JOINT CAPABILITIES GROUP
HEAD OF INFORMATION WARFARE

Transcript

MILITARY COMMUNICATIONS AND INFORMATIONS SYSTEMS (MILCIS) CONFERENCE

15 NOVEMBER 2018

CANBERRA, AUSTRALIA

SPEECH – MAJOR GENERAL MARCUS THOMPSON, HEAD INFORMATION WARFARE, JOINT CAPABILITIES GROUP

INFORMATION WARFARE – A NEW AGE?

Good morning ladies and gentlemen.

It's a great pleasure to be here again this year. I recall standing here this time last year and being privileged to talk through my experience as a new appointment to the role of Head Information Warfare in Australian Defence Force Headquarters.

It's been a year and as you know, a lot can change in that time! In our world – the cyber, electronic and information domain – small changes can mean a great deal.

But today, rather than walk you through a list of those changes, I am going to pose you some questions. I do so because I think these questions represent both where we have gotten to after roughly 18 months of a formal Information Warfare Division in Australian Defence Force Headquarters. They also shine some light on where we have to go next.

My questions are these:

Does Australia possess the right legislative frameworks to meet the threats of conflict in the information environment?

Does The Australian Defence Force's force-structure reflect the true nature of the threat environment in the Information Age?

Have we prepared the Australian public to understand the nature of war in the information environment? Or, is the Australian public's lack of awareness a risk to Australia's force-structure development for information warfare?

These are deliberate questions, loaded to generate a response from each of you. I pose them to you here at MILCIS because, like I said to you last year, we consider industry and our external partners essential to our ability to solve the information warfare problem for the ADF. Without partnerships with you, the ADF will remain unable to meet the emergent threats of this new warfighting domain.

Let me address each question in turn.

Does Australia possess the right legislative frameworks to meet the threats of conflict in the information environment?

On 30 May this year, the Commonwealth Attorney-General announced that the government has commissioned a comprehensive review of the legal framework governing the National Intelligence Review[1]. The review is being led by former Defence Secretary Mr Dennis Richardson, AO.

The review is of considerable importance to the Australian Defence Force. This is not simply because of the internal intelligence capabilities the Australian Defence Force possesses in each of its three Services, as well as our own Defence Intelligence Organisation (DIO) and the Australian Geospatial Organisation (AGO). It is also because we live at a time when the relationship between Australia's whole of Government intelligence capabilities and our military operations have appropriately and sensibly become closer. The reasons for this are complex, connected not least to changes in how wars are being fought. The ADF's nearly constant operational tempo is another reason for this military-to-intelligence proximity. A renewed account of the appropriate boundaries between Government's intelligence agencies, their roles, functions and authorities has become essential.

This is especially the case within the so-called "information environment." I remarked two weeks ago, to a conference on information warfare held here in Canberra with my five-eyes peers – senior staff from Australia, Canada, New Zealand, the United Kingdom and the US – that we are currently at risk of missing the point about conflict in the information environment.

We are at risk, in short, of failing to realise we are already in a fight in this domain.

We might therefore need to act as militaries in the information environment in a way that preserves our national interests, and also preserves our militaries from full-frontal assault in the information domain.

The ADF operates under the Defence Act 1903, and has a tight interest in the Intelligence Services Act 2001 when it deploys. These pieces of legislation, with their updates, cover the intelligence and warfare activities the ADF is invariably involved in on operations.

However, the information environment, and the continuing exponential growth of IP-based military and dual-use technology, has thrown the ADF a real curve-ball. Information capabilities,

[1] Australian Government Attorney-General's Department, "Comprehensive review of the legal framework governing the National Intelligence Community", https://www.ag.gov.au/NationalSecurity/Pages/Comprehensive-review-of-the-legal-framework-governing-the-national-intelligence-community.aspx

and conflict using them, straddle the legal areas of both intelligence collection and responses to offensive, malicious, state-sponsored acts. It can therefore become difficult to account for information capabilities' use as warfare, as espionage, as criminal activity, or as a combination of all three.

It is my hope that the Richardson Review into Australia's intelligence framework will account for problems of this kind.

For example, what will the ADF do where its freedom to manoeuvre is physically hindered by attacks in the information environment?

I'll invent a scenario here for argument's sake, to make my point.

