-arounds and organisations learn. Understanding the capabilities available to both the own-force and hostile networks as these continually change through tactical actions across the land, sea, air, space and cyber domains would be important to success.

This high-level outline of a fifth-generation air war suggests important considerations for commanders preparing their battle networks for conflict. The networks need to be of a sufficiently large scale that is 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.

Commanders should also attempt to prevent an adversary mapping friendly force networks, as this is likely to be a precursor to an adversary determining overall network vulnerabilities. Cyber operations in particular have the potential for an adversary to glean important intelligence. Ideally, battle networks should operate in a covert manner so as to minimise enemy exploitation and be self-contained to counter cyber intrusions. However, the wide area networks with the numerous transmitting nodes that fifth-generation air warfare concepts are based on make these ideals somewhat difficult to practically achieve.

Such considerations highlight 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. There are several tactical solutions to this dilemma including pre-positioning defensive assets to engage expected attackers and having pre-planned dispersion points. Another is to organise friendly forces into small, agile, nimble entities able to unmask, collect network data, and then 'shoot and scoot' before an adversary can respond. The US Army is trialling a Multi-Domain Task Force, some 1500 personnel strong, that is capable across land, sea, air, space and cyber domains and which can move quickly enough to be hard to pin down on a modern battlefield. Readily deployable air force units able to access numerous permanent and transitory air bases may be able to employ 'shell game' tactics and be similarly 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. For commanders considering this later option however, the force available to them in the new domain must have sufficient scale to shift the move-countermove cycle in their favour. If not, the other side may still succeed with its steadily accelerating attacks.

There is a concealed bite in this possibility of battle network wars progressively accelerating. Some—the Chinese and Russians in particular as discussed later—consider fifth-generation wars might be less costly, in terms of materiel and lives lost. 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 be two-phased. 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.

Fighting Offensively

In considering operational alternatives commanders have a choice between fighting their networks offensively or defensively. In discussing the offensive option, four different approaches are useful as examples—other options are possible as Russian thinking examined later reveals. In the discussion here however, each alternative focuses on different fifth-generation air warfare network grids and seeks a decision through cumulative tactical actions as noted earlier.

Option 1: Attack Adversary Sensing Grids. Fifth-generation air warfare concepts place a premium on information. Without accurate information on where adversary forces are located in time and space, the combat cloud and multi-domain battle concepts flounder. Significantly degrading an adversary's ability to determine

friendly force location would greatly enhance own-force combat effectiveness and survivability. Purposefully attacking an adversary's sensing grid may yield significant operational benefits.

An adversary's sensing grid would not necessarily need to be degraded across the whole battlespace. Instead, highest priority would be over friendly territory, next between friendly and adversary territory and lowest priority over an adversary's territory. The further an area is from an adversary territory, the fewer nodes and lower density an adversary's sensing grid is likely to possess. An adversary may have relatively few long-range sensor systems making their progressive attrition more feasible.

In this it must be remembered that in fifth-generation air warfare it is not just geo-location data that is important. As discussed in Chapter 2, in a conflict all involved will probably try to immediately change their electronic signatures to gain some tactical advantage. Until, an adversary's electronic signatures are determined and aircraft mission data files updated, friendly force units will have constrained effectiveness and survivability.

The best way to collect the necessary updated electronic order of battle information on an opponent is to operate over their territory, perhaps across multiple domains. Denying an adversary such an opportunity is important but also suggests that protecting friendly force sensing capabilities is crucial. In this, undertaking obviously focused attacks on an adversary's sensing capabilities may lead to a progressively faster move-countermove cycle as discussed earlier. Attacks on an adversary's sensing grid may be met with a response in kind.

A major issue is determining when and by how much an adversary's sensing grid has been degraded. If there is high confidence that it has been severely impacted, then friendly forces can readily operate and freely manoeuvre in the area between friendly and hostile territory. On the other hand, an adversary may seek to deceive friendly forces into thinking the hostile sensing grid has been rendered ineffective and draw friendly forces into pre-planned trap. Focusing on attacking the sensing grid presents some significant battle damage assessment challenges.

Even if friendly forces are able to significantly succeed in the counter-sensing grid campaign, they are unlikely to eliminate the enemy's sensing abilities entirely—especially across multiple domains—or an adversary's ability to regenerate at least some parts of it. The counter-sensing grid campaign will most probably not blind the adversary but rather cause him to blink or have impaired vision for some time. Accordingly, commanders need to be ready to take advantage of the possibly narrow windows of opportunity that emerge and have their effects grid 'shooters' ready to surge.

There are more ways to harmfully impact an adversary's sensing grid then physically attacking some of its nodes. The various grids are internally and externally linked presenting many opportunities for virtual exploitation, corruption and deception.

Exploiting another's sensing grid can be undertaken through mapping it, understanding its traffic flows, tapping into it physically or virtually, and if possible breaking its data encryption. The aim would be to gain an appreciation of how an adversary plans to employ his sensor assets. With this, shortcomings in coverage in time and space may be able to be determined allowing carefully timed friendly force activities to go undetected and untargeted. Such exploitation of an adversary's sensing grid may be more easily undertaken than it may appear. In 2009, Iraqi insurgents were able to use commercially available, low cost SkyGrabber software to regularly access video feeds from USAF Predator drones. As noted earlier, there are inherent vulnerabilities in the fifth-generation air warfare's reliance on datalinked information.

Corruption and deception activities are more complicated but can yield greater results. The intent would be to corrupt the data flowing through the sensing grid. This may be achieved by making friendly forces less detectable (across multiple domains), jamming hostile sensors, interfering with information flows across the grid, deleting sensor data being input and injecting false information. Success with corruption and deception activities may lead to the adversary's battle network breaking down so it is unable to attack friendly force units particularly those at extended range. Moreover, an adversary may also lose confidence in their sensing grid and be inclined to disregard its future outputs. As noted earlier, such problems may be limited in time and space and so friendly forces would need to be positioned to take advantage of them.

Option 2: Attack an Adversary's Long-Range Strike Systems. Significantly reducing an adversary's ability to strike friendly forces at long-range would limit an adversary's freedom of manoeuvre while enhancing that of

friendly forces. Friendly forces would then be expected to able to operate with considerably greater effectiveness and survivability in the contested area between friendly and adversary territory.

