ASPI

SPECIAL REPORT

Digital land power

The Australian Army's cyber future

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

INTERNATIONAL
CYBER POLICY
CENTRE

Zoe Hawkins and Liam Nevill

December 2016

Zoe Hawkins

Zoe is an analyst in ASPI's International Cyber Policy Centre, researching and writing on international and domestic cyber issues. Zoe previously worked as a research assistant on the policy implications of quantum technology for the Centre for International Security Studies at the University of Sydney.

Liam Nevill

Liam is an analyst in ASPI's International Cyber Policy Centre, researching and writing on international and domestic cyber issues. Prior to joining ASPI Liam worked at the Australian Department of Defence on strategic and international defence policy issues.

Acknowledgements

As noted in the report the conclusions drawn from the digital land power roundtable are solely those of the authors. However the quality of the roundtable would not have been possible without the unique contribution from those who participated from the Australian Army, industry, Defence and academia. It is also important to acknowledge the additional support provided by UNSW Canberra without which ASPI could not have conducted the event.

About ASPI

ASPI's aim is to promote Australia's security by contributing fresh ideas to strategic decision-making, and by helping to inform public discussion of strategic and defence issues. ASPI was established, and is partially funded, by the Australian Government as an independent, non-partisan policy institute. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

Cover image: Australian Army communications system operator listens to her radio handset at the Taji Military Complex, Iraq, August 2015. The Communications Information Systems Task Unit runs communications across Task Group Taji and maintains contact with coalition forces in Iraq. Photo courtesy Department of Defence.

Digital land power

The Australian Army's cyber future

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

INTERNATIONAL
CYBER POLICY
CENTRE

Zoe Hawkins and Liam Nevill

December 2016

First published December 2016

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

Tel + 61 2 6270 5100
Fax + 61 2 6273 9566
enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

Facebook.com/ASPI.org

@ASPI_org

CONTENTS

Communication Information Systems Troop Leader Lieutenant Iain McLeod is deployed to the Taji Military Complex, Iraq, August 2015. Communications personnel from Australia and New Zealand work at the Taji Military Complex in Iraq, to support Iraqi Security Force training efforts. Photo courtesy Department of Defence.

INTRODUCTION

Earlier this year ASPI hosted a roundtable discussion on the strategic, technological and force structure adjustments that must be made so that the Australian Army can successfully adapt to the challenges, and exploit the opportunities, of cyberspace. The roundtable was a closed-door discussion under the Chatham House rule among representatives from the Army, the Department of Defence and academia. This report is the authors' summary of the roundtable.

The discussions covered the framing of the challenge and a variety of different potential cyber postures. The group considered the importance of employing the right technology and individuals, generating appropriate policies, and finally the obstacles that need to be overcome.

This report is an overview of the conceptual and practical challenges that the Army will face in an effort to both exploit and secure its cyber capabilities. It includes clearly distinct assessments from the authors on how the Army should address those challenges.

The market for change

Armed forces around the world are taking advantage of the benefits of cyberspace, and that has implications for the Australian Army. In a context of global competition, Australia can no longer be complacent in comparison to its international peers, particularly those in our nearer region. Military advantages accrue from relative power, and Australia must remain cognisant of the collective shift towards sophisticated, connected militaries.

Australia is certainly highly networked by global standards. The Army's recent modernisation and digitisation programs have further increased this connectivity.[1] The successes and challenges of this process are discussed in ASPI's *Mission command and C3 modernisation in the Australian Army: digitisation a critical enabler* and *ADF capability snapshot 2016: C4ISR—winning in the networked battlespace*.[2] Protecting the Army's increasingly large digital footprint will be critical to retaining its ability to project power and deter adversaries. The Army's priority should be protecting its information and cooperating within Defence to defend strategic and deployed networks.

Digitisation efforts involve the expansion of the Army's networks, from computers, tablets and smartphones to battle management and mission systems, and to reach-back capabilities extending to commercial supply chains and critical national infrastructure. That breadth and depth of connectivity offers great operational advantages, but also generates liabilities. The threat, risk and consequence of cyber threats to the Army and broader Defence systems vary but, overall, impacts on operational efficiency and security are the most consequential. Complacency about developments in cyberspace means not only missing out on potential benefits, but also neglecting the growing number of vulnerabilities that require active defences.

Connectivity without a guiding policy framework will reduce effectiveness, complicate upgrades or supplementation, and create critical areas of exposure to cyber threats for the Australian Army, the ADF as a whole and the rest of the Defence organisation. The need to determine the nature of the Army's cyber skills, capability and operations and implement reforms remains a formidable big-picture challenge. There's a need for a renewed focus on the Army's cyber development, within the context of broader ADF and Defence developments, in order to maintain Australia's force projection and protection capabilities. The correct frameworks, policy, technology and training are essential to translate Australia's technical strengths into an effective, cybersecure Army.