There is a cyber strike against Australia's homeland infrastructure which limits the ADF's ability to communicate with deployed and allied forces. Would the ADF be licensed to respond here? Or would the ADF need to call other civilian agencies to its aid?

In such a scenario, would such agencies – like the Australian Signals Directorate – have sufficient resources and tasking priorities to support the ADF?

Or, would they be occupied elsewhere with other more complex problems that a clever enemy has set us to ensure we are hindered from using our military?

An effective attack on Australia, for example, might be sequenced to ensure that ADF units were taken out of any meaningful fight before they even get to it, and the ADF loses the ability to do anything but watch a larger kinetic battle taking place in front of it.

Could the ADF be left tactically hamstrung in a battle designed to ensure that our multi-billion dollar force structure is muted through deliberate chaos sent through our C4 and ISR systems?

This is a particularly tough question. I pose it in order to ask a bigger one. Have we, the ADF and its stakeholders, truly thought through the risks to the ADF, and indeed, the Nation, emanating from the information environment?

The information environment today is so pervasive that anything short of a full assessment of its reality could jeopardize Australia's ability to respond militarily in ways we are used to.

The world has shifted. I believe we have to fundamentally shift with it.

This might mean updating legislation so that tactical and operational commanders can have full authority to conduct responses anywhere on the globe to preserve the force for their own operations, inside and outside the information environment.

Or, it might mean enabling Australia's civilian apparatus to have fuller purview into the military's activities, so it can ensure the military's activities are in no way jeopardized by the existing "seams" in Australia's cyber and information environment.

Certainly, it means a full assessment of the realities of the risks of the information environment to the ADF, and a commitment to ensure we are hardened and agile to remain capable in this new world.

Law is certainly one way to address this. But it is only a single component of our response. What is actually required is a shift in Australia's conceptual imagination concerning the nature of warfare and the integration of information into the modern fight.

I am therefore calling for a review of how we consider force-structures in the light of the information environment. I want this call to be taken seriously by you, our stakeholders, since we've already started asking the question within the ADF.

So let me move to my second question.

Does Australia's force-structure reflect the true nature of the threat environment in the Information Age?

To help make my point, I am going to take a quick detour through history. The history was consequential to Australia and it bears re-examination today.

In 1941, the Royal Navy was stretched to breaking point due to the global nature of its World War 2 conflict. Britain had devised a clever, but ultimately fatal, plan to defend its Asian holdings against Germany and now against a mobilised and warfighting imperial Japan.

The naval component of the British plan comprised a small, but highly capable, purpose-built strategic naval force known as Force Z. This comprised six outstanding modern battleships, the HMS Prince of Wales and HMS Repulse among them. The Force was commanded by Admiral Sir Tom Phillips, a doyen of the Royal Navy. Its job was to use Britain's sea-power expertise to deter and defy, as far as possible, any naval threats to Britain's Asian landholdings while Britain's main war raged in Europe.

At 1015 h on 10 December 1941, three days after Pearl Harbor, a small Japanese scout plane that had been hunting for Force Z spotted Admiral Phillips' task group.

Within minutes the Wales and Repulse were taking barrages of torpedo fire from Japanese Nell Torpedo bombers. One of these managed a single, fatal hit on the Wales and sent her sinking. The Repulse, meanwhile, had been faring well tactically against the Japanese swarm. She looked likely to survive that fatal hour. With Wales hit, however, Repulse turned to aid her stricken comrade. She soon shared Wales' fate. Repulse took one starboard torpedo, then three more in the next few minutes. Within half an hour, the pride of the Royal Navy had been sent to the bottom of the South China Sea.

How did this happen? Was it bad planning from the British admiralty or was it a series of tactical errors? Or, was it a failure of strategic and tactical imagination?

Like most history lessons, it was a combination of all of these. But I am here to tell you I think it was principally a failure of imagination. In 1940, one year before the Japanese attacks on Pearl Harbor, the Royal Navy had accomplished the first all-aircraft, ship-to-ship naval attack in

history at the Mediterranean port of Taranto. The British sank half of Italy's capital ships that day.

But strangely, with Pearl Harbour only three days old, the British Commander did not perceive the peril that a swarm of Japanese bombers could bring to his own fleet, afloat as it was in the middle of the ocean. The Japanese bombers were low on fuel and Force Z was a dispersed and moving target. Pearl Harbor and Taranto were attacks in harbor, against sitting ducks. No need to break radio silence to call for air cover. The Japanese planes probably wouldn't run the distance and submarines were the greater risk anyway.