In a similar way to activities earlier discussed concerned degrading an adversary's sensing grid, operations against an adversary's long-range strike systems could be prioritised in effect. Highest priority would be attacking long-range strike systems that could reach friendly territory, the next would be those strike systems capable of attacking targets between friendly and adversary territory and the lowest priority would be those systems useful over an adversary's territory. In conceptualising in grid terms, an adversary's effects grid is likely to possess many short-range nodes but considerably fewer long-range strike nodes. This relative scarcity makes them a practical target set for friendly forces to engage and achieve meaningful tactical results. Moreover, replacing lost long-range strike is likely to be difficult and protracted making their loss operationally significant.

Option 3. Rapidly Attrite Adversary Forces. In some circumstances nations will be willing to accept higher loses than might be necessary to achieve a quick victory. Such an approach implies that the friendly force is significantly larger than an adversary and is able to absorb higher loses and still prevail. In this case, attacks massed in both space and time may be employed to quickly attrite adversary forces. The operational intent behind this action is to cause the adversary battle network to catastrophically collapse. In conceptual terms, this is a form of parallel air warfare where there are simultaneous attacks against as many nodes across the four grids as practical.

There are several issues with this option. Firstly, there must be considerable intelligence available about the adversary battle network to allow prompt accurate attacks across multiple domains. This intelligence is needed not just before an operation commences but also while it is underway to ensure no attacks are wasted engaging already destroyed nodes. Secondly, enough nodes across the adversary's four grids must be impacted in a time period short enough to cause overall network collapse. If not, the network may repair damaged nodes in time to avoid complete failure. Thirdly, a premium is placed on own-force capabilities to be able to surge, quickly rearm and conduct rapid reattacks. Key attributes include adequate availability, reliability and survivability. Lastly, the own-force needs to be of an appropriate scale to absorb combat losses and continue with high tempo operations.

Option 4: Force Horizontal Escalation. An adversary network will have been designed to cover a particular area sufficiently to support their chosen strategy. In this, the network is likely to have more nodes and linkages in those areas deemed high value. Undertaking friendly force activities in peripheral regions, outside the immediate area of competition, may encourage or compel an adversary to stretch their battle network to cover this additional zone, lowering node density and over-extending high demand nodes such as long-range sensors and strike systems. Alternatively, horizontal escalation may draw an adversary's main forces away from those areas that provide a geographic advantage. Either outcome may open up opportunities to rapidly reorient friendly forces back into the key high-value areas and try to force a decision.

Fighting Defensively

The alternative to adopting an offensive option is to instead employ a defensive posture. Such an approach might be adopted by the numerically inferior force that is at risk of being defeated in detail if attempting to engage in a broad offensive. The intent in fighting defensively is to avoid early defeat, and remain a viable force-in-being that influences the battlespace while awaiting more favourable circumstances. The adversary is unable to force a decision but must honour the potential threat posed.

A significant part of the adversary force must remain allocated to the defence so as to avoid defeat if the other force suddenly takes the offensive. In this way, the friendly force may impose a 'virtual' attrition on the adversary force and limit the number of adversary force assets that can be swung to offensive operations. Furthermore, in so doing the friendly force may decease the operational tempo ratcheting down the move-countermove cycle earlier noted.

In battle network terms, letting the adversary take the offensive permits the friendly force to gain significant information on the adversary force. In undertaking offensive operations, the adversary is forced to reveal the operational electronic signatures of the adversary battle network's most capable nodes. Moreover, the friendly

force will be able to map the opposing battle network and gain an understanding of how it is being fought. With this information, friendly force mission data files and electronic order of battle information can be readily updated, and multi-domain electronic countermeasures optimised. In contrast, the corresponding data concerning the friendly force can remain hidden from an adversary. The friendly force can arrange itself to be well-prepared for when it takes the offensive.

Indeed, the complicated nature of fifth-generation air warfare suggests that taking the defensive at the start of a conflict may bring real advantages. The multi-domain battle and fusion warfare concepts aim to achieve synergistic effects across time and space through undertaking coordinated actions in multiple domains. Achieving this requires being able to closely synchronise the various multi-domain actions being undertaken. Staying on the defensive until everything is in place to achieve the necessary synchronisation and harmonisation may bring significant operational benefits. There is undoubtedly a greater likelihood of being able to achieve tactical surprise and to create temporary tactical dilemmas to which the adversary has difficulty responding to.

Battle Network Analysis

The decision about adopting an offensive or defensive battle network posture may be made after considering not just one's own battle network capabilities but also that of the adversary. In undertaking this there are several factors to consider.

Firstly, the most important issue is determining what the network is designed to do. In broad terms there may appear clear distinctions between an offensive and a defensive network. The offensive network will place emphasis on extended range operations deep in hostile territory while the defensive network may stress, and be limited to, short-range operations over friendly territory. Such distinctions though are being eroded as ostensibly defensive systems are becoming longer-ranged, and now may overlay the adversary's territory to a considerable depth. Modern surface-to-air missile systems are an example (as discussed later).

In assessing defensive battle networks it may be better to determine if they have an anti-access or area denial purpose. Anti-access battle networks aim to build a fence around an operational area that stops adversary forces entering. Area-denial battle networks in contrast aim to impose progressive attrition on any adversary forces operating in the operational area, denying them freedom of manoeuvre. The two alternatives will have quite dissimilar design characteristics with different node densities and locations, and data flows.

Secondly, battle networks may be further defined by the attributes of key nodes. An offensive battle network for example may be built around supporting the employment of a particular long-range surface-to-surface rocket system. In being optimised towards this task, the network may lack flexibility for other roles. Another example might be an anti-access battle network that sought to attack adversary forces at long range entering an operational area. This function may make long-range active sensors able to give precise location data central to the battle network's operation. The attributes of these key nodes may give important insights into how vulnerable the network as a whole is to different types of attack or exploitation.

Moreover, key node attributes may be the limiting factor concerning the tempo a battle network can operate at. For example, a battle network built around long-range surface-to-surface rocket systems may rely on space-based data collection for reconnaissance and battle damage assessment. The orbital parameters of the various satellites involved may then determine the rhythm and pace of a battle network.

Thirdly, battle networks will evolve during operations in response to adversary actions; the networks in a sense will learn. Fifth-generation air warfare may be particularly competent in this respect by virtue of having inbuilt redundancies and multiple pathways. The 'systems of systems' network basis, combat cloud construct, multi-domain battle and fusion warfare concept all have as an attribute an ability to self-heal and shift important functions onto other nodes. The multi-domain battle is especially important here as functions may be moved into completely different areas of competition. The disruption of space-based nodes for example may see information dissemination functions shifted to air domain gateway aircraft with reconnaissance functions moving to the cyber domain.

