Australia's defence and national security: how Defence is enhancing Australia's cyber resilience

A paper based on an online presentation to the Institute on 27 July 2021 by

Major General Susan M. Coyle, CSC, DSM
Head, Information Warfare Division, Department of Defence[1]

Information and cyber today constitute a 5th warfighting domain. This domain can be either an enabler for the traditional sea, land, air, and space warfighting domains or the primary domain on which the other domains are critically dependent. Cyberspace is software-defined, virtualised and non-physical, but resides upon physical hardware, so can be targeted with kinetic effects. Cyber warfare is influenced by its domain characteristics: speed, reach, span of consequence, scale of effects, state of flux, complexity and the challenge of attribution. A Defence cyberworthiness framework seeks to ensure warfighting capabilities survive against adversary actions in cyberspace across all phases of war, including grey-zone operations.

Key words: cyber resilience; cyberspace; cyber warfare; cyberworthiness; information and cyber domain; information warfare; national security; survivability; 5th warfighting domain.

In June 2021, the Department of Defence (Defence) advised the Senate Estimates Committee that Defence is a "target for persistent cyber threats and attacks ranging from issue-motivated individuals and groups, through to nation-state actors and trusted insiders" (Pearson 2021). How, therefore, as Head of Information Warfare, can I enhance our cyber resilience in the context of Australia's defence and national security?

Before I get to what successful resilience looks like, I will take you through the vocabulary we are developing for what we call the 5th warfighting domain – the information and cyber domain.

Information Warfare

What is information warfare? In April 2021, at the Chief of Army Symposium, in the context of discussing the relationship and interconnectedness between the information and cyber domain and the land domain, I said that: "Information warfare is the contest for the provision and assurance of information to support friendly decision-making, whilst denying and degrading that of adversaries" (Coyle 2021).

Information warfare is timeless. It was as equally applicable in ancient times, as attested by Sun Tzu in the widely known *Art of War* (Sun Tzu 1963), as it is in the new digital age, where a pervasive cyberspace allows the transmission and manipulation of information to span the globe within milliseconds.

The character of future warfare will not resemble that for which we have traditionally prepared. Indeed, that future has already arrived. We need to understand better, and rapidly drive towards, a new vision of what it means for Defence to contribute information and cyber domain support for our national and military objectives. We need to understand faster, manage our cyber and operational risks, make superior decisions and act at a new speed of war.

Defence capability development is now more sophisticated, particularly in our approach to the *information* aspect of our recently declared 5th warfighting domain – but that is not the focus per se of this paper. That focus is *cyberspace* – specifically how we enhance its resilience in support of our mission. Towards this end, in the Joint Cyber Directorate, my team and I are addressing how Defence capabilities will operate in a contested and hostile cyberspace environment across the "shape, deter and respond" continuum[2] in a rapidly evolving strategic environment and threat landscape.

Cyberspace

What is cyberspace? We think of cyberspace as the global digital environment of partitioned and interdependent logical and hardware infrastructures, networks, systems, information and services. This definition is not constrained to the internet, computer systems and telecommunications networks (information and communications technology – ICT). Much of cyberspace is not an interdependent network, and is

[1]Email: susan.coyle@defence.gov.au

[2]The "shape, deter and respond" continuum is a reference to Australia's *2020 Defence Strategic Update* (Defence 2020a) which replaced the strategic defence framework set out in the *2016 Defence White Paper* (Defence 2016) with three new strategic objectives: to ***shape*** Australia's strategic environment; to ***deter*** actions against Australia's interests; and to ***respond*** with credible military force, when required.

not limited by ICT alone, nor does it stand separate from the electromagnetic spectrum and electronic warfare. Cyberspace explicitly includes what we have traditionally considered as separately-nested operational technologies or within traditional warfighting platforms, like ships, tanks and aircraft. We also recognise that the majority of cyberspace is now software-defined, virtualised and non-physical. Cyberspace ultimately resides upon a physical hardware layer, which also means we can target it with kinetic effects (*i.e.* military action, including firepower and lethal force).

Defence protects a complex cyberspace environment of over 1000 networks comprising more than 320,000 endpoints and devices. The total investment in strengthened information and cyber domain capabilities is to be approximately $15 billion over the next decade, and includes $5 billion for resilience improvements, $1.4 billion for strengthened defensive cyber and deployed combat platforms, and $1 billion for security upgrades (Pearson 2021).

We recognise that for Defence and our mission, we need to describe cyberspace with fidelity to frame a unified construct of manoeuvre in and through cyberspace. We recognise that we need to consider the full breadth of scope and global digital supply chains if we are to achieve situational awareness, decision superiority, and agile command and control of our cyber domain operations and activities.

