The ADF and cyber warfare

Brigadier Marcus Thompson, AM, Australian Army

Introduction

The realisation of cyberspace as a warfighting domain generates a series of questions regarding the nature of war, the characteristics of war in cyberspace, and the role of cyber capabilities in any future conflict.

In his keynote address to the *Australian Defence Magazine's* 5th Annual Cyber Security Summit in June 2015, Major General Fergus McLachlan stated that 'the Australian Army subscribes to the Clausewitzian view that despite changes in the character of war, the nature of war remains largely unchanged'.[1] McLachlan further argued that:

> [W]ar is and will remain a fundamentally human endeavour, rather than a technical or engineering problem ... [and that it] is and will remain a context of wills in which rational actors seek to mitigate weakness and vulnerability while attempting to exploit either an opportunity or a weakness.[2]

In essence, McLachlan was arguing that there is nothing new in cyber warfare; rather, it involves the application of established military methods in a new warfighting domain. It is, therefore, important for the ADF to consider how to deal with the Clausewitzian characteristics of chance, uncertainty and friction in cyberspace and how cyberspace can be used to facilitate the application of violence to damage the will or change the behaviour of an adversary.

The ADF has joined its main coalition partners in recognising cyberspace as a warfighting domain alongside land, sea, air and space. For example, the Chief of the Army has characterised the Army's mission command system as his main modernisation effort, which involves shifting the Army's command and control system into cyberspace.[3]

The openness of contemporary information-sharing technologies has facilitated a massive transformation in the global security environment due to increased opportunities for malicious cyber activities that cross national boundaries. An increased dependence on cyber capabilities and the subsequent exposure to emerging cyber threats present a significant challenge to the ADF. Since cyberspace is now the primary domain for global communications and commerce, this challenge is likely to grow quickly and continually.

It is reasonable to argue that espionage, theft, deception and disruption are not new. However, the conduct of such activities in cyberspace has only been made possible by the relatively-recent proliferation of digital information-sharing technologies. Nevertheless, if the ADF is to fight and win in a hostile cyber environment, it must consider the types of cyber capabilities it needs—and how those capabilities might be developed and applied in order to achieve an advantage in the contemporary battlespace.

The aim of this article is to propose a broad framework for the development of cyber warfare capabilities for the ADF. It initially provides an interpretation of cyber warfare, based on the Clausewitzian view of war. It then describes the types of cyber capabilities required in a joint context, and why those capabilities are important. The article concludes with a description of how the ADF might seek to develop the required workforce to fight and win in cyberspace.

Recognising cyber warfare

A considerable amount of recent work on cyber warfare has emanated from Australia, the US and the UK, particular dealing with the complexities of defining cyber warfare, as well as presenting academic research agendas and operational definitions. Australian commentators identified in a comprehensive literature review include Peter Dortmans, Nitin Thakur and Anthony Ween of the Defence Science and Technology Group, who perceive cyberspace as an 'unconventional' domain for Australia, and see the nature of cyber warfare as 'nascent' for Australia.[4]

Michael Robinson, Kevin Jones and Helge Janicke, in their 2015 article 'Cyber warfare: issues and challenges', present an international review of contemporary thought on cyber warfare.[5] However, their paper does not provide a new definition of cyber warfare but rather presents various opinions on a range of relevant topics. The greatest problem the paper leaves is the confusion that is often present in media-focused and unclassified literature, where the realm of intelligence and cyber attack, involving both commercial espionage and possible attack on nation states, is not differentiated from the offensive or defensive uses of military cyber effects. Both are equally termed 'cyber warfare', which does not simplify the issue either academically or in practice.

As opposed to the perspective of Dortmans and his colleagues, contemporary military and political conflicts are likely to have a cyber dimension. The well-known cyber attack on Estonia in 2007 is arguably one of the most publicised hacking operations in recent computing history, demonstrating the effectiveness of propaganda and malicious attacks in the cyber domain. The cyber threat facing Australia is far-reaching, diverse and not widely recognised. However, the threat creates real challenges for government agencies, businesses, society and individuals, as well as for the military.

Cyber attacks can be conducted at a fraction of the cost and risk of other forms of attack, and with a high degree of anonymity due to the maze-like structure of the Internet. This creates a significant opportunity for a weaker party to generate a disproportionate effect against a stronger, conventional adversary. Other major powers have mature cyber warfare and cyber espionage capabilities at the strategic level, and their tactical and operational military cyber capabilities are beginning to be better documented.