Achieving these reforms will require dedicated resources. It's important that the Army capitalises on the recent release of the 2016 Defence White Paper (DWP 2016). Establishing and articulating the business case for significant investment in the Army's cyber capabilities will be an important element in delivering the desired reforms. Requests for new capability must be clearly communicated while avoiding the duplication of effort and ensuring that the resources provided are commensurate with the Army's task at hand. This will make sure that the resulting joint force is properly supported.

Fortunately, the current market is a positive one in which to be implementing cyber reforms. There's a convergence of funding from DWP 2016, the Prime Minister's National Innovation and Science Agenda and the Cyber Security Strategy. The private and public sectors are demonstrating increasing interest in cybersecurity in both their rhetoric and their investments. The topic is also receiving increased attention from academia, where there are now more options for tertiary study in this area.

It's important that the Army take advantage of this context, capitalising on public and private interest, to advance its cyber reforms.

Conceptual frameworks

Cyber modernisation in the Australian Army will be more effective if it's framed in a clear understanding of the nature of cyberspace and how best to respond to it. DWP 2016 assigns the overall lead for national cyber operations to the Australian Signals Directorate (ASD), and everything the Army does will occur within that construct. The Army's understanding of the divisions between its own and ASD's responsibilities is maturing, but there remains a lack of clarity within the Army about how, with the support of other groups and services, it will manage cyber threats and exploit opportunities in support of Defence operations.

Executing a well-coordinated program of reforms should involve a consideration of the development of appropriate doctrine and plans for step-by-step adjustments. This is an important part of constructing a clear organisational narrative, as well as communicating policy needs more broadly.

However, the nature of cyberspace and technological change demands a more fluid, on-the-go development. The agility to respond to changes in the threat landscape and embrace new technologies is an essential component of the Army's cyber capability requirements. It must reconcile the need for an overarching vision and the imperative for immediate and adaptive reform models.

Evolution or revolution?

The nature of military cyber operations remains unclear, and uncertainty persists over whether they are simply a new way for the Army to manage and exploit information or an unprecedented strategic change akin to a revolution in military affairs. Establishing clarity on the nature of cyber operations is vital in order to inform the design and implementation of appropriate responses.

There's a tendency to characterise the proliferation of cyberspace as a civilisational change. It's true that these developments have had significant and wide-reaching impacts on the global economy, the propagation of social movements and the dynamics of international relations.

However, there are notable similarities between the characteristics of earlier electronic and information warfare capabilities and concepts and the challenges and opportunities presented to armies by cyberspace. Like previous information technologies, cyberspace is used to provide intelligence, surveillance and reconnaissance for greater situational awareness and better communication networks for an increasingly accurate shared operating picture.

On the offensive, it provides the means to deceive an adversary through misinformation or to disrupt their operations. Cyberspace also facilitates information operations more broadly through the dissemination of public messaging. Our adversaries will seek to use these capabilities to gain a similar technological advantage.

In this sense, the big-picture opportunities and challenges of cyberspace for armies could be seen as simply an acute modern iteration of an old dilemma. This is a new stage in the constant cycle between a technological advance and the exploitation of its vulnerabilities by an adversary.

However, it would be a mistake to conflate strategic similarities with the assumption that nothing needs to change. Each technology era requires different skills, and the Australian Army must develop new tactics to engage new challenges in pursuit of strategic goals in cyberspace. This idea echoes the Clausewitzian principle: while the nature of war remains the same, its character changes and is determined by 'the spirit of the age'. Thus, the Army needs to adjust its tactics, workforce and thinking to address these contemporary technological developments.

GETTING STARTED

There are many alternative frameworks in which the Army could position its cyber capabilities, and there's significant debate about whether the choice should be informed by a thoughtfully constructed theoretical framework or simply decided on the go as part of an iterative process. The Army must take the time to assess the benefits and challenges of both methods in order to construct a coherent approach to cybersecurity operations and capability. This clarity is necessary to support funding prioritisation and supplementation and broader policy reforms.

Operational flexibility is important, so there's an argument that the Army should focus on directly addressing the issue on the ground, rather than getting caught up in esoteric debates. A 'learn by doing' approach could allow for the integration of improvements and patching of problems to help policies keep up with rapidly developing technology. An agile, spiral development process with feedback loops for mid-project reflection and changes may be the Army's key to success in cyberspace.

However, when tackling that task, the Army must also consider the role of theory and doctrine. Cyber operations are a complex challenge with significant interdependencies and risk, so there's value in tailoring the Army's reform policies and avoiding slipping into a reductionist one-size-fits-all approach to the construction of a coherent organisational cyber concept and doctrine. The Army's approach to cyberspace will necessarily be developed in a broader organisational context, but it needs to have its own cultural and doctrinal approaches to cyber operations and a clear focus on what it must do to support whole-of-Defence and whole-of-government cyber priorities and missions.

