2016 Blamey Oration: The cyber and space domains in 21st century warfare

An edited version of the keynote address delivered at the
2016 Seminar on Military Strategy on 31 May 2016 by

Mr Steve Meekin, AM

Deputy Secretary, Department of Defence, Australia[1]
Member, United Services Institute of the Australian Capital Territory

Today, war can be conducted not only on, in or through the land, sea or air, but also through cyberspace and space. This paper describes these newer domains of warfare and details where they fit within Australia's recently released defence policy and cyber security strategy. Australia is increasing its investment in space and cyber capabilities and has the capability to disrupt, deny and degrade the computer networks of malicious cyber actors.

Key words: Field Marshal Sir Thomas Blamey; 21st century warfare; warfare domains; cyberspace; space; cyber warfare; space warfare; Australia's 2016 Defence White Paper; Australia's Cyber Security Strategy.

I wish to thank the Royal United Services Institute of New South Wales and the Field Marshal Sir Thomas Blamey Memorial Fund for inviting me to deliver the 2016 Blamey Oration. It is just over 65 years since the death of one of Australia's most distinguished soldiers.

My objective today is not to cover the well-tilled ground of his career, achievements and the controversies that characterised many of his actions and influenced his reputation. Over the years, his biographers John Hetherington, Norman Carlyon and David Horner have addressed the Field Marshal's performance and legacy with great insight and analysis (Hetherington 1954; Carlyon 1980; Horner 1984).

Any discussion of Blamey's command and performance as commander-in-chief of the Australian Military Forces during World War II almost always becomes an examination of his strengths and weaknesses as a commander. As David Horner wrote: "Blamey's record contains no outstanding peak, rather it is marked by year upon year of wise decisions, stubborn determination to further the interests of Australia and a deep concern for the well-being of his soldiers" (Horner 1984: 224).

What we do know is that in France 98 years ago Blamey, as a very capable chief-of-staff to the brilliant General Monash, comprehended new capabilities, especially tanks and aircraft, and, more importantly, the integration of these capabilities with the ground scheme of manoeuvre with infantry and artillery. Blamey's operations orders would become models for study at the British Army's staff college. His careful planning, attention to detail and preservation of Australian lives would characterise Australian operations. In today's terms, we might call this the synchronisation of the battle-space operating systems.

This afternoon we have the opportunity to explore two areas in which there has been significant development in recent years and each has significant impact on the battle-space operating systems of today. So my task in this paper is to provide an overview of 21st century warfare and the strategic significance of cyber and space, drawing on the 2016 Defence White Paper (Defence 2016) and the National Cyber Security Strategy (Prime Minister and Cabinet 2016). I will not be providing definitive conclusions; rather I will be setting the scene for my co-presenters who will deal in detail with space and cyber.

21st Century Warfare

Sadly, and unsurprisingly, war has a future and warfare in the 21st century will remain a reality. War will continue to exist at the fault lines of the international system and it is at these fault lines that we see the constants of inter-state competition, armed conflict in failing states, the re-emergence of an apparent descent into barbarism, and the empowerment of the forces of disorder, such as trans-national criminals.

As bleak as this may sound, less than 30 million people have perished in wars since 1945 whereas 110 million were killed in the first 45 years of the 20th century. And since 1945 the global population has doubled from three to six billion. We tend to forget the scale and devastation of the two world wars. As interesting as these statistics are, I feel sure few of us are willing to wager that we will feel more secure in the future.

While I will address the changing nature of warfare in the 21st century and Australia's most recent effort at positioning to meet those challenges, I do so with the enduring relevance of the theories of the student of war Carl von Clausewitz (Clausewitz 1832). They remain as relevant today as they have been for two centuries, simply because they do not depend upon a particular belligerent, technology or time for their underlying analysis. They are superior as the most unambiguous fundamental statement on the nature of war. And this is perhaps even more so now with the future of warfare so hard to predict and define and at a time when there has never been more written on the subject.