Importantly, this thinking allows us to get after the information aspect of the 5th warfighting domain in a way that spans horizontally the entire Defence enterprise and its mission, and that recognises that cyberspace is loosely, but not literally, coupled to it. This thinking also allows us to recognise the rising prevalence of sub-conflict 'grey-zone' operations as a part of a new strategic setting and the role that Defence plays. We know that information and cyber is now both a primary domain for warfighting in its own right and a domain on which the traditional sea, land, air and space warfighting domains can be critically dependent. This thinking allows us to address the risks and exploit the opportunities presented by cyberspace for military advantage.

The character of cyber warfare, how we project offensive power and also operate to defend our cyber terrain, is influenced, in particular, by its key domain characteristics: accelerated speed; global reach; the span of consequence and strategic risk considerations; the scale of cyberspace effects, the constant state of which is fragile and inherently complex; that cyberspace can be reconfigured or destroyed; and the challenge of attribution and confidence on account of its fundamental uncertainty. One aspect of its warfighting domain characteristics is the concept of cyber resilience.

Resilience

What is resilience? Since the launch of the *2020 Defence Strategic Update* (Defence 2020a), there has been significant focus on the Government's direction to enhance the lethality of the Australian Defence Force (ADF) for high-intensity operations, especially as to what this means for Defence's kinetic options through area denial and long-range strike capabilities. This is understandable as increasing our resilience and self-reliance means that Australia is positioned to make an even stronger contribution to regional security and to our alliance with the United States. This focus, however, looks past an important part of lethality – the ability of our force elements to survive. Survivability is a key concept that underpins lethality as it allows systems to remain mission capable, maintain their presence, and continue to deliver effects (Coyle 2021). We are ensuring survivability is a key consideration for all Defence capabilities.

Defence (2020a) also stated that Defence should move to contest in the 'grey-zone', taking a persistent engagement posture short of war. Defence also must be capable of conducting and responding to information warfare and its effects as part of high-end conflict (Coyle 2021).

Let us now consider what resilience means in a non-technical sense. Various dictionary sources have described it as: the capacity to recover quickly from difficulties; tough yet elastic; the ability to spring back into shape; and the ability to respond to, or recover readily from, disruption, shock or crisis.

These could be equally considered in terms of people, processes and technology. Indeed, we need to consider all three for Defence, as resilience must mean our capacity to recover must be strong, our layers must be deep, and we must be able to fight even when hurt. Resilience means survivability.

Cyber Resilience

We now arrive at the core question I have been asked to address in this paper: what is cyber resilience? I will answer this not from the perspective of what will be done at a technical level, but from what that means for Defence and our capabilities across all five warfighting domains. And that answer is the word: 'cyberworthiness'.

ADF operations are the headline of the work government tasks Defence to undertake. It is what we focus on, what we train for, and for what many of us in uniform signed on. But in the realm of cyberspace and the critical dependency of traditional domain operations on it, a resilient foundation is vital. For us, this means a secure, assured and survivable cyberspace and the ecosystem that surrounds it. That, in turn, postures us to maintain the confidentiality, integrity, availability and survivability of the information resident in and through cyberspace. We must prioritise and focus our efforts through the lens of our missions and tasks. Without this, our house is built on quicksand or will be overrun with things we do not need or, more to the point, no longer need, and our operations will never be as effective as we designed them to be.

To that end, the ADF has developed a concept called 'cyberworthiness'[3]. The term itself may seem vaguely familiar – each of the ADF Services have a worthiness framework that supports technical regulation and assurance in their respective environments. For example – is a Royal Australian Air Force aircraft 'airworthy' to fly or not? We have taken this concept and applied it to the cyberspace environment – no simple task! But it is necessary.

Organisationally, our span of cyberspace terrain – which I said before includes a blended information-communications, technology-operational, technology-electronic warfare landscape – is highly complex, difficult to map and can represent a largely unmanaged attack surface for Defence if we are inattentive. This, coupled with very adaptive and malicious cyber threat actors who are presenting a persistent threat to current and future Defence capabilities, means we can no longer address this issue as we have traditionally. And this is not something we can do alone. Our government colleagues and industry partners are key enablers of any success we will achieve in this space.

Cyberworthiness, therefore, encompasses assurance of cyber security and extends this to include the fundamental inputs to capability. Cyberworthiness facilitates an assessment of cyber security risk to mission assurance, in accordance with the capability managers' operating intent, and is necessarily context dependent.

Put less formally, the ADF cyberworthiness framework is designed to ensure our warfighting capabilities are survivable against adversary actions in cyberspace across all phases of war, including sub-threshold phases such as persistent contest and grey-zone operations and activities. It is, in essence, a risk management and continuous improvement framework, enabling the ADF to effectively manage our risk in cyberspace as we execute our mission.