Unfortunately, doctrine can take substantial time to mature, and the bureaucracy is slow to embrace change at the best of times. In contrast, technology evolves rapidly, as do the capabilities and strategies of advanced states and threats from agile violent non-state actors. As soon as an innovation is created, so is a counterstrategy. So, in practice, top-down and bottom-up activities will have to coexist, and a compromise will have to be struck between direction and agility.

Once a balanced policy approach is identified, it's important to keep its accompanying narrative simple and accessible. Cyberspace permeates all facets of operations and, in one way or another, involves all Army personnel. Thus, clearly articulated concepts and ideas will most effectively generate understanding and elicit behavioural change in the Army. Unnecessarily technical terminology may undermine the process of communicating the importance of the cause to all levels of management.

ASPI comment: Clarify the Army's conceptual understanding of cyberspace and define its role and responsibilities in Australian cyber operations

Creating concepts and doctrine based on a small number of high-level principles, such as maintaining decision-making superiority, protecting information, building resilient networks and establishing a culture of cybersecurity, would offer clarity on the goals, roles and responsibilities of the organisation, while allowing for responsiveness to new technological developments.

Establishing definitions of key terms (including cyberspace, cyber operations and so on) would enable a more nuanced policy discussion. Significant work to that end is already underway in Australia and among our allies. A critical aspect is delineating the differences between cyber operations, information operations and electronic warfare. Efforts must be made to address the commonalities and linkages between them and how they would work to together to create complex effects.

Furthermore, considering the theoretical dimensions of the Army's cyber activities would help to demarcate accountabilities. This is necessary to avoid friction between services and agencies and to ensure that legal and regulatory requirements are met. Importantly, it would also help ensure compliance with international law, including principles such as proportionality and self-defence.[3]

Legislation and policy

The task of applying policy and legislation to Army operations in cyberspace is challenging, as the rapid evolution of technology means that policy frameworks that are based on anything other than broad principles will always be slightly out of date. There's a lack of detailed strategic guidance to the services from the departmental level about cyberspace and operations, and documents such as DWP 2016 don't provide suitable granularity. This should be addressed in association with the other two services. Modernisation in other areas, such as networked vehicles and C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance), also strengthens the imperative for more sophisticated Army cyber capabilities to secure existing assets that now have network vulnerabilities.

In addition, since the Army has to integrate its cyber activities into a variety of existing frameworks, legislation, such as the Defence Act and the Intelligence Services Act, clarity is important to help delineate the roles and responsibilities among different organisations, including the Army, Chief Information Officer Group and ASD.

For these reasons, there's a need to review and refresh the policies informing the Army's activity in cyberspace. However, this process must be handled delicately. The Army must engage in an iterative process with other Defence groups and services to reach a consensus on the required policy reform—a historical challenge.

ASPI comment: Review and refresh policy guidance

Policy guiding the Army's approach to cyberspace and cyber capability should be reviewed and refreshed to acknowledge new threats, the pace of technology, and the service's responsibilities in this area.

Cooperating with service and departmental partners, the Army should work to modernise policy frameworks and develop specific guidance that provides greater granularity on the scope and objectives of its cyber operations.

Integration

Adapting to the requirements of an increasingly connected world involves tasks specific to the Army, but those efforts don't take place in a vacuum. Cyber modernisation is a whole-of-government activity, so the Army must understand how it integrates with broader policy structures.

DWP 2016 gives ASD the overall national lead for cyber operations. However, like all highly valuable capabilities, cyber capabilities can be in short supply, so there'll inevitably be a limit to the capacity and reach of ASD. The Army needs to work with ASD to identify the Army's specific needs and, where possible and appropriate, to develop the capacity to provide organic cyber capability under ASD's policy and authorities. This will rely on a robust relationship between the two organisations.

The Army's reforms must also be conceived within a broader joint force structure, and the priority of modernisation must be to support the coordinated growth of cyber expertise in a joint context. The Vice Chief of the Defence Force is the capability manager for joint capabilities, including cyber capability. Each service is responsible for the operation and assurance of constituent capabilities and should adopt a hub-and-spokes systems approach to role division. However, the utility of these capabilities is undermined if they can't be effectively integrated between services.

Much of the value of cyberspace is tied to intelligence collection and dissemination, so the Army's connection to the Five Eyes community will be an integral part of its cyber activity.

ASPI comment: Integrate Army cyber reforms into existing frameworks and relationships

The Army must work with other Defence groups and services to ensure clarity of responsibilities within the Defence organisation and operational cohesion across the organisation. Relationships with ASD and the Vice Chief of the Defence Force Group will be critical. A strong conceptual understanding of the Army's objectives is necessary for it to meet its needs in the joint context.

When modernising, the Army must also consider its integration with allied forces. Australia benefits significantly from its alliance framework, and those partnerships should be part of the Army's consideration of operating in cyberspace.