There is a key distinction between the nature of war and warfare. The nature of war – that is the imposition of the will of one belligerent on that of another and the forcing of compliance – is enduring. If you like, it is the 'Clausewitzian' element.

[1]E-mail: stevemeekin55@gmail.com

On the other hand, current trends indicate that future warfare will increasingly involve a diverse range of protagonists, each competing for control and the support of their targeted populations, in an inter-connected and, in part, empowered world.

In contrast to the immutable nature of war, the conduct of warfare changes over time. The analysis of trends, both incremental and radical, the application of technical developments in transforming the weapons of war, the general conditions in the society fighting the war, as well as the characteristics of conflict, all contribute to making any forecast of the shape of future warfare extremely difficult.

This is all the more so in the 21st century when one is tempted to be nostalgic for what seemed to be the certainties of the Cold War and great power competition. Professor Michael Evans, who holds the General Sir Francis Hassett Chair of Military Studies at the Australian Defence College, writes of an era in which the shape of warfare is transformed by digital networks, media penetration and precision weapons (Evans 2014). And to this we can soon add ubiquitous surveillance of the battle space.

This is where the power of the space and cyber domains is emerging alongside increased automation through robotics and unmanned systems. Importantly, Evans highlights the contested nature of the factors that shape future war, particularly continuing globalisation, challenges to the state and rapid demographic changes, especially urbanisation and the so-called youth bulge.

Without doubt we are in a global security environment of growing complexity in which there is increased instability, uncertainty and a wider and more diverse range of threats. In recent years there has been a good deal written on the character of future war – its continuities and discontinuities. Certainly there is discussion about warfare in urban areas, terrorism, the Islamic State phenomenon, miniaturisation of combat power, wider participation through the internet, the proliferation of real-time reporting and relatively easier access to sophisticated weapons. Political instability, the rise of populist politics, virulent nationalism, transnational organised crime and growing political radicalisation are also symptomatic of the underlying causes of conflict in the 21st Century.

Currently there is a bewildering list of terms to describe contemporary and future warfare by Western thinkers. Hybrid, proxy, asymmetric, information, ambiguous and new generation are labels. To these one could add war among the people and cities, particularly the mega cities. And the notion of so-called Fourth Generation Warfare where the state has lost its monopoly on war and there is reversion to conflict between cultures and religions.

Most are influenced by contemporary operations and the assimilation of lessons learned, especially analysis of the actions of a resurgent Russia, the growing economic and military power of China or the many Islamist conflicts in the unravelling of the Middle East and parts of Africa.

Australia's 2016 Defence White Paper does not identify or describe the fundamentals of the nature of war or how warfare might be pursued by either an adversary or the Australian Defence Force (ADF) in the next few decades of this century. It does, however, identify key drivers that will shape Australia's security environment to 2035. These drivers, drawing on our own analysis, are:

- the relationship between the United States and China and the likelihood of a mix of co-operation and competition;
- challenges to the stability of the rules-based global order, including competition between major powers promoting their interests outside the established rules;
- the enduring threat of terrorism and the foreign fighter phenomenon, including threats emanating from the ungoverned parts of the Middle East and Africa;
- state fragility, especially within our immediate neighbourhood, caused by uneven economic development, crime, social, environmental and governance challenges and climate change;
- the pace of military modernisation and more capable regional forces, including enhanced ballistic missiles; and
- the emergence of new complex non-geographic threats, including cyber threats and threats in space to the security of information and communications systems.

While these six drivers do not define or describe the future wars we may be required to fight, they are influential in focusing our thinking about the types of forces we need to develop and how we might employ those forces, either unilaterally or in coalition in order to prevail.

The Domains

In Australian doctrine, the operational environment embraces all elements, conditions and circumstances influencing the employment of military capabilities and the decisions of the commander during operations. In effect, this is the battle-space.

Within the operational environment there are six overlapping and interrelated physical and non-physical domains in or through which military activity takes place. These domains are land, maritime, air, space, information and human, with the information and human domains being the most recent and least settled in terms of conceptual and practical understanding.