Cyberworthiness is a key element of defence preparedness, ensuring capability fitness-for-purpose for those who wish to employ it – our Government, Chief of Defence Force or Chief of Joint Operations.

Worthiness is not just about security. Traditional cybersecurity is focused on activities designed to ensure the confidentiality, integrity and availability of systems. Cyberworthiness is rooted in survivability – business continuity, in corporate terms – and assurance of our mission. We view our capabilities as holistic ecosystems, not just bundles of technology, and our worthiness in cyberspace must address the whole rather than the part. Unsurprisingly, therefore, our future cyberworthiness governance framework has been scoped across three key pillars – people, processes and, of course, technology.

When you pause a moment to think about that, across the span of defence capabilities, and through the whole of the life cycle from concept to operation and decommissioning, the breadth of what Defence needs to ensure is cyberworthy – what we need to ensure is resilient – is staggering. But if we are good at anything, Defence is good at planning!

My team and I within Joint Capabilities Group, along with all Services and Groups across the Defence enterprise, are leading a number of people-based and process-based initiatives to advance some of the aspects of what it means to contribute to what we call the Joint Force and its relationship with uplifting Australia's sovereign capabilities.

We have commenced a pilot, designing a fit-for-purpose maturity model based on global best practice, creating solutions that service the unique defence environment, while also enabling industry to interact with, and support, our efforts in the most robust and mutually beneficial manner. We have commenced a limited implementation internally, selecting within each of Navy, Army and Air Force a focus area to align our practices to the model at the coalface of capability. We also are tackling the broader strategic problem of enterprise-wide implementation across the lifespan of our capabilities, integrated with our industry partners and allies.

People and Organisations

Defence continues to face a significant challenge in the recruitment and retention of a skilled cyber workforce, due to the high market demand and global shortage of cyber practitioners. Workforce resiliency is a vital priority for us. We, therefore, are focusing on what we can uniquely offer and features that may be of deciding value to the sort of people we need as our future operators and leaders of our joint cyber workforce. These include three aspects:

- ***mission***: our cyber workforce has access to unique technical or leadership responsibilities in Defence operations or activities that defend and keep safe our cyberspace terrain or project offensive effects;
- ***service***: the patriotic pride associated with placing the security and interests of our nation and its people first and above self; and
- ***culture***: being a part of a team of Defence people who strive to behave in a way that lives our values of Service, Courage, Respect, Integrity and Excellence (Defence 2020b) – remember, we all volunteer to serve our nation.

Defence has committed to increasing the ADF cyber workforce by 230 positions by January 2024. Yes, we are hiring! I therefore encourage people who gain strength and excitement through the prospect of working for an organisation with the above features of mission, service and culture to please keep us in mind as your career progresses or, indeed, make an appointment with Defence Force Recruiting now!

[3]Note: Australian Defence – Future Cyber Concept Operations proposes that the current Australian Defence Force Services only scope of cyberworthiness be extended Defence-wide and, also, to the extent of dependency, be extended to industry.

ADF Cyber Gap Programme: For those studying a cyber-related tertiary course, we have another initiative underway. Government has asked Defence to provide leadership in uplifting Australia's national cyber workforce through the ADF Cyber Gap Programme, where benefits flow to Defence and the nation. This programme, led and managed by my staff, in itself is a case study in how people have come together from all areas from which Defence needs to draw its cyber people, to deliver an integrated cyber workforce capability. It is led by an ADF officer supported by two Australian Public Service full-time employees of Defence, contractors from industry with specific expertise, and multiple Defence Force Reserves from Navy, Army and Air Force. The ADF Cyber Gap Programme, over the next three years, will support the skilling and mentoring of 800 Australians, to advance their cyber employment and contribution towards our national security mission. We wish to identify and recruit the best and brightest people into a lifelong career stream that, skilfully and speedily, will shape and control an increasingly software-defined, artificially-intelligent cyberspace.

Defence Cyber College: We also recently broke ground for the construction of a joint information warfare facility at HMAS *Harman* in Canberra, which is scheduled for completion in February 2023. It will house the soon-to-be-established Defence Cyber College which will enable full-spectrum cyber training for the Defence cyber workforce.

Cyber Units: Another initiative that the ADF has undertaken, which provides an organisational platform for us to further build upon, is the establishment and operational service contributions from four new organisations: Joint Cyber Unit; Fleet Cyber Unit – Navy; 138 Signal Squadron – Army; and No. 462 Squadron – Air Force. These are our front-line units, able to deploy and operate on domain and context-specific cyberspace terrains. They also work in combination and co-ordination with the successful Defence Security Operation Centre to defend strategic and deployed environments in order to maintain Defence's mission continuity in a contested cyber environment. They are not solely responsible – it requires everyone in varying degrees to ensure we are resilient. Our new journey has begun to assure our mission and our lethality at the core of our capabilities, fit for the strategic setting in which Australia now finds itself.