Force posture and structure

Agreement on the basic goals that the Army intends to achieve through its use of cyberspace is a prerequisite to developing its cyber posture and must be established before a more agile 'form follows function' approach can be adopted. The Army could pursue several potential outcomes in cyberspace: passive defence, active defence, cyber-enabled information operations, offensive cyber effects, or any combination of them. Once the desired effects have been identified, then policies, technology acquisition and the workforce can be designed to deliver the outcomes in an iterative manner.

ASPI comment: Develop and implement the appropriate force posture and structure to achieve tactical, operational and strategic objectives

The Army should clearly define and articulate its role in Defence's organisational approach to cyberspace. Taking into consideration the other services, ASD and the Chief Information Officer Group, and clarifying how the Army and the ADF will use ASD's offensive capabilities, will help to mature the approach of the Army and the ADF to cyberspace in order to achieve tactical, operational and strategic objectives.

The sections below examine several potential outcomes that the Army could pursue through its cyber operations.

Enabling, securing and assuring

Increasingly sophisticated technology is leading to a growing dependence on network communications, from the front lines all the way back to strategic headquarters. In this paradigm, cyber operations aren't decisive military effects *per se*, but a prerequisite supporter for other operations.

Military decision-makers require a high level of assurance of the accuracy of information provided to inform the planning and command of operations, so verifying and guaranteeing the availability and integrity of information networks is a central priority for the Army's cyber capabilities. First, this involves hardening military networks so that they are more capable of passively withstanding attempted breaches. Second, networks must be resilient and able to retain functionality, limit damage and recover quickly when an incident does occur. Achieving these goals is a substantial task, but provides the necessary level of assurance that information will be timely, relevant and accurate. This must be achieved across the Army's own tactical and operational networks, on current and emerging platforms, and on the strategic Defence information networks that Army-owned networks and platforms interlink and exchange information with.

There's an argument that true network defence can't be achieved only through this kind of passive reactionary posture, and that a more proactive strategy of ongoing engagement with the threat landscape is required. A comparison can be made to the physical world, where even defensive action normally involves action 'beyond the wire'. In this sense, the concept of active defence, including patrolling and occupying strategic terrain, can be applied in principle to cyber operations.

This paradigm necessitates engaging adversaries in contested spaces and anticipating incidents rather than simply relying on the network's capacity to withstand attacks or recover after the fact. Achieving this requires a different set of policies, technologies and skills. For example, it demands 'hunt teams', red teaming, penetration testing and intelligence collection on adversary systems, drawing on capabilities that for financial and policy reasons the Army doesn't, or can't, generate and sustain organically.

ASPI comment: Focus on protecting information

Modern networked military capability, from the individual soldier up to major formations, depends on the exchange of information to achieve the maximum possible effect at the least cost. Because of this, the Army should prioritise the protection of its information and work within Defence to defend deployable and strategic networks.

Doing so assures the confidentiality, integrity and availability of information needed by commanders at all levels to make informed choices and take advantage of decision superiority. The principle of resilience should inform the Army's approach to the security of its information.

Undermining adversary decision superiority

In this paradigm, cyber operations are conceived not just as a mission enabler, but as an independent and direct line of effort. Cyber effects have a wide variety of possible applications, but their potential to undermine an adversary's capacity to make choices at the most basic level is particularly valuable. By combining approaches that assure the accuracy of information provided to friendly forces with operations to degrade the quality of information used by an adversary, the Army can achieve decision-making superiority over the adversary. This acts as a force multiplier, allowing commanders to more effectively target critical nodes and achieve the maximum effect at the least possible cost.

Australia's possession of offensive cyber capabilities was acknowledged by the Prime Minister at the recent launch of Australia's Cyber Security Strategy, and described as providing 'another option for the Government to respond'.[4] However, DWP 2016, released only a month earlier, did little to elucidate the ADF's cyber posture and referred only to defensive needs, skills and technology.[5] This discrepancy highlights the importance of establishing clarity within Defence about the nature of Australian cyber operations.

ASPI comment: Consider and pursue opportunities to undermine adversary decision-making

The opportunity to undermine adversaries' information networks to multiply the information advantage offered by assured networks shouldn't be overlooked.

The Army should work with its partners in Defence, particularly ASD, and our allies to understand how to capitalise on these opportunities.

Non-linear effects

Cyberspace can also be considered as a medium through which to influence people as part of information warfare. Inspired by Warden's 'five rings' theory,[6] this approach targets one of an adversary's 'centres of gravity': the population. The Army can exploit modern connectivity for more effective dissemination of public messaging in psychological operations.

In fact, this tactical effect is one of the key outcomes in cyberspace currently being successfully achieved by violent non-state actors. The savvy use of social media for the propagation of radical content has played a crucial role in such groups' spread of terror and in their recruitment rates. This approach requires the Army to engage with adversaries in this context, degrade their popular support and reinforce positive narratives. The strategic nature of these activities means that this is likely to be in the form of Army input to a national effort rather than discrete Army use of such capability. The Army's existing intelligence and information operation capabilities would be a significant enabler of Defence's ability to plan and integrate non-linear effects, especially when coupled with the technical capability of other Australian and allied partners.