In this construct, at least for now, cyberspace and the electro-magnetic spectrum are part of the information domain. That said, I think it highly likely that cyber will subsume or incorporate both information and the electro-magnetic spectrum becoming the domain name. I will refer to the cyber domain today.

Fundamentally and as a pre-requisite for success, a key objective in any conflict is to deny an adversary freedom of manoeuvre and ultimately access to a domain, while at the same time ensuring that the manoeuvre of one's own forces is as unconstrained as possible.

There are theorists who are clarifying the characteristics, concepts and general principles of the cyber and space domains. Sun Tzu (1988), Clausewitz (1832), Mahan (1890) and Douhet (1927), among many others, provided a basis for land, maritime and airpower. Similarly, there are visionaries, strategists and especially large numbers of vocal proponents building our understanding of what is possible (and not) in space and cyberspace. Unlike their predecessors much of their work, in the absence of being forged in the fire of general conflict, remains theoretical. With the accelerating pace of change, especially globalisation; a body of work, some tentatively based in experience, some speculative, is steadily being amassed. And particularly as I have indicated, the notion of cyber as a domain in its own right is contested.

Apart from the pleasure that may be gained from a discussion of the semantics of the for-or-against case for cyber as a domain, there is little point in distraction from the purpose of today, which is to better understand the national security impact of developments in cyberspace and space and Australia's response to those changes.

Quite separate to any consideration of the military domains, it is worth mentioning that both outer space and cyberspace are considered enabling domains, as well as, in some quarters, global commons, along with the oceans, atmosphere and the polar regions. As such, they are seen as shared resources. But it is the practical management of both cyberspace and space that is no less contentious than the other global commons, especially in balancing the multiplicity of vested state and private interests.

In December 2014, Chatham House – the Royal Institute of International Affairs – under the leadership of Caroline Baylon completed a multi-year research project examining the intersection of space and cyber (Baylon 2014). A number of security challenges that are common to both domains were identified and all are linked to growing militarisation and perhaps ultimately weaponisation. For Australia these are real challenges. Chief among them are:

- Growing asymmetric threats in the cyber and space domains where offence is technologically easier, cheaper and more cost effective than defence.
- A blurring between offensive and defensive actions and a shifting of the line to permit increasingly offensive activities under the guise of being defensive.
- A blurring of the line between non-military and military roles with increased use of dual-use technologies.
- An escalatory cycle of increasing militarisation of the space and cyber domains by a small number of states, which in turn, leads to more states responding to perceived threats.

Cyber

Cyberspace is not intuitively understood as a domain in a physical sense. It is fundamentally man-made and unbounded by geography; its speed and reach exceeds all; and it has a high degree of intangibility in that it is largely non-physical with little to touch. But it can be affected through the physical domains where its physical network components reside.

It is also interactive and made up of digital networks that are used to store, modify and communicate information. It includes the internet, but also other information systems that support business, infrastructure and services.

A key feature is that cyberspace consists of overlapping networks and nodes and is often described as being in three layers – the physical, where data are transported; the logical, where web sites are hosted on servers in multiple locations; and the persona layer, which is the people, organisations and entities on the network.

It also has a relatively low cost of entry in terms of component cost, technology and skills and it can evolve rapidly and unexpectedly creating new challenges and opportunities. And cyberspace is of itself indirect and lacking a sense of coercive power – at least for now.

Importantly, it has many owners and users who are allies, adversaries or neutral who may simultaneously use the same infrastructure. Operations in cyberspace can be stealthy with perpetrators remaining largely anonymous. Attribution of malicious activity can be difficult without compromising our capabilities.

On the other hand, everything that occurs in cyberspace has at its origin at least, a human being who has undertaken an activity at a particular place and time. Certainly, cyberspace has extended the operating environment, with weapons that are almost always dual-use.

The threat of cyber conflict is not limited to conflict between states; it can also involve non-state actors who pose a risk to the information economy. The perpetrators or threat actors include criminals; industrial competitors; foreign intelligence services; hackers and hacktivists; and employees – the so-called trusted insider.