Cyber Resilience, Industry Dependencies and Participation

So, how does cyber resilience map to industry dependencies and participation? As I emphasised earlier, we cannot do this alone. Industry is a key component of our fundamental input to capability. We need industry and will engage with industry in new ways that underpin our future concept for cyberspace operations and activities.

We are critically dependent upon the global digital supply chain and how that passes through and into what we call our internal 'Blue-Terrain' – that which is owned and managed inside our firewalls or network edge, to use an historic concept of scope demarcation.

Defence has a critical dependency on defence industry as part of its cyberspace environment. For Defence, commercially-owned cyberspace – where the accountabilities for cyberspace infrastructure and systems lie outside Defence – is what we call 'Grey-Terrain' and for which we must account in our mission-planning and capability development.

Anything short of a shared appreciation of commercial industry-risk and Defence mission-risk will create exploitable gaps in a specific cyber ecosystem whose vulnerabilities are higher because of their high value as an adversary target. I also can see a future where industry's status as a core Defence cyber-dependency could combine with Defence's significant procurement power to develop a Defence-industry cyber ecosystem which generates competitive advantage for industry and the Australian Government alike.

Defence is urgently looking to a new future out of necessity and, as Head of Information Warfare, how we communicate what that looks like to industry is a key focus for me and my team.

Cyber Resilience and the Defence Mission

What does cyber resilience in the context of Australia's defence and national security mean? Quite simply – it means we can!

It means we can have a Navy ship sail where it is tasked to go and perform the missions for which its capabilities were designed – whether they be freedom of navigation, contributing to regional stability efforts with our regional friends and allies, through to, if it comes to it, high-end conflict.

It means an Air Force aircraft is able to take off and undertake its assigned mission, deploying the effects for which it was designed.

It means the Army can operate with the use of cyberspace that may be heavily contested and, indeed, heavily degraded, but it and Army are resilient and are able to continue the fight and prevail.

And finally, it means that, as government (through our Secretary and Chief of the Defence Force) reprioritises and resets whenever needed, we are agile and able to respond in accordance with our national and military mission – and, therefore, we can map that task to our cyberspace terrain and reprioritise our capability development and operation of it.

That is how we are contributing, resiliently and urgently as we must, to a Defence mission that is changing to meet newly-arisen and future national security requirements.

Conclusion

We, collectively, must rise to the resilience challenge. Robust partnering arrangements between Defence services and groups, and our defence industry,

upon which we are critically dependent, need to pivot to align to our new understanding of the warfare domain characteristics of cyberspace and to keep pace with the new speed of war.

I appreciate this is no small challenge, but it is one to which we must rise. Collectively, we need to grow our capacity to reconstitute, regenerate and continue to evolve, at speed, for our cyberspace mission. Successful resilience means survivability of a cyberworthy Australian Defence Force.

The Author: Major General Susan Coyle is Head of Information Warfare for the Australian Defence Force. Born in Kyogle, NSW in 1970, after gaining a degree in science at the Australian Defence Force Academy, she graduated from the Royal Military College in 1992 into the Royal Australian Corps of Signals. She has worked at the tactical, operational and strategic levels in a variety of command and staff appointments, including Commander Joint Task Force 633 (Middle East), Commander 6th Combat Support Brigade, inaugural Commander Task Group Afghanistan, and Commanding Officer 17th Signal Regiment. She was awarded a Distinguished Service Medal as the Deputy Commander JTF 636/Commander Task Group Afghanistan, and a Conspicuous Service Cross as the Commanding Officer 17th Signal Regiment. She holds a Master of Strategic Studies from the United States Army War College, a Master in Organisational Development and Strategic Human Resource Management from the University of New England, and a Master of Management in Defence Studies from the University of Canberra. [Photo of General Coyle: Department of Defence]

References

Coyle, Susan (2021). *The relationship and interconnectedness of the cyber and land domains*. Presentation by Susan Coyle, Head, Information Warfare, Department of Defence, to the Chief of Army's Symposium on 20 April 2021.

Defence (2016). *2016 Defence white paper* (Department of Defence: Canberra).

Defence (2020a). *2020 Defence strategic update* (Department of Defence: Canberra).

Defence (2020b). *Our values: Defence values and behaviours*, 1 October 2020 (Department of Defence: Canberra).

Pearson, Stephen (2021). *Resilience of Defence capability to cyber attacks*. Presentation by Stephen Pearson, Chief Information Officer, Department of Defence, to the Senate Estimates Committee, Parliament of the Commonwealth of Australia, on 1-2 June 2021 [SB21-000137].

Sun Tzu (1963). *The art of war* (Clarendon Press: Oxford).