In fighting between battle networks, at some point in the move-countermove cycle one network may jump to an unconventional solution to the challenges the adversary is presenting. In assessing battle networks, it is

important to think ahead and consider when and how a battle network might evolve, change some key attribute or readjust its purpose. Such shifts may then force a move in the other battle network from an offensive posture to a defensive one or vice versa.

Hybrid/ Proxy 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 defending battle networks. Examples include hybrid and proxy wars, which may also be used in combination. This section assumes that adversary, rather than friendly, forces will wage offensive hybrid/ proxy wars.

Hybrid wars are waged using a variety of dissimilar actors: state, non-state, sub-state and 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 substate 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 substate 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.

There seem several implications for fifth-generation air warfare. Firstly, the sensing grid may 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. 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.

Secondly, 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 of 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.

Thirdly, there may also be impacts on the effects grid. The problems posed in localising non-state and sub-state actors in well-populated areas might be partly addressed by using persistent armed unmanned aircraft. The difficulty in this is that the state forces may deploy long-range surface-to-air missile systems that prevent such air support being provided to friendly forces. For hybrid war the effects grid needs to provide diverse nodes to cover the full range of potential operational circumstances.

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 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.

Proxy wars are broadly similar to hybrid wars but with some subtle differences. The adversary may be using conventional military forces to wage war but these forces are now composed mainly of third party military units. Without large-scale direct involvement, the adversary homeland cannot be engaged and moreover generally neither can the regions the third party forces emanate from. The battlespace becomes limited to the immediate battlefield with other areas effectively turned into sanctuaries. Horizontal escalation is then disallowed. Furthermore, the use of proxy forces may make it hard determining who is involved in a conflict, their real interests and why they are fighting.

Most of the issues in using fifth-generation air warfare concepts in hybrid war also apply to proxy war. Proxy wars though may be slower paced again as the third parties involved may need training in the adversary's homeland before deployment. The level of technology used by such proxies may also be lower allowing unimpeded use of persistent unmanned aircraft for both attack and reconnaissance.

In proxy war though, a slower pace and lower technology levels may also work in favour of the adversary. In terms of pace, having more time may allow the adversary to develop, trial and implement effective countermeasures to fifth-generation air warfare capabilities. In terms of technology, an adversary may be able to make greater use of commercially available equipment modified as necessary to meet operational demands. In being commercial, such equipment may have signatures that allow it to blend into the background civil environment and at least partly negate some fifth-generation air warfare capability advantages.

While generally, proxy wars tend to involve mainly less skilled and less well equipped forces this may not always be the case. A high technology military force may join a proxy war at short notice to provide some critical military capability needed to avoid defeat or support an offensive. A quick unexpected introduction of new forces may strain force mission data file re-programming and electronic order of battle information collection. Until these support functions respond with new data files, friendly fifth-generation air warfare capabilities may be noticeably constrained.

The two different types of war help reveal the complexities in waging fifth-generation air warfare. The nature of the network 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/ proxy 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/ proxy forces also then have more time to adapt and introduce effective countermeasures.

The discussion here about these two different types of wars has taken a generic perspective to explore some of the issues involved in waging fifth-generation air warfare. It is based, however, on fifth-generation air warfare as we conceive it. Others have different perspectives and accordingly other conceptions.

5. OTHERS' FIFTH-GENERATION WARS

The fifth-generation air warfare concept has been principally shaped by American thinkers, in the main working within the boundaries set by American strategic culture. Beyond America however others have adopted subtly different approaches to fifth-generation air warfare influenced by their own strategic cultures and needs.

China and Russia have both been particularly active in developing integrated battle network capabilities even if their operational concepts stress different aspects. China has focussed on a conventional military force air/sea battle while in contrast Russia has focussed on a hybrid force, air/land battle. The Chinese battle network is defensively oriented but able to swing to the offensive when necessary. In contrast the Russian battle network is offensively oriented.

Considered together the two nations offer some interesting twists on fifth-generation air warfare concepts applied in dissimilar contexts. Given the future is uncertain, Chinese or Russian fifth-generation ideas may find application in other environments and circumstances.

Chinese Concepts

Since the 1990s, Chinese military thinkers have embraced 'informationised warfare' as the modern way of war. In the preceding industrial age, 'mechanised warfare' was the main form of war with the most important determinants of combat effectiveness being the size of the nation's armed forces and the quantity of key weapons like ships, tanks and artillery. In the view of the PLA Academy of Military Sciences, the rapid development of information technology has fundamentally changed this perspective. While weapons clearly remain important, advanced military information systems have now become the key determinant of combat effectiveness.

Contemporary Chinese defence strategy has embraced the informationised warfare idea and sought to implement it across all branches of the PLA. This implementation has been influenced by the strategic guidance flowing from Chinese government documents broadly equivalent to Australia's defence white papers. China's Military Strategy (2015) declared that while major wars were unlikely, localised conflicts were possible given power politics, ethnic troubles and territorial disputes. The most worrying local wars for China were those that might break out on its periphery. China's defence forces should then be developed to be able to end nearby local conflicts quickly, decisively and in China's favour. The combination of the informationised warfare idea with government strategic guidance shapes how China's defence forces are to be structured and postured. China's Preparation for Military Struggle (PMS) needs to focus 'on winning informationised local wars' and especially the 'maritime military struggle and maritime PMS'.

For China, fighting local maritime wars involves 'offshore waters defence'. Western observers have usefully broken China's offshore waters into two segments: the first extending some 600 kilometres from the Chinese coast lies within the first island chain; the second extends beyond this out to about 2000 kilometres and lies between the first and second island chain. If war broke out, the PLA would try to gain sea control in the closer segment—by establishing an anti-access fence—while further out seeking only sea denial. The later would try to impose progressive attrition on any adversary forces and deny them freedom of manoeuvre. The combination of the two would mean that closer an adversary got to the Chinese coast the more intense the defences would be, with a particular aim being preventing distant areas being used by hostile forces to launch long-range missile attacks.

In the area out to some 2000 kilometres from the Chinese coast, the PLA would wage informationised warfare however this idea is broader than it suggests. Chinese thinkers view informationised warfare as a confrontation between all the systems of the two (or more) countries at war. Not solely the military systems are involved but also the various national 'systems' of politics, economics, law and public opinion. This is a complex conception of a 'systems of systems' battle where not just hostile fielded military forces might be engaged but also the adversary's critical national infrastructure, its societal cohesion, and its governmental functions.