Cyber warfare is both a tool of statecraft and a weapon that can generate its own psychological effects; *e.g.*, the 2007 Russian denial-of-service attacks against Estonia. Attacks of this nature demonstrate the vulnerability of modern economies in an environment of cyber dependence and increasing vulnerability.

The power of western states, especially the United States, to dominate the internet is strongly challenged by Russia, China and Iran among others. Debate on how to run the internet and cyberspace is bogged down in differences of national interest and ideology.

Against this background, the importance of cyberspace continues to grow as states are contesting who shapes the norms in cyberspace and internet governance. It is the lack of agreed norms and codes of behaviour that creates havens or sanctuary for adversaries.

Space

Space, unlike cyber, is a physical place and a relatively crowded one at that. There are over 60 states and 20 organisations that own one or more space platforms and there are at least 1300 operational satellites in orbit.

But these are not the only objects in space with at least 11,000 trackable objects consisting of defunct satellites through to spanners dropped by astronauts. And with these objects orbiting at about six times the speed of a standard NATO rifle projectile, each represents a kinetic threat to another.

From the outset, military technologies have been essential to the development of space technology. All technologies are inherently dual-use, with advances in one field being applicable in the other. This is so from launch vehicles based on ballistic missiles; to global positioning systems (GPS) used for commercial navigation and for the guidance of cruise missiles.

Dependence on space is growing. In precision targeting for example, almost 70 per cent of United States weapons used in the 2003 Iraq invasion were guided through space-based systems in contrast to just 10 per cent in the 1991 Gulf War. Today, it is well in excess of 70 per cent.

Space is certainly militarised, but it is not yet weaponised. It is a critical enabler of most military activity, being widely used for: surveillance, including signals and geospatial intelligence; the targeting of precision weapons; navigation and timing services; weather forecasting; early warning; and communications.

Space has always been a high-cost and highly technical endeavour. It is now becoming increasingly accessible with the entry of more nation-states, start-up companies, universities and even very rich individuals. As indicated by growing participation, space is no longer the domain of the major powers and accessibility will continue to grow with

advances in micro-technology and cheaper launch services.

It is against this background that the United States space strategy speaks of space as being congested, contested and competitive. And it is the United States and its allies who are increasingly dependent upon space with the United States reckoned to own 150 or so of the 170 declared military satellites in space. Many civilian satellites, of course, are inherently dual-use, with military applications such as communications.

Putting aside the threat of destruction or neutralisation of satellites through the use of kinetic, blinding or jamming from space-based or terrestrial-based weapons; satellites and their ground-based infrastructure are critical infrastructure and susceptible to cyber attack.

The 2016 Defence White Paper

Australia's 2016 Defence White Paper (Defence 2016) provides a comprehensive, rigorous, sustainable, and affordable long-term plan for Australia's security, especially the defence of our territory and interests. Its strategic underpinnings comprehend a more uncertain operating environment over the coming decades. State and non-state actors, in our region and globally, will have access to a range of cheaper, more precise and capable platforms and weapon systems.

Reflecting this uncertain operating environment, new investment in Defence capability will deliver a more effective, technologically sophisticated and responsive ADF. This investment will enhance Defence's ability to rapidly and effectively respond to strategic uncertainty over the coming decades with the highest levels of military capability and scientific and technological sophistication that Australia has seen.

Importantly, the White Paper recognises the vital role so-called 'key enablers' play in binding military capabilities together. And it is these enablers, neglected in the past, that underpin our aspiration to maintain decision-making superiority, both in strategic planning and the execution of military operations.

To this end, there is to be greater investment in intelligence, surveillance, space, electronic warfare, and cyber capabilities to ensure the ADF has superior situational awareness and knowledge of the battle space. This will enable operations in a more contested electronic environment.

To ensure our forces can operate effectively and securely, they require a comprehensive picture of what is happening around them – situational awareness. This requires collection, analysis, fusion and dissemination of information to support decision makers at all levels. And it is these activities that are the essence of decision-making superiority with both cyber and space capabilities critical elements.