Cybersecurity incidents affecting the 2016 US presidential election campaigns indicate that governments are now also seeing value in such a strategy. The Australian Cyber Security Centre's *2016 threat report* acknowledges a growing pattern of malicious actors using cyberspace 'to seriously impede or embarrass organisations and governments—equating to foreign interference or coercion'.[7] The official attribution of malicious cyber activity to the Russian Government by the US Department of Homeland Security and Office of the Director of National Intelligence indicates that powerful global players are incorporating such information operations into their statecraft.

ASPI comment: Select and implement a coherent approach to cyberspace

The Army should consciously consider the full spectrum of approaches to cyberspace and determine which provide the most value to its operations. It must identify the capabilities that it should develop organically and those that can be provided more effectively by other groups, services or allies. A suitable force posture and structure design to meet those requirements should then follow.

Allied and adversary approaches

At a time of rapid change in adversary and allied approaches to cyber operations and security, it's vital that the Army considers its posture in cyberspace in the context of the cyber activities of Australia's international peers. The militaries of the US, China and Russia are rapidly developing sophisticated cyber capabilities and competing for primacy in the digital domain. Allied and adversary approaches provide an example, but usually at a scale significantly different from Australia's, and the Army's choices must be grounded in the practical reality in which it operates.

The Army should gain a detailed understanding of the different cyber policies, organisational structures and technologies used by various militaries. Such an evaluation would illuminate examples of best practice, while identifying organisational mistakes to be avoided.

Importantly, the evaluation would also provide an indicator of the pace at which other states' militaries are adapting their operations to exploit the benefits and vulnerabilities of cyberspace. This will enable the Australian Army to make informed decisions about both the nature and speed of its cyber reforms and offers an important starting point from which to conceive the cyber future of the Army.

Retaining connectivity and independence

The Army must strike a delicate balance between increasing its exploitation of cyberspace and developing an operational dependence on it. There's a risk of generating a posture of complete reliance on networked capabilities because of their undeniable benefits, but the Army mustn't lose sight of the importance of operational resilience and the ability to sustain other capability if cyber capabilities are denied or disrupted (as in US Navy exercises in which space-based assets are denied). Developing and maintaining the capacity to undertake operations differently when necessary is an essential part of the Army's defences.

Required technology

These policy decisions take place in a context of nearly constant technological change. Accelerating connectivity suggests a future operating space based on a level of connectivity barely imaginable today. There's an imperative to anticipate these changes and appropriately future-proof the Army's technology acquisition strategies to support the sustainability of its cyber operations.

Technology is evolving quickly. As soon as a new capability is introduced, a vulnerability or counter-capability is developed, and this cycle is only likely to speed up. This is at direct odds with the traditional nature of the Army's procurement process. The conventional approach to asset acquisition—at least for major acquisitions—is tightly regulated, rigid and designed to address multiple decades of military need in advance. That style of procurement simply doesn't work for many C4ISR applications. Not only does it mean that the Army's in danger of missing out on beneficial technologies as they become available between procurement cycles, but it also leaves assets vulnerable as the capabilities of adversaries adapt and become more advanced. The problem is that networks are only as strong as their weakest link: a few unaddressed vulnerabilities can render the entire system insecure.

Cyberspace will change significantly over the next 10 years, and networks are likely to become more complex and less centralised. It's estimated that by 2025 average data speeds will have increased to 1.3 gigabytes per second in major population centres, and most data will be stored in, or move through, the cloud. The growth of open Wi-Fi networks and the increase in device numbers will allow increased use of Wi-Fi meshing and multi-hop networks. This potential future technology landscape will require markedly different approaches from the Army.

It's critical that the Army monitors technological advances and changes in the threat landscape and uses that awareness to inform and shape the near-term requirements of its cyber capabilities. Shortening the acquisition cycle and speeding up the flow of technology from initial development stages to operational deployment will make better use of each technology before it's overtaken, thus representing a better investment.

To achieve this, the Army should prioritise modular design features in its technology development. Establishing this model in discussion with industry partners will enable security considerations and interoperability with existing and future systems to be built into the acquisition cycle. This will make the acquisition process more flexible and facilitate an incremental spiral upgrade process.

This proliferation of capabilities will need to be supported by increasing bandwidth from strategic bearers. Long-term investment in fundamental communications infrastructure is essential to capitalise on new developments and enable effective reach-back capabilities. Therefore, the Army must simultaneously be flexible in individual capability design and forward thinking in terms of the supporting frameworks that such technologies will require.

These changes are necessary in order to generate an evolutionary sustainment capability and reconcile the Army's technology acquisition with the reality of cyberspace.