In undertaking such system-versus-system combat, the PLA Academy of Military Sciences 'Science of Military Strategy' (2013) argues the adversary should be considered as a single organism. By inflicting precise blows against the key points in adversary systems that rapidly reduce their integrity, stability and balance, these systems can be paralysed, operational activities disrupted, and military functions undermined. An adversary's

ability to resist can accordingly be overcome through the control and paralysis of its 'systems of systems' without having to cause heavy human casualties or inflict great material damage. Given this, the scale of informationised wars should be smaller than that of mechanised wars of the industrial era.

At the operational level, the waging of informationised wars morphs into 'noncontact warfare'. Pan Zhaonian writing in the *China Military Science* professional journal in 2013 declared that the 'concept of distance on the battlefield is fading away. Distance is no longer an obstacle…. This meets the inherent requirement for noncontact joint firepower attacks in informationised war. This is the essence of an informationised battlefield.'

The form of informationised wars then is the use of long-range precision-strike systems from beyond adversary defences against key nodes throughout the strategic and operational depths of the hostile system. Such noncontact attacks can be kinetic or cyber with the primary targets including command-and-control systems and logistics facilities. Indeed, the influential *Science of Military Strategy* argues that an adversary's main combat forces should be attacked only after the destruction of their key information nodes and logistics capabilities as this will significantly weaken them making their later destruction easier. The goal then becomes not the annihilation of an enemy but instead the paralysis of its combat forces by robbing them of essential information and supplies. Chinese thinkers draw analogies to damaging a body's brain and central nervous system.

The intent behind such attacks is to gain information dominance—sometimes also called 'information blockade'. With this Chinese forces will be able to seize the initiative early in a campaign and be able to set the conditions needed to achieve air and sea superiority. Information blockade though involves more than attacks. It also involves protecting Chinese information networks, using electronic warfare to deny an adversary collecting information and employing information warfare to deceive. PLA thinkers envisage that to succeed in a system-on-system confrontation will require close coordination of multi-domain kinetic attacks, cyber intrusions, denial efforts and deception.

The need for such close coordination in fighting such informationised wars has led the Chinese government to adjust the traditional three-Service structure of Army, Navy, and Air Force. The main innovation has been the establishment of a Strategic Support Force (SSF) that brings together single service and national-level space, cyber, and electronic warfare capabilities. The formation of the SSF enhances the PLA's ability to fight multi-domain conflicts. President Xi Jinping perceives the SSF as a 'new type of operational force' that is a 'major growth point of our military's new-quality combat capability'.

Establishing the SSF builds on the PLAs earlier adoption of the concept of Integrated Network Electronic Warfare (INEW), that combines electronic warfare and cyber into a hybrid capability. Behind INEW are battle network warfare concepts where electronic warfare enables network attacks to bridge the air-gap and enter relatively less-protected, isolated battlefield networks.

In this, the PLA has long stressed electronic warfare as a fourth combat dimension to combat, equal to traditional ground, sea, and air forces. Electronic warfare is considered an important force multiplier that can suppress or deceive enemy electronic equipment during combat. Electronic warfare for the PLA focuses on radio, radar, optical, infrared and microwave frequencies, in addition to adversary computer and information systems.

The SSF is however more than a fighting force. In also sponsoring numerous research and development activities, it is hoped that the SSF will accelerate indigenous military and civilian technology developments. The SSF will aim to develop disruptive technologies appropriate to military needs and which also have dual use application. This close association between military and civilian aspects is perhaps unsurprising given that the informationised warfare concept is derived from modern commercial information technology.

China's Battle Network

The Chinese battle network may be envisaged as comprising the four multi-domain grids as discussed in an earlier chapter: information, sensing, effects and command.

In terms of implementation, the information grid encompasses numerous multiple linkages between strategic headquarters, operational commands and tactical units out to, and in some cases beyond, the second island chain. Civilian and military leaders can communicate with in-theatre forces using secure fibre-optic cables,

HF and VHF communications, microwave systems and data links. Secure voice and data communications is provided through PLA communications satellites.

In this, all the PLA Navy's major combat ships are networked and can share data while for land forces, digitisation extends down to regimental level. In the PLA Air Force (PLAAF), most of the newer fighter aircraft are able to share data and connect with an information system managed by the PLAAF's airborne early-warning aircraft.

A major thrust for the PLAAF is meeting the 2015 Military Strategy document's guidance that it must 'build an air-space defence force structure that can meet the requirements of informationised operations'. This involves building an air force similar to that of many Western air forces with airborne early warning and control aircraft (AEW&C), an extensive land-based radar network, a modern surface-to-air missile force, a multi-role air combat fighter force and appropriate communications infrastructure. There are however some noteworthy aspects.

Firstly, The PLAAF considers air power as 'firepower warfare' where the greatest impact is achieved by using coordinated multi-domain aircraft, missile and information warfare attacks. The PLAAF may accordingly use its modern air combat force in mass attacks rather than in small unit operations, perhaps borrowing from the USAF playbook of employing force packages comprised of multiple fighter, strike and combat support aircraft. Given its increasing use of datalinks, the PLAAF appears notionally able to employ combat cloud techniques—or if not now, potentially in the future.

Secondly, the PLAAF appears to be developing a force structure that reflects earlier noted advice in the *Science of Military Strategy* about attacking key information nodes and logistics capabilities. The PLAAF is acquiring long-range surface-to-air missile (SAM) systems—some with anti-radiation seekers—able to engage hostile combat support assets such as AEW&C aircraft, ELINT collection platforms and air-to-air refuelling tankers if they close within range. Moreover, the PLAAF's new J-20 long-range stealth fighters may have been purposefully designed to engage hostile combat support aircraft. In this regard, US sources believe that the PLAAF may be developing a long-range air-to-air anti-radiation missile optimised for use against AEW&C aircraft. In informationised warfare, airborne sensing grid nodes may be as vulnerable to physical attack as ground based radar sites are.

Thirdly, the PLAAF has placed a particular stress on acquiring a large long-range SAM force that today includes the indigenous HQ-9, the Russian SA-10 and SA-20 and shortly the 400 kilometre range Russian SA-21 (S-400) system. China is also continuing Research and Development to extend the range of the HQ-9 to beyond 200 kilometres. Such ranges will allow engagements extending well off shore, including across that part of the first island chain around Taiwan. The PLAAF's land-based SAMs as an integrated part of the Chinese battle network can be an important part of the extended air superiority battle, rather than just for home airbase defence. SAMs have a place in the combat cloud construct as another effects grid node.