The White Paper and its companion Integrated Investment Program bring together for the first time all Defence capability-related investment. It has a 20-year outlook from financial year 2016-17, with more detail on the first decade.

Investment in a range of enabling capabilities that contribute to decision-making superiority constitutes about 9 per cent of a $195 billion, 10-year, Integrated Investment Plan. That is in the order of $18 billion (about $1.8 billion per annum) with much of it for cyber and space related capabilities.

In workforce terms, the ADF will grow to around 62,400 permanent personnel over the decade to 2025-26 – its largest size since 1993. Some of that growth is to enhance decision-making superiority. The Australian Public Service (APS) workforce will also be rebalanced with 1200 new positions created in critical areas including intelligence, cyber security and space-based capabilities. The future APS workforce will number around 18,200 – down from around 22,300 in June 2012. The 1200 new positions will be offset by continuing reductions in non-essential areas. Success will depend upon recruiting and retaining service-people and public servants with the right skills and building the expertise to operate a more technologically advanced force. This will be very challenging and our greatest risk.

Cyber

Returning to cyber capabilities, the cyber threat to Australia is growing and we are experiencing increasingly sophisticated attempts to infiltrate public and private sector networks. The cyber threat is also a real and present risk to our national security and economic prosperity and cyber attacks can occur with little or no warning.

The security environment of the future – both in peace and war – will feature increased threats from offensive cyber. State and non-state actors have ready access to highly capable and technologically advanced tools to target others through internet-connected systems. Indeed, this is a conflict in which we are already a participant – as both victim and defender.

Cyber attacks are a direct threat to the ADF's war-fighting power given its reliance on information networks. Through the White Paper, Defence will have enhanced capabilities to deter and defend against cyber attack.

Defence already has considerable cyber capabilities and will continue to make a significant contribution to the Government's cyber security efforts through its leadership and significant contribution to the Australian Cyber Security Centre.

There is significant new investment to increase Defence's capacity to protect critical Australian Government systems from malicious cyber intrusion and disruption. Around 1500 of the new APS and ADF positions will be created to meet the increased demands of the cyber workforce and systems.

Space

Interest in space is not new. Space considerations have been reflected in every White Paper since 1987. That said, the 2016 White Paper places space in the context of our strategic interest in a secure and resilient Australia, noting that Defence must be prepared to manage the security consequences for Australia of threats in space and cyberspace.

Space-based systems are intrinsic to everyday Australian life. They have transformed the way we communicate, navigate, predict weather, conduct commerce and access information. While GPS is an enabler of military operations, it also makes the international banking system function. We also rely on space-based satellite systems to support networked capabilities and to communicate and fight.

Space-based capabilities also offer potential state adversaries advanced information gathering opportunities, including imagery collection. The availability of commercial

space-based systems also means smaller countries, private interests and non-state actors can access sensitive information, such as imagery of bases, exercises and equipment trials.

To ensure the security of our space-enabled capabilities, the White Paper points to strengthened space surveillance and situational awareness capabilities, including through the space surveillance radar operated jointly with the United States, and the relocation of a United States optical space surveillance telescope to Australia.

Enhancements to Defence's imagery capacity will provide the basis to further develop our intelligence, surveillance and reconnaissance capabilities, including through potential investment in dedicated space-based sensors.

Further investment in commercial leasing arrangements and future acquisitions will expand and strengthen Australia's assured access to space situational awareness information.

The ADF and its partners are reliant on space-based satellite systems to support networked capabilities and to communicate and fight when on operations. But we know that some countries are developing capabilities to target satellites to destroy these systems or degrade their capabilities.

Limiting the militarisation of space will require the international community to work together to establish and manage a rules-based system. This does not seem likely in the immediate future, but like-minded countries need to continue to work together on applying existing international rules and norms to space.

Australia's Cyber Security Strategy

Australia's Cyber Security Strategy (Prime Minister and Cabinet 2016) was produced against a landscape where the threat of malicious cyber activity is assessed as serious and growing and where this malicious activity threatens the privacy and safety of individuals and the wealth, prosperity and national security of our nation.