Similarly, Western militaries have reasonably well-developed, albeit reactive, defensive capabilities but have been reluctant to declare or acknowledge the development of offensive cyber warfare capabilities. Australia's electronic warfare community continues to maintain traditional capabilities to intercept and maintain analogue push-to-talk voice communication, yet we now live and work in a world becoming increasingly dominated by Internet-protocol communications. This can only serve to increase the cyber threat to Australian public and private sector organisations and individuals.

Fortunately, the public discussion seems to be broadening. Michael Lehmann, in a recent article in this *Journal* titled 'The case for an offensive ADF cyber capability: beyond the Maginot mentality', notes an increase in public discourse among practitioners, academics and senior public policy figures alike.[6] However, much of the discussion lacks specificity in the development and practical application of cyber capabilities—or what a cyber war might look like.

In considering the character of cyber warfare, noted US authors Peter Singer and August Cole have produced a remarkably-believable suite of vignettes in their futuristic novel *Ghost Fleet.*[7] While the scenario includes close combat in the land, sea and air domains, the authors' descriptions of combat in cyber and outer space generate significant food for thought. However, while the actions in cyberspace in the book were critical to each adversary's success or failure, cyber capabilities were not individually decisive. The operational effectiveness of cyber effects was derived from their complete integration with operations in the environmental domains. Additionally, in the posited scenario, pre-emptory cyber activities were not recognised nor considered as acts of war.

One of the most coherent descriptions, outside the legal community, of an activity in cyberspace being considered an act of war also comes from Singer who, with his co-author Allan Friedman, argues in *Cybersecurity and Cyberwar* that any activity in cyberspace should be considered with regard to its effects.[8] They argue, for example, that if a cyber attack destroys a power station and, in the process causes massive damage and loss of life, it is analogous to a kinetic strike; moreover, such a kinetic strike delivered by missile, bomb or ground attack would unambiguously be considered an act of war.

As the hypothetical cyber attack on a power station generated a similar effect to a kinetic strike, it too can be considered an act of war. Conversely, stealing confidential information from the power station control network is not likely to be considered an act of war. Cyber war can, therefore, be recognised by modelling the effects of a cyber event, and comparing those effects to warfare in the land, sea, air or space domains.

The description by Singer and Friedman complements the argument by Greg Austin that 'there has to be a clear distinction made between "cyber security" on the one hand and … discussions of military and defence needs in cyber space'.[9] Further reinforcing the earlier argument that there is nothing new in cyber conflict, rather only old methods being applied in a new domain, Austin's point can be satisfied by drawing an analogy to national security, where the Australian Army's 'Fundamentals of Land Warfare' notes that actions occur and effects are generated across 'the modern spectrum of peace, crisis and war'.[10]

Yet most national security activities occur well short of war. So it would seem reasonable to argue that activities conducted in the cyber domain can only be considered to be 'cyber warfare' if the resultant effects are similar to acts of warfare in the physical domain.

The importance of cyber capabilities to the ADF

In his 2013 book, *Cyber War Will Not Take Place*, Thomas Rid has argued that, in isolation, effects generated in cyberspace are unlikely to be decisive.[11] Such arguments do not make cyber effects any less attractive to the ADF. In a similar manner to indirect fire effects, such as artillery and air-delivered munitions, cyber effects are highly likely to be key enablers to land combat.

However, as 'the networked battlefield represents our greatest asset but also our potential Achilles heel',[12] it is clear that any potential adversary will analyse the ADF's strengths and very quickly seek to understand and undermine any advantages. Just as with kinetic operations, where effective defence requires offensive action, so it is with cyber operations. It is, therefore, critical that the ADF considers the requirement to secure and actively defend itself in cyberspace.

To continue the comparison with indirect fire support, the ADF (and particularly the Australian Army) has well-practised tactics, techniques and procedures for defence from indirect fire effects. From a defensive land operations perspective, if an adversary has the ability to deliver indirect fire effects, everyone on the ground knows to spread out and quickly seek appropriate cover if an alert is sounded.

Similarly, proactive measures such as aggressively patrolling 'rocket boxes' and dominating terrain that could be used to launch an indirect fires attack are key elements of defensive measures. From an offensive perspective, every officer and non-commissioned officer in the Australian Army, regardless of Corps, has observed the effects of indirect fire during training and knows how to call for indirect fire support.