Lastly, in considering fifth-generation air warfare within the Chinese battle network there are further elements to consider, and in particular rocket forces, space-based capabilities and cyber.

Rocket Force. The PLA Rocket Force is a separate service alongside the Army, Navy and Air Force. In the battle network the Rocket Force uses ballistic rockets and cruise missiles to attack distant and well-defended targets. Manned aircraft are used in the anti-access zone for offensive and defensive purposes but in the outer area denial region the Rocket Force is preferred.

The Rocket Force operates various types of road mobile ballistic rockets fitted with either unitary HE warheads or able to dispense various submunitions (armour-penetrating, FAE, and possibly electromagnetic-pulse). Some rockets have Beidou (Chinese GPS equivalent) midcourse guidance to achieve reasonable accuracy while the anti-ship DF-21D has an active radar terminal seeker to target large warships. The Rocket Force also operates the CJ-10 ground-launched long-range cruise missile.

In Chinese thinking ballistic and cruise missiles can contribute to achieving air superiority through being used to attack battle network command centres, communication nodes, ground-based radar, electronic surveillance systems, airbase infrastructure and parked aircraft. Such a capability is practical principally because of the information that the Chinese battle network provides. Without accurate near real-time/real-time processed

intelligence on the location and status of adversary forces the combat effectiveness of the Rocket force would be significantly reduced. Certainly, attacking warships at sea would be impossible but so also would be viable attacks on parked aircraft. Without real-time targeting it would be unknown if the aircraft were currently there or had instead been deployed elsewhere.

In this the Rocket Force uses sophisticated tactics to enhance the survivability of its deployed units. These tactics involve manoeuvring between fixed operational and support positions when on operational deployment and on mobile operations as the main combat mode. In combat, the Rocket Force would rely on warnings from the Chinese space surveillance system to avoid detection by adversary satellites passing overhead; operate mainly at night; maintain a high tempo when preparing to launch or redeploying post-launch, and utilise multiple field operating areas and widely dispersed positions. In attacking targets the Rocket Force would try to launch closely coordinated, well-timed, multi-axis multi-domain attacks involving multiple ballistic rockets and cruise missiles, cyber intrusions and, if within range, manned strike aircraft.

Such tactics reflect a belief that operational speed is essential to both prevent being targeted by hostile battle networks and to defeat them. The newest missiles like the DF-26 intermediate range ballistic missile have numerous 'fast' features being able to quickly switch between nuclear and conventional warheads, swift road movement, fast launch preparation, and rapid withdrawal.

Space-Based Systems and Cyber. Space is seen as is the 'new commanding heights' with the ability to use space-based systems—and to deny them to adversaries—central to making informationised war. A robust, space-based C4ISR system is accordingly seen as a critical component of the battle network essential for power-projection and precision-strike. Remote sensing satellites (EO, SAR and ELINT) provide strategic intelligence before a conflict begins and real-time intelligence on adversary forces during combat. Communication satellites provide global connectivity, facilitating communications between far-flung forces. Navigation satellites provide critical own-force location information on location and improve strike accuracies.

To deny an adversary use of space the PLA has tested a direct-ascent, kinetic kill anti-satellite weapon (ASAT) based on a medium-range rocket. Other systems under development include jammers to disrupt space-based signals, micro-satellites that can shadow and later attack spacecraft, and directed-energy systems that could dazzle, blind, or potentially damage orbital systems.

Cyber can also potentially participate in multi-domain anti-satellite operations. Qi Xianfeng writing in a PLA professional engineering journal noted that: 'A military satellite cannot connect with the internet. Therefore, some people think "hackers" cannot attack a satellite's command and control [system]. But in actuality, the microwave antenna of the satellite control is open, so one can intercept satellite information through technological means and seize the satellite's command and control [system]. Using this as a springboard to invade the enemy's independent network systems is entirely possible.' If executed successfully, access to a satellite's controls could allow an attacker to damage the satellite; deny, degrade, or manipulate its transmissions; or access its capabilities and the information collected by its sensors.

Beyond anti-satellite usage, cyberspace is perceived in the latest (2015) Military Strategy White Paper as a new domain of national security and an area of strategic competition. Cyber is seen as both integral to achieving information superiority and as an effective means to disrupt an adversary's networks by targeting critical nodes. Cyber warfare capabilities support the battle network in three ways. Firstly, such capabilities can be used to collect data for intelligence purposes and for planning later offensive cyber operations. Secondly, to constrain an adversary's actions by targeting battle networks, network-based logistics, communications, and commercial activities. Lastly, cyber warfare capabilities can be a force-multiplier when combined with kinetic attacks in times of conflict

The Chinese battle network is a complicated, multi-domain system of systems designed to sharply enhance PLA combat effectiveness and win wars. This battle network reflects the Chinese view that informationised warfare is the principal way of war in an era shaped by information technology. The Chinese battle network thus has a somewhat philosophical foundation that looks across history to discern emerging warfare styles of war. There are some resonances in this in the foundations of Russian thinking about battle networks.

Russian Concepts

There are two distinct strands in Russian military thinking relating to the concept of fifth-generation warfare. Dating back to the 1980s and the Cold War, there is a 'digital-technological' line of thinking that progressively moved from reconnaissance-strike complexes into network-centric warfare. Such discussions both led, and at other times mirrored, American thinking about the impact of information technology on warfare. There was though a second strand that had deeper roots and conceived war as a battle of minds and favoured deception, information warfare and waging asymmetric war. This later stand focused much more on the psychological aspects of war and the cognition (thinking processes) of political and military decision-makers. The two strands have come together in recent years in a form called new generation warfare.

In a seminal 2013 article the Chief of the Russian General Staff, Valery Gerasimov, laid out his thinking on the new character of war. His discussion of modern warfare initially followed mainstream Western military thinking in noting that large scale force-on-force engagements are becoming rare, that stand-off precision guided weapon attacks are now the principal means used in combat, that an adversary may be attacked across the full depth of its territory and that 'the differences between strategic, operational, and tactical levels, as well as between offensive and defensive operations, are being erased'.