ASPI comment: Adjust the acquisition process to reflect the reality of technological development

Procurement needs should be informed by changes in the threat landscape, and capability take-up should be rapid and based on a modular upgrade system, with maximum use of commercial and military off-the-shelf hardware. Although the task is challenging, the Army needs to anticipate and mitigate the near-term redundancy of certain capabilities so that it can keep pace with rapid developments on the ground.

The Army must embrace a spiral procurement process in order to exploit the benefits and avoid the dangers associated with the iterative nature of cyberspace and cyber technologies. Acquiring tools with temporary utility in mind will prevent the accumulation of legacy technologies and retain the agility to upgrade. Increasing the speed and agility of the procurement process will also require effective project management feedback loops and the ability to acknowledge and address shortcomings as they arise.

This iterative nature also needs to be reflected in the acquisition process. Streamlining reviews, reducing timelines and improving cooperation between users and acquisition staff would prevent the Army from receiving platforms that are already out of date.

WORKFORCE STRUCTURE

Redesigning force structure and attracting and retaining personnel with the necessary skills are essential for ensuring the Army's ability to achieve its cyber goals. It currently faces a severe shortage of skilled personnel in a range of technical and professional categories, which is limiting its ability to adapt to new challenges.

Design

Addressing the challenge of staffing the Army's needs requires careful consideration of the most effective management architectures and distributions of responsibility. While there may be a role for specialised single-service and joint capabilities within the ADF and Defence, cybersecurity can't be isolated as a niche task within the Army. The nature of the job necessitates a broad skill base across the Army, in which cybersecurity is normalised within all activities. This requires all Army personnel to have some level of training on cyber issues and skills, beginning in *ab initio* training and continuing throughout their careers. This should be a training priority for all personnel due to the significant risk that cyber incidents pose to operational efficiency and security.

Addressing the issue comprehensively demands a complex ecosystem of skilled individuals—not just engineers, mathematicians, computer scientists and hackers, but also policy experts, intelligence professionals and risk management specialists. The Army's requirements for specific skills are currently unclear, and it needs a stronger awareness of the skills it needs, and in what quantities, to ensure that education, recruitment and retention initiatives are focused on areas of critical need.

For roles requiring more in-depth knowledge and skills, integrating cyber professionals and upskilling existing personnel throughout the service will be important. It will require fresh thinking and approaches to personnel recruitment and retention.

The Army's need for these skills is time sensitive, so this human resources dilemma must be addressed from the bottom up. New administrative processes, such as the creation of new trades or new courses at the Defence Force School of Signals, are important and should take place. However, waiting for them before implementing changes on the ground would cause an unacceptable delay in the Army's adaptation to networked conflict. Responses to this challenge must be practical, reasonable and grounded in the context of resource shortages across many critical trade categories in the Army.

Developing skills: existing personnel

The Army should review the distribution and application of skilled individuals in its existing workforce. Assessing and understanding the full capability range of staff will help to ensure the most efficient use of human resources. People with valuable cybersecurity skills that aren't currently being exploited should be repositioned to contribute to the effort, and obstacles to their movement and promotion should be removed to encourage retention. Informed leadership and an agile workforce can enable better staffing decisions.

Proactive efforts should also be made to raise the knowledge and improve the abilities of personnel already in cyber roles. Continuous training cycles and drills, up to and including brigade-level exercises, should be used to upskill the service and keep it up to date on technological opportunities and challenges.

Developing skills: reserves

Re-imagining the design of the Army Reserve may be an alternative strategy for augmenting the Army's cyber capabilities. The creation of new dedicated cyber reserve units, constituted by new recruits and existing reservists with cyber skills, would supplement its existing personnel. This approach has recently been adopted by the British Ministry of Defence, which created the Joint Cyber Reserve in 2013.[8]

However, there are significant obstacles to this approach that mean the Army shouldn't rely on it as a solution to its personnel shortages in the long term. While the reservist approach would offer more operational capacity in certain scenarios, it might not supply the additional long-term capacity required.[9]

Also, it's often understood that the appeal of being is a reservist is the chance to experience the 'Hollywood' aspect of military service, including the challenge of the practical training. However, this approach would be designed to help skilled cyber reservists bypass the rigorous training requirements in order to expedite their integration into the service and capitalise on their abilities immediately. The necessarily 'civilian' experience as a reservist may undermine the market appeal for registrations in the first place.

Recruitment

The Army should also broaden its recruitment horizons in order to fill the growing need for cyber skills in the service. Its current approach to recruitment is understandably constrained by filters such as security clearances, educational backgrounds and experience. This funnel is currently excluding certain demographics that may possess the valuable attributes needed for cyber operations.

The Army will need to recruit from a broad base of educational backgrounds and skills. To meet this challenge, the recruitment profile needs to become more inclusive and open in order to accommodate the diverse backgrounds of cyber-skilled individuals, and process them faster.

Moreover, many individuals who possess highly valuable attributes for this field might not necessarily have taken the traditional path through higher education or ever considered a role (technical or policy) in the Army. The absence of training shouldn't remain a significant barrier to recruitment, since raw capability is rare and talented individuals can easily acquire the necessary qualifications.