These procedures are analogous to the application of both passive and active cyber effects. Every member of the ADF should know how to defend themselves against a cyber attack—from not opening links in phishing emails, changing passwords regularly, to taking great care when using USB devices. Similarly, all leaders in the ADF should understand the effects available to support them in cyberspace, know how and when to integrate those effects into operational plans, know how and when to call for those effects, and understand the complexity and preparation required to generate cyber effects.

The indirect fire support comparison is particularly relevant given the references in the recently-published *Defence White Paper 2016* to defending systems from the threat of cyber attack, including systems used by Australia's deployed forces.[13] While the *Defence White Paper 2016* assigns overall lead for cyber operations to the Australian Signals Directorate, it is important to recognise that, like all highly-valuable capabilities, they can be in short supply, meaning there will inevitably be a limit to the capacity and reach of the Australian Signals Directorate.

Depending on the scale and nature of an Australian joint task force deployment, the Australian Signals Directorate may not be able to meet the full expectations of a deployed commander, especially in terms of integrating operational and tactical effects. Therefore, it is important that the ADF be able to generate both passive and active tactical cyber effects well forward, in support of the immediate priorities of the local commander. Passive effects would include informing the design and implementation of defensive security measures, detecting penetrations, containing adversary effects, and resolving security breaches.

Recognising that it is not good enough for a professional military force to be capable of only 'taking a punch', the ADF must also be capable of delivering active cyber effects, particularly to exploit opportunities as part of tactical action in support of local commanders. Such effects could include the design and delivery of malware, and extending the reach of the Australian Signals Directorate. However, the activity of ADF personnel in cyberspace will inevitably generate national sensitivity, and must occur only within a nationally-sanctioned legal and policy framework.

Lehmann argues that 'the legal, policy and conceptual issues around military cyber attacks should not prevent the ADF from immediately establishing a prototype offensive cyber unit'.[14] While this argument is strongly endorsed by the author, Lehmann's subsequent argument that such a unit should be established under the Vice Chief of the Defence Force to 'avoid parochial interests' seemingly fails to recognise that the Services remain the nursery of joint capability. Therefore, it is important for each of the Services to consider their respective requirements in both a single-Service and joint context.

Finding cyber warriors

To maximise operational effectiveness, the delivery of military effects in cyberspace must be fully integrated into joint plans and operations. Military effects will ideally be delivered by appropriately-trained and empowered military personnel. Given the specialist nature of cyber operations, personnel employed in such roles should be selected based on their attributes and aptitude, rather than their technical skills. While technically-qualified personnel will certainly have a critical role to play, intelligence and targeting functions are equally important to the successful execution of cyber operations. In an environment that is constantly changing, the required technical skills will require frequent refresh—and can be taught.

From an Australian Army perspective, passive and active cyber operations are not the sole domain of technically-qualified personnel from the Royal Australian Corps of Signals. While the required workforce is likely to be drawn from the Royal Australian Corps of Signals in the first instance, any member of the Australian Army with the attributes required to successfully execute cyber operations can be trained to be cyber warriors, regardless of their rank, trade, Corps or gender.

More broadly, and in order to find the right personnel to prosecute cyber warfare, the ADF may need to reconsider its recruiting model, physical entry standards, its pay structure, and traditional corps/speciality structures in order to open any cyber-related trades to both new and existing personnel with the appropriate attributes.

Conclusion

Despite the enduring nature of war, its essential character continues to evolve. Advances in technology and the pace of change of that technology will continue to increase, providing

opportunities for both the ADF and its adversaries, especially when it comes to influencing the perceptions of target populations. The complexity of modern systems and the quantity, accuracy and urgency of data bring a new level of complexity to the battlespace and a new range of challenges.

The seemingly-exponential proliferation and subsequent reliance on information-sharing technologies and tools will lead to an increasingly-congested, contested and accessible cyberspace. These circumstances will also enable more actors to access technologies that can potentially be used to attack the ADF's information-sharing systems.

Actual and potential malicious activity in cyberspace from various threat groups has forced the recognition of cyberspace as a warfighting domain. Professional military forces cannot always choose the terrain in which they fight. Nevertheless, they must understand, and be prepared to fight in, any terrain occupied by an adversary. It is, therefore, critical that the ADF develops the capabilities required to fight and win in cyberspace.