Gerasimov then though then added to this the central importance of information space—a term that in Russian military thinking denotes the space in which people form their perceptions. Information space encompasses both information technology and human cognitive processes; it is perceived as a zone of state and non-state actor competition where battles are fought over people's opinions. For Gerasimov asymmetric conflicts could be waged in information space through using information networks to significantly influence a country's political structures and its society. He laid out an aggressive three-stage strategy to overthrow hostile regimes through 'colour revolutions' that exploited fissures in a country's society, crucially at a low cost to the external parties.

Accordingly, the Russian view of modern warfare has become based on the idea that the most important battle-space is the opponent's mind. Waging new-generation wars then involves using network-enabled information and psychological warfare to both disrupt hostile military command and control systems and influence an adversary's military personnel and society. Such an approach can reduce the need for hard power significantly by making the opponent's military and civil population actively or passively support the attacker to the detriment of their own government.

Viewed in the terms of the four-element network discussed earlier, Russian thinking focuses strongly on attacking the command grid—the province of human decision-makers. There is a further innovation though in not being simply about attacking military commanders' perceptions but also about shaping their societies' thinking as well. The idea of influencing people is at the core of Russian operational planning and to be undertaken using cross-domain coercion. This involves orchestrating means across multiple domains within a unified program that either deters or compels an adversary. The aim is to manipulate the adversary's perceptions, change their decision-making and influence their strategic behaviour all the while minimising, compared to the preceding industrial warfare era, the hard power needed to be used.

This perspective sees information as a universal weapon that is low-cost, has unlimited range, is easily accessible and readily permeates state borders. It is not the only weapon available to a state but is one of the most effective. Using information in such an instrumental way can destabilise countries quickly and efficiently. Regime change in some circumstances might then not require armed intervention to achieve. In this the global internet is of considerable importance as it allows direct engagement of a hostile country's society.

Such a perspective in the terms of the four-element network concept conceives the four grids not as closed and exclusive but instead open and inclusive. The grids effectively are global given the world-wide web extends everywhere and so people's perceptions may be shaped from any direction. Moreover, anyone can be part of the network. The Russian viewpoint dramatically expands in space and membership the network-centric ideas that underpin fifth-generation air warfare concepts.

Perception is the centre of gravity in a new generation warfare campaign with the principal means being 'informational struggle'. To prevail in a conflict, informational superiority over the adversary must be gained and this involves using informational struggle both offensively and defensively. Informational struggle has

both technological and psychological elements that are employed to shape an adversary's perceptions, create a false strategic appreciation and obstruct the decision-making processes of individuals, organisations and governments.

In Russian military thinking, the aim of such activities is not simply to obscure the true picture but instead create a particular image of reality that causes the adversary of its own accord to choose to take specific actions advantageous to Russian objectives. Vladimir Lefebvre, a major Soviet-era thinker on this 'reflexive control' approach, observed that using this method: 'We can influence [the adversary's] channels of information and send messages, which shift the flow of information in a way favourable for us. The adversary uses the most contemporary method of optimisation and finds the optimal decision. However, it will not be a true optimum, but a decision predetermined by us.'

In its implementation, informational struggle has three important aspects. Firstly it combines cyber intrusions and electronic warfare with psychological and cognitive assaults. The computer network and electronic attacks aim to disrupt military and state command and control systems while the psychological assaults endeavour to deceive individuals, discredit leadership groups, and disorient society and the armed forces. Importantly, the focus of informational struggle is not just the armed forces but all of the opposing society—including the families of the members of the opposing armed forces.

Secondly, informational struggle is synchronised in time and space with other kinetic and non-kinetic means. These other means may not be military, with a ratio of 4:1 non-military means to military means being proposed. The emphasis is to minimise kinetic actions involving using military force. Information operations, deception, diplomatic activities, economic measures and political actions all loom large in new generation warfare.

Lastly, the informational struggle is ongoing being waged in peacetime as well as wartime and throughout the depth of the adversary's territory. There are no distant rear areas immune from attack. Moreover, it is waged across all levels of war (tactical, operational, and strategic) and whether seeking to deter or coerce another.

Informational struggle as a concept then coordinates and integrates all operational efforts across all domains. The idea of informational struggle makes Russian new generation warfare somewhat different to some Western notions of hybrid warfare. Achieving the desired outcome, while minimising the use of force, is different to the view of hybrid war as a strategy that wins through avoiding defeat. Informational struggle is about breaking the internal coherence of the adversary's systems of systems rather than its destruction. Russian new generation warfare includes the measured use of force but it is principally a strategy of influence not annihilation. Accordingly, cross-domain coercion is central.

New generation Russian warfare may seem remote to fifth-generation air warfare concepts but there are definite similarities particularly in network-centric thinking, combat cloud constructs and multi-domain battle. Network-thinking has been discussed earlier but the other aspects can be realised in considering the integration of air defence, artillery, unmanned air vehicles and electronic warfare in Russian operations in the Donbass region of eastern Ukraine.

Air Defence. Until mid-June 2014 Ukrainian air power was becoming increasingly effective and notably assisting the recapture of rebel territory. Russia then introduced various types of shoulder-fired anti-aircraft missiles to the battlefield and these quickly shot down or damaged several attack and transport helicopters, and some low-flying fixed-wing transport aircraft. To counter fast jets and highflying aircraft, radar-guided SAM systems were next employed.

Radar-guided SAMs were occasionally bought across the border and used before quickly retiring back to Russian territory; this 'shoot and scoot' tactic seems to have shot down a high-flying Antonov An-26 transport aircraft, two Mig-29 fighters and a Su-24M bomber. It was one of these SAMs, a Buk (SA-11 Gadfly) that also bought down Malaysian Airlines MH-17, killing 283 including 27 Australians. In addition, the Ukrainians lost three Su-25 ground attack aircraft from SAMs fired from Russian territory and reportedly one from AA-10 air-to-air missiles fired by a Russian fighter in Russian airspace.

By the end of August, Russia had gained control of the air domain over the battlefield mainly through using SAMs, rendering the Ukrainian air force ineffective and allowing Russian land forces to freely manoeuvre.

Artillery. Some 85 per cent of the Ukrainian land force casualties have been caused by Russian artillery and rocket attacks. Describing this high lethality, an American observer, Phillip Karber noted that: 'in a three minute period… a Russian fire strike wiped out two mechanised [Ukrainian] battalions with a combination of top-attack munitions and thermobaric warheads'. The Russians moreover have placed a noticeable emphasis on the use of Multiple Launch Rocket Systems (MLRS) with some five types deployed; most fitted with modern GPS-assisted highly accurate fire control systems. The rockets used range in size from 122mm to 300mm with warheads including high explosive, self-guided munitions, scatterable anti-tank mines and thermobaric. In this, the Russian battalions now field three times as many MLRS systems as previously, with three MLRSs today for every four artillery pieces.