For the first time it mentions offensive capabilities and acknowledges that Australia has the capability to disrupt, deny and degrade the computer networks of malicious cyber actors in response to their actions or threatened actions. Therefore, the use of offensive cyber capabilities is an option to respond to activity such as intrusions and disruptions.

Conclusion

Both cyber and space are of growing strategic significance at a time when the nature of future conflict is quite unclear. Certainly, our observation and analysis of current conflicts tells us that the spectrum for future warfare is wide and likely protagonists, both state-based and non-state, are increasingly able to exploit both cyberspace and space to further their objectives while capitalising on our dependence. They seek to deny us the freedom of manoeuvre we need, indeed depend upon in both domains.

Most potential adversaries understand the opportunities afforded by cyberspace and space. Equally they understand our dependence on cyberspace and space to maintain our decision-making superiority in the battle space.

In response, the White Paper sets out the priorities for investment in Defence's capabilities and creates the conditions for the generation and sustainment of the ADF's fighting power. It also notes the increasing security threats in cyber space and that state and non-state actors will continue to challenge the rules-based global order in unhelpful ways leading to uncertainty and tension.

Importantly, the White Paper also places a high priority on investment in space and cyber capabilities as a means of enabling our decision-making superiority and protecting our own capabilities that reside in, or we depend upon, in these domains.

Sculptor Raymond Ewers' 1960 statue of Blamey in Melbourne's King's Domain depicts the Field Marshal standing in a jeep rather than more traditionally astride his charger. This recognises Blamey's role as a modern leader and driver of the Army's technological transformation. I wonder at the likelihood of any successor being portrayed in close proximity to a satellite down-link or a keyboard. Aesthetics aside, I hope not, as any rendering of a latter-day military leader of Blamey's stature, if true to Blamey's legacy, would indicate that our nation had again been in great peril.

The Author: Steve Meekin, the 2016 Blamey Orator, was appointed Deputy Secretary of Defence in March 2012 to lead the department's intelligence and security agencies. Earlier, he was Director of the Defence Imagery and Geospatial Organisation following a career in the Australian Army. Before retiring as a Major General in 2010, he gained extensive operational and intelligence experience. He later held senior appointments in the three Defence strategic intelligence agencies. He also served with the armed forces of the United Kingdom and the United States and completed a number of deployments in the Middle East, including command of a task force in Iraq. He is an Officer of the United States Legion of Merit; and a Member in the Military Division of the Order of Australia.

References

Baylon, Caroline (2014). *Challenges at the intersection of cyber security and space security: country and international institution perspectives.* Chatham House Report 29 December 2014.

Carlyon, Norman D. (1980). *I remember Blamey* (Macmillan: South Melbourne).

Clausewitz, General Carl von (1832). *Vom kriege* ("On war") (Ferdinand Drümmler: Berlin).

Defence, Department of (2016). *2016 Defence White Paper* (Commonwealth of Australia: Canberra).

Douhet, Giulio (1927). *The command of the air* 2nd edition; translated by Dino Ferrari 1943 (Faber and Faber: London).

Evans, Michael (2014). Forking paths: war after Afghanistan. *Parameters* **44** (1), 77 – 94.

Hetherington, John (1954). Blamey, the fighting field marshal (Angus and Robertson: Sydney).

Horner, D. M. (1984). Field Marshal Sir Thomas Blamey: Commander-in-Chief Australian Military Forces. In D. M. Horner (ed.) *The commanders: Australian military leadership in the twentieth century* (George Allen & Unwin: Sydney).

Mahan, A. T. (1890). *The influence of sea power upon history, 1660 – 1783* (Sampson Low: London).

Prime Minister and Cabinet, Department of (2016). *Australia's Cyber Security Strategy* (Commonwealth of Australia: Canberra).

Sun Tzu (1988). *The art of war.* Translated by Thomas Cleary (Shambhala: Boston).