Education

Given that there's an acknowledged shortage of cyber-skilled individuals across all sectors, the Army should deepen and broaden its collaboration with educational institutions in order to generate a sustainable pipeline of cyber talent.

Investing time and resources in the establishment of relevant education courses will help to produce individuals with the right cyber skills for the Army. Unfortunately, some IT courses are still relatively theoretical, with a mathematical focus, and while that approach is valuable it's not sufficient, as it doesn't provide the practical skill development that's essential for military cyber operations. The training process should include collective response action training, exposure awareness and red team exercises. Syllabus design must be informed by the Army's operational requirements and, to achieve that, the Army needs to establish strong consultative dialogues with educational institutions.

Courses can also be co-designed with industry partners to ensure that the students benefit from technical experience and the best practical knowledge. Boosting connectivity between the Army, education and the private sector will help to amalgamate the knowledge of academics and the experience of industry to provide people with the right cyber skills.

This approach should be implemented across a broad variety of institutions. The Army currently has a strong engagement with the University of NSW at the Australian Defence Force Academy; however, expanding that engagement and replicating it with more universities and additional educational institutions may be important in order to diversify and increase the delivery of cyber skills to the Army as demand changes.

In the light of the national deficit of science, technology, engineering and mathematics (STEM) students, the Army would also benefit from taking a proactive role in promoting STEM studies more broadly. It should encourage young individuals to engage in STEM classes in coordination with existing initiatives, such as those outlined in the National Innovation and Science Agenda and the Cyber Security Strategy.[10] The establishment of youth competitions, internships and cadetships is an important way of capturing potential talent before their attention gets taken elsewhere. Specifically, encouraging the representation of women in this field through merit-based scholarships will support the strength and balance of the pool of STEM talent from which the Army can draw. A focus on practical network defence skills should be a guiding principle for the design and implementation of these programs.

Education initiatives won't deliver cyber capability into the Army overnight; setting up effective courses and moving people through them takes time. However, initiating this process is an essential element in following up on near-term measures with a sustainable workforce generation program.

Company contracts and lateral transfers

There would be benefit in deepening the Army's cooperation with the private sector. In scenarios in which it can't provide the required skills internally, it should contract out certain roles to experienced individuals in industry. Some companies have been operating in this space for significant time and have already developed mature and sophisticated methodologies from which the Army could benefit.

Moreover, in a context of global cyber skills shortages, this allows the Army to benefit from some of the talent that it may inevitably miss out on because of tough competition with better paying private-sector organisations. This approach is not a long-term substitute for bolstering indigenous capabilities, but may provide critical support and continuity at times of transition.

Attracting talent

Because of national skills shortages, attracting cyber personnel will require additional attention to how jobs are marketed. Unfortunately, the Army is competing with the private sector to attract the services of in-demand cyber-skilled people.

There's significant intellectual capital and historical tradition associated with current titles and job descriptions in the Army. There's also a certain resistance to the term 'cyber' due to poor levels of understanding and some sensationalism. However, occupational terminology such as 'cyber specialist' has proven to successfully attract both people and resources. Given the Army's critical need for these individuals, it will be necessary to integrate researched understandings of the job market into the Army's rhetoric when it comes to recruitment.

Retaining skills

The Army should prioritise the retention of skilled cyber personnel. In practice, skill sustainment is even more important than skill generation, as each individual lost has already cost the Army significant funds in training resources. Unfortunately, management issues within the Army and the attractiveness of private-sector wages are resulting in a high rate of attrition of cyber-skilled people. The lack of necessary frameworks to support them through their career evolutions is resulting in valuable human resources leaving the service. It's necessary to create better processes to integrate their skills into the service in a permanent way. Leadership needs to clearly demarcate cyber career pathways in the Army, emphasising longevity, rewards and the potential for promotion.

ASPI comment: Invest time and attention in addressing the Army's deficit of cyber-skilled individuals

The Australian Army should take immediate action to address its shortage of vital cyber expertise. It should seek to upskill existing personnel, broaden recruitment demographics, capitalise on reservist talent, take advantage of private-sector knowledge through contractors, and collaborate with educational institutions to increase the volume and diversity of people prepared to contribute to its cyber operations. This should be grounded in a strong understanding of what skills the Army needs, and in what quantities.

The elevation and maintenance of basic cyber awareness across the Army is necessary to support the development of a strong cybersecurity culture. Every member of the Army should have a basic understanding of cybersecurity threats and the need for due caution, for example about suspicious emails and the need for strong passwords. This will also support the identification of people with the aptitude to acquire more advanced cyber skills.

All commanders must be aware of the potential opportunities and risks now that that cyberspace permeates all military operations.