However, in order to do so, much work is required. Firstly, an appropriate policy and legal framework must be established for the development and application of ADF cyber capabilities. It is critical that Australian Defence policy maintains pace with technology to ensure that the ADF is empowered to meet any potential adversary in any warfighting domain. Given the emphasis in the *Defence White Paper 2016* on the development of cyber security capabilities, an additional layer of actionable policy is required to ensure appropriate implementation of the Government's intent at the operational and tactical levels.

Secondly, resources must be allocated for the education, training, and equipping of cyber warriors, including both individual and collective training, as well as simulation systems. Further, doctrine must be updated to recognise cyberspace as a warfighting domain, and to describe what that means for the ADF. Additionally, the ADF must revise traditional internal and external recruiting practices in order to staff this capability with the best available personnel. This will also require a clear understanding of the personal attributes that the ADF requires of its cyber warriors.

Cyberspace is a key element of the contemporary battlespace, whether Australia likes it or not. It is critical, therefore, that the ADF responds accordingly and develops the capabilities required to successfully prosecute the nation's wars in cyberspace.

Brigadier Marcus Thompson graduated from the Royal Military College Duntroon in 1988 and was allocated to the Royal Australian Corps of Signals. He has served in a variety of regimental, staff and policy appointments and is currently the Commander of the 6th Combat Support Brigade. He holds Bachelor degrees in Electrical Engineering and Business, Masters degrees in Defence Studies and Strategic Studies, and a PhD in cyber security.

Notes

1 Fergus McLachlan, 'Modernisation priorities for the Australian Army', presentation to Australian Defence Magazine's 5th Annual Cyber Security Summit, Canberra, June 2015, summary at <http://www.slideshare.net/informaoz/cyber-sec-2015-program> accessed 28 June 2016.

2 McLachlan, 'Modernisation priorities for the Australian Army'.

3 See, for example, Michael Clifford, Michael Ryan and Zoe Hawkins, 'Mission command and C3 modernisation in the Australian Army: digitisation a critical enabler', Australian Strategic Policy Institute: Canberra, December 2015, available at <https://www.aspi.org.au/publications/mission-command-and-c3-modernisation-in-the-australian-army/SR84_army-modernisation.pdf> accessed 28 June 2016.

4 See, for example, Peter Dortmans, Nitin Thakur and Anthony Ween, 'Conjectures for framing cyberwarfare', *Defense and Security Analysis*, Vol. 31, Issue 3, 2015, pp. 172-84, abstract available at <http://www.tandfonline.com/doi/abs/10.1080/14751798.2015.1056935?journalCode=cdan20> accessed 22 June 2016.

5 Michael Robinson, Kevin Jones and Helge Janicke, 'Cyber warfare: issues and challenges', *Computers and Security*, Vol. 49, March 2015, pp. 70-94, abstract available at <http://www.sciencedirect.com/science/journal/01674048/49> accessed 22 June 2016.

6 Michael Lehmann, 'The case for an offensive cyber capability: beyond the Maginot line', *Australian Defence Force Journal,* Issue No. 198, 2015, pp. 31-8.

7 P.W. Singer and August Cole, *Ghost Fleet: A novel of the next world war*, Houghton Mifflin Harcourt: New York, 2015.

8 P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What everyone needs to know*, Oxford University Press: New York, 2014.

9 Greg Austin, 'Australia rearmed! Future needs for cyber-enabled warfare', Australian Centre for Cyber Security, Canberra, 2016, available at <https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/DISCUSSION%20PAPER%20AUSTRALIA%20REARMED.pdf> accessed 28 June 2016.

10 Department of Defence, 'Land Warfare Doctrine 1: fundamentals of land warfare', Department of Defence: Canberra, 2014, available at <http://www.army.gov.au/Our-future/Publications/Key-Publications/Land-Warfare-Doctrine-1> accessed 28 June 2016.

11 Thomas Rid, *Cyber War Will Not Take Place*, Oxford University Press: New York, 2013.

12 McLachlan, 'Modernisation priorities for the Australian Army'.

13 Department of Defence, *Defence White Paper 2016*, Department of Defence: Canberra, 2016, available at <http://www.defence.gov.au/whitepaper/Docs/2016-Defence-White-Paper.pdf> accessed 28 June 2016.

14 Lehmann, 'The case for an offensive cyber capability'.