Unmanned Air Vehicles (UAVs). Russia has deployed some 14 different types of UAVs to support its land forces ranging from high-altitude surveillance UAVs that fly along the border, to medium-range reconnaissance drones that orbit overhead Ukrainian positions, to small very-short range quad-copters used for scouting. The Russian use of UAVs in the Ukraine war is closely integrated with their artillery and rocket units. As a rough rule of thumb, Ukrainian forces consider that if a UAV flies overhead and identifies them, a Russian area attack from multiple artillery pieces and MLRSs can be expected within 10-15 minutes. Exploiting this fear of UAVs, the Russians fly multiple drones at varying altitudes; if one draws fire this can highlight the location of the Ukrainian forces to other drones.

The Russian UAVs used tactically are vulnerable to hostile fire especially from 14.5mm machine guns or 23mm/30mm rapid-fire cannons, but they have proven difficult to engage and so a rare loss is acceptable given their generally low cost. The most successful drone 'killer' seems to be electronic warfare where the Russians have been able to jam Ukrainian drone command and control transmissions, and the GPS signals being used for air navigation.

Electronic Warfare. Russian land forces in the Ukraine make extensive use of electronic warfare (EW) for various purposes. Some EW systems are used to geo-locate electronic signals emanating from Ukrainian land forces (or mobile phones) and pass this targeting data onto command centres, allowing multiple artillery and rocket attacks. Other EW systems can undertake wide area jamming preventing dispersed Ukrainian forces either communicating using radios or accessing GPS signals for navigation. Other systems intercept Ukrainian transmissions to collect useful intelligence information. Still others jam the electrical fuses used in Ukrainian artillery shells preventing these exploding. Lastly, mobile phones can be exploited with text messages sent to local communities just prior to an attack to create confusion and panic, while the defending Ukrainian soldiers receive personal SMSs calling on them to surrender. Russian EW then has both offensive and defensive roles.

The close integration of air defence, artillery, unmanned air vehicle, cyber and electronic warfare activities is readily apparent. This allows 'combat cloud' type distributed fire operations to be undertaken where sensors such as UAVs or EW geolocation systems can digitally designate targets to distant artillery units so they can quickly engage using MLRS. This is only possible given Russian air defence systems deny the use of the air domain by the Ukrainian Air Force. The multi-domain battle aspects are evident in the seamless combination of activities in time and space in the air, land and cyber domains with electronic warfare, space domain support and the use of information warfare.

Interestingly, Russian military thinkers unlike their Chinese counterparts do not devote attention to a conflict involving opposing battle networks. The Russian discussion makes a distinction between Russia possessing network-enabled capabilities and actually conducting network-centric operations but the issue of what is termed system-network war is only implied never examined. Instead the discussions are more about using digital networks in an operational environment where the human terrain constitutes the key battleground. The interactions between the opposing forces rather than the technical issues remain the focus.

The two battle network ideas have similarities but real differences. The Chinese approach implies fighting a symmetrical war involving mainly military forces with the sensing and information grid nodes preferred targets. In contrast, the Russian approach implies fighting an asymmetrical war involving mainly non-military forces with the command grid the preferred target. Together, Chinese and Russian thinking provides useful insights that help us better understand the possibilities fifth-generation air warfare potentially offers.

6. CONCLUSION

The aim of fifth-generation air warfare is to make air power significantly more effective and efficient through applying advanced information technology. Conceptually, fifth-generation air warfare has four parts:

1. **Networks**. Network-centric thinking envisions four interconnected and interdependent virtual grids—information, sensing, effects and command—overlaying the operational theatre. The various force elements, from individuals and 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.

2. **Combat Cloud**. In working together the grids can form a combat cloud that the various nodes can pull data from and add data to as necessary. This brings several tactical benefits including considerably improving situational awareness, making long-range engagements more practical, ensuring no single node is critical to mission success, allowing each node to designate targets to other nodes and ensuring the best use is made of the different diverse capabilities offered by each node.

3. **Multi-Domain Battle**. The five operational domains are considered land, sea, air, space and cyber. 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. Acting in a complementary manner—rather than an additive one—each capability enhances the effectiveness of the whole while lessening the individual vulnerabilities of each platform. Moreover, linking across domains means that the integrated force overall can be self-healing in that destruction of any single node may be able to be compensated for by another node in a different domain.

4. **Fusion warfare**. The fusion warfare concept seeks to address command and control concerns arising from the increasing volume and speed of information flows, software incompatibilities and intrinsic vulnerabilities to attack and deception.

Fifth-generation air warfare offers much but its practical implementation is not easy. 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. Fifth-generation air warfare is a very complicated way of war that requires substantial focused preparation being undertaken before a conflict and significant dedicated support during it. Success in fifth-generation air warfare is hard won.

There are also two in-built vulnerabilities in fifth-generation air warfare given its information technology foundation. Digital systems are inherently susceptible to cyber intrusions that may steal data, delete data, change data or insert false data that can then quickly spread across the network. While cyber security techniques are steadily improving so are cyber intrusion methods; it is like all warfare, a game of to and fro. Moreover, fifth-generation air warfare relies on datalinks that need to transmit to send information and sometimes to receive it. Emitters are inherently vulnerable to detection meaning that network participants can be located and tracked—and thereby targeted by precision-guided weapons. Some datalinks are harder to detect than others however just like in cyber, technology continually improves; again this is a game of to and fro. Cyber security and datalink emission tracking will remain concerning issues for the operational life of fifth-generation air warfare. They are its Achilles heel.

Fifth-generation air warfare capabilities principally exist for the purpose of fighting wars. In this, such capabilities are generally seen as most appropriate to high technology wars, which in the modern era means wars involving advanced information technology. Such a conflict would then probably be a symmetrical one where a friendly battle network grappled with an adversary battle network with both sides searching to determine which nodes on which grids were best to attack to defeat the other battle network. Battle network wars would be fast paced but given the complicated nature of fifth-generation air warfare capabilities keeping up would be problematic. Fighting asymmetrical hybrid/proxy wars would seem easier albeit these types of wars introduce other difficulties some of which favor the adversary. Achieving success in either kinds of war would make real demands on fifth-generation air warfare capabilities and the air forces that employed them.