CONCLUSION

The Australian Army understands that cyberspace represents both a significant risk to operations if threats are not managed and, simultaneously, the opportunity to enhance its capability if cyber operations and land power are successfully combined. The Army also understands that there are some significant changes that must be made to its organisation and practices to ensure that it embraces the potential offered. Like the rest of the Defence organisation, it's in the challenging position of having to adapt to a rapidly changing operational environment in cyberspace. Skills shortages also require immediate action to remediate existing vulnerabilities. At the same time, the Army must conduct a careful and considered analysis of the concepts that will underpin its transformation into a digitally secure land force to ensure an appropriate force posture and structure aligned with the needs of the whole ADF.

The Army should build consensus within itself, the broader ADF and the Defence organisation about what its responsibilities in cyberspace are, what it's seeking to achieve, and how it will do it with the support of or in support of Defence. It also needs to establish what capability acquisition and human resources doctrine it will adopt in this effort. Doing so will make the necessary changes easier to achieve, accelerating the development of the Army's digital land power.

NOTES AND ACRONYMS

Notes

1 Australian Army, *Our future*, no date, online.

2 M Clifford, M Ryan, Z Hawkins, *Mission command and C3 modernisation in the Australian Army: digitisation a critical enabler*, ASPI, Canberra, 2015, online, M Davis, *ADF capability snapshot 2016: C4ISR—winning in the networked battlespace*, ASPI, Canberra, 2016, online.

3 UNGGE (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security), report A/70/174 to the UN General Assembly, 2015, online.

4 M Turnbull, 'Launch of Australia's Cyber Security Strategy, Sydney', transcript, 21 April 2016, online.

5 Department of Defence, *2016 Defence White Paper*, Department of Defence, Canberra, 2016, online.

6 John A Warden, 'Air theory for the twenty-first century', in Karl P Magyar (ed.), *Challenge and response: anticipating US military security concerns*, Air University Press, Maxwell, Alabama, 1994.

7 Australian Cyber Security Centre (ACSC), *2016 threat report*, ACSC, Canberra, 2016, online.

8 UK Government, 'New cyber reserve unit created', media release, 29 September 2013, online.

9 Defence Reserve Service (Protection) Act 2001, online.

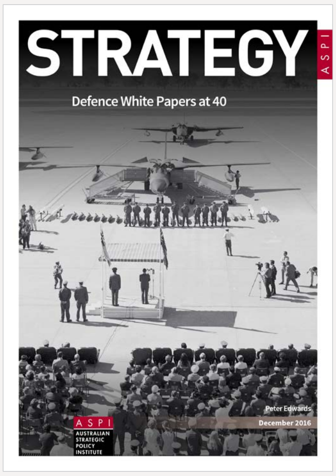
10 Australian Government, 'Young Australians', *National Innovation and Science Agenda*, 2016, online.

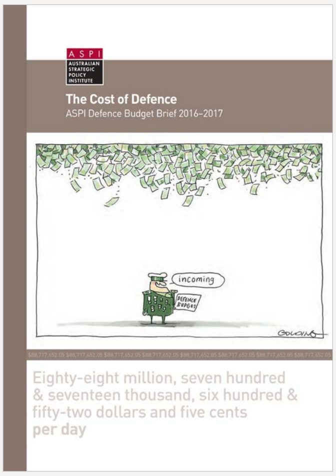
Acronyms and abbreviations

ADF	Australian Defence Force
ASD	Australian Signals Directorate
C4ISR	command, control, communications, computers, intelligence, surveillance and reconnaissance
DWP 2016	2016 Defence White paper
STEM	science, technology, engineering and mathematics

Some previous ASPI publications

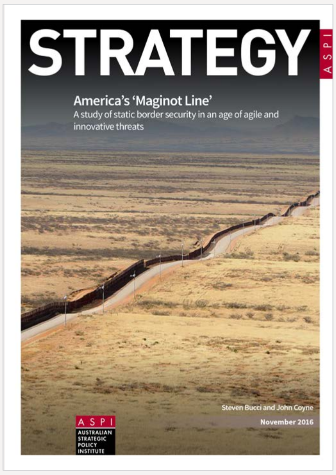
STRATEGY
ASPI
The eagle has landed
The US rebalance to Southeast Asia
Peter Chalk
June 2016
ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE


STRATEGY
ASPI
Defence White Papers at 40
Peter Edwards
December 2016
ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE


ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE
The Cost of Defence
ASPI Defence Budget Brief 2016–2017
incoming
DEFENCE BUDGET
Eighty-eight million, seven hundred & seventeen thousand, six hundred & fifty-two dollars and five cents per day

STRATEGY
ASPI
Agenda for change 2016
Strategic choices for the next government
Edited by Malcolm Davis
June 2016
ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

STRATEGY
ASPI
Why Russia is a threat to the international order
Paul Dibb
June 2016
ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE


STRATEGY
ASPI
America's 'Maginot Line'
A study of static border security in an age of agile and innovative threats
Steven Bucci and John Coyne
November 2016
ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Digital land power

The Australian Army's cyber future

ISSN 2200-6648