Chinese and Russian thinking both take a more expansive view of many of the underlying ideas behind fifth-generation air warfare. The fifth-generation idea implicitly suggests conflict being constrained to a well-defined battlespace but Chinese and Russian thinkers demur. No part of an adversary's territory or any of the various national 'systems' of politics, economics, law and public opinion are considered off-limits. Both hold that informationised warfare can achieve success at low cost in blood or treasure.

Chinese and Russian fifth-generation warfare thinking is also alike in that neither focus on the effects grid's nodes. They both seek to avoid force-on-force, high-attrition wars. Chinese thinkers suggest focusing their efforts on attacking key sensing and information grid nodes with Russian thinkers stressing assaulting the command grid—for them people's minds are the real battlefield. Chinese conceptions favour using mainly military means to inflict multi-domain kinetic and non-kinetic damage. In contrast, Russian conceptions stress the cross-domain use of non-military means in preference to military means, with a 4:1 ratio suggested. Chinese battle network ideas accordingly imply fighting symmetrical wars whereas Russian ideas are very heavily oriented towards asymmetrical approaches.

By now, it will be readily apparent that the fifth-generation air warfare concept has many twists and turns. Implementing this concept, turning it into an on-call warfighting capability, seems a truly daunting prospect even if it accords with the *zeitgeist* of our information age. Becoming a fifth-generation air force would involve a substantial long-term technological and intellectual investment much greater than simply acquiring some new platform. It would indeed require an air force to completely transform itself.

SELECT BIBLIOGRAPHY

Adamsky, Dmitry (Dima), 'Cross-Domain Coercion: The Current Russian Art of Strategy', *Proliferation Papers*, No 54, IFRI Security Studies Center, Paris, 2015

Air Power Development Centre, '5th–Generation Air Force', *Pathfinder*, Department of Defence, Canberra, 2016

Berzinš, Janis, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*, National Defence Academy of Latvia, Riga, 2014

Carlisle, General (USAF) Hawk, 'C2 and Fusion Warfare', *Air Force Association Air Warfare Symposium*, 2017, http://secure.afa.org/events/AWS/2017/postOrlando/audio/3-2-17-Carlisle.asp [accessed 23 April 2017]

China's Military Strategy, The State Council Information Office of the People's Republic of China, Beijing, 2015, http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm [accessed 23 April 2017]

Cowan, Captain (USAF) Nicholas P., 'Rethinking Command And Control Of Intelligence, Surveillance, And Reconnaissance', *20th International Command and Control Research and Technology Symposium*, Institute Paper 94, 2015

Deptula, Lieutenant General (USAF Ret.) David A., 'A New Era for Command and Control of Aerospace Operations', *Air & Space Power Journal*, July-August 2014, pp 5-16

Deptula, Lieutenant General (USAF Ret.) David A., *Evolving Technologies and Warfare in the 21st Century: Introducing the 'Combat Cloud'*, The Mitchell Institute for Aerospace Studies, Arlington, 2016

Future Joint Force Development, *Cross-Domain Synergy In Joint Operations: Planners Guide*, Department of Defense, Washington, 2016

Garvin, Wilford L., 'Reflexive Control By Design: Crafting Emergent Opportunity in Complex Systems', *Over the Horizon*, 2017, https://overthehorizonmdos.com/2017/02/20/reflexive-control-by-design/ [accessed 23 April 2017]

Gerasimov, General (Russian Federation Armed Forces) Valery, 'The Value of Science Is in the Foresight', *Military Review* January-February 2016, pp 23-29, [Originally published in Military-Industrial Kurier, 27 February 2013]

Giles, Keir, *Handbook of Russian Information Warfare*, NATO Defense College, Rome, 2016

Harrigian, Major General (USAF) Jeff and Marosko, Colonel (USAF) Max, *Fifth-Generation Air Combat: Maintaining the Joint Force Advantage*, The Mitchell Institute for Aerospace Studies, Arlington, 2016

Jamieson, Major General (USAF) VeraLinn 'Dash' and Calabrese, Lieutenant Colonel (USAF) Maurizio 'Mo', *An ISR Perspective on Fusion Warfare*, The Mitchell Institute for Aerospace Studies, Arlington, 2015

Kass, Dr Lani, 'Panel: C2 and Fusion Threats', *Air Force Association Air Warfare Symposium*, 2017, http://secure.afa.org/events/AWS/2017/postOrlando/audio/3-2-17-C2Panel.asp [accessed 23 April 2017]

Kimminau, Dr Jon, 'Finding Clarity in Complexity: Interview with Dr. Jon Kimminau (Part I), (Part II), Part III)', *Over the Horizon*, 2017, https://overthehorizonmdos.com/2017/01/24/interview-kimminau-part-1/ [accessed 23 April 2017]

Krepinevich, Andrew F., *Maritime Warfare In A Mature Precision-Strike Regime*, Center for Strategic and Budgetary Assessments, Washington, 2014

Massie, Wing Commander (RAF) Andy, *Domain Control for Cross-Domain Effect:*

Defining the Central Purpose of the US Air Force, The Mitchell Institute for Aerospace Studies, Arlington, 2016

NIDS China Security Report 2016: The Expanding Scope of PLA Activities and the PLA Strategy, National Institute for Defense Studies, Tokyo, 2016

Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016*, Department of Defense, Washington, 2016.

Otto, Robert P., Lieutenant General (USAF), *Data Science and the USAF ISR Enterprise*, Department of Defense, Washington, 2016

Reilly, Dr Jeffrey M., 'Multidomain Operations A Subtle but Significant Transition in Military Thought', *Air & Space Power Journal*, Spring 2016, pp 61-73

Saltzman, Brigadier General (USAF) B. Chance, 'Multi-Domain Command And Control: The Air Force Perspective With Brigadier General B. Chance Saltzman (Part 1) (Part 2)', *Over the Horizon*, 2017, https://overthehorizonmdos.com/2017/04/03/multi-domain-command-and-control-the-air-force-perspective-with-brigadier-general-b-chance-saltzman-part-1-of-2/

[accessed 23 April 2017]

Schneider, Jacquelyn, *Digitally-Enabled Warfare: The Capability-Vulnerability Paradox*, Center for a New American Security, Washington, 2016

Stillion, John and Clark, Bryan, *What It Takes To Win: Succeeding In 21st Century Battle Network Competitions*, Center for Strategic and Budgetary Assessments, Washington, 2015

Wylie, Rear Admiral (USN) J.C., *Military Strategy: A General Theory of Power Control*, Naval Institute Press, Annapolis, 2014.