That mistake by Admiral Phillips cost him his own life and the British their defence of the Malay Peninsula. Arguably, it wasn't even the wrong call. Japanese submarines might well have been close and calling for air support might have alerted them to Force Z's presence, ending the day badly for Britain in either case.

Critically, the British hadn't imagined their way to thinking that Japan might outdo them at something the British started, in decisive naval air warfare.

Britain did not conceive that Taranto could be reframed, reimagined and reshaped to destroy the heart of Britain's imperial power in the far East. The Japanese were a tenacious, highly trained warfighting enemy. The British commanders underestimated them. Singapore fell only two months after the Wales and Repulse were sunk, and took the 8th Australian Division with it. The future of what we now call the Indo-Pacific was changed forever.

It is easy to take lessons from history and misuse them, so let me do something simpler. I am going to tell you that Australia's force-structure is currently geared to a conventional future fight which may, or may not be warfare's future. Certainly, it won't be its centre of gravity. One of my staff is on record as saying "the ADF is currently at risk of burning tomorrow's money to solve yesterday's problems." My "spider-senses" are telling me he may be right.

Just as the British forces in Malaya in 1941 were not prepared for a tenacious, well-rehearsed, and empowered Japanese enemy, Australia's force-structure is looking very much like it's addressing conventional threats we can already see. We are not yet agile to face possibilities we know could send us to the bottom of the ocean, but which we question if anyone will actually pull together. Where is Australia's sliver of tactical imagination to set a battle on its edge in the information domain?

Where is our realization that just because we are good at cyber today, we couldn't be comprehensively beaten at it by a competent and determined enemy who has already imagined themselves into the wars of tomorrow, better than we have done?

What if the ADF's combat capabilities are grounded because of cyber-generated confusion? What if we never put to sea because we simply can't command properly with our 20th century C4ISR systems?

These aren't rhetorical questions. They go to the heart of how we are structuring for future threats, and how we are preparing to defend ourselves in a world that has already changed more times than people could have predicted even five years ago.

Because rapid, unpredicted change is the new normal, we should feel discomforted by the size and shape of our old defence force beliefs in a world that is daily setting new constants in technology, politics, and even warfare itself. We should be discomforted in order that we evolve faster than our competitors.

I propose to you today not that conventional threats will dissolve in the light of information warfare's future. I propose instead that information capabilities have opened up such a vector of imagination for warfighters that we are at risk of being sent to the bottom of the ocean like the Wales and Repulse of old. Unless we imagine conflict differently, we are at risk of being undone by competitors who perceive the stakes of conflict as far higher than we do.

We – the ADF, and you, our stakeholders – have an obligation to act now, or we risk not being left with the choice of action at all.

In another lesson from history, the turn-of-last century British Dreadnoughts were fearsome battleships whose conventional superiority also marked the beginning of British naval decline[2]. Seaborne mines and torpedoes ended their life-expectancy, rendering their firepower redundant. In a case of history rhyming, not repeating, the UK Chief of the General Staff told a conference earlier this year that "a cyber 9-11 might already have happened, and we wouldn't know about it."[3]

If I may interpret the UK CGS here, I read him as saying that the "mines" in the cyber-domain may already have been laid. The fearsome dreadnoughts of our modern force-structures may already have passed their used-by date. Our conventional forces might not even get out of bed in the morning before the next war is over.

The US Congress recently authorized US special forces to support foreign forces working against "hybrid" war or "grey zone" conflict[4]. This was a welcome legal move. It came after years of conceptual discussion about "hybrid" and "grey" war in strategic circles. Certainly, I view the typical (and convenient) distinction between Phase 0 and Phase 1 as having become so blurred, that that doctrinal construct has now collapsed to the point of irrelevance. We also need to start working out now what these authorities mean for information war. If grey-zone activities – those beneath the threshold of physical conflict – disable our information systems, we won't have time to argue about whether the war was hybrid or grey. We will have already lost it

And, I might add, cyber is only one arm of the information environment. So I suggest to you, that as a nation, we have only just started to think through the information warfare challenge.

A force-structuring response

---

[2] https://www.wired.com/2014/08/the-wwi-battleships-that-saved-and-doomed-the-british-empire/

[3] "British Army Chief reflects on whether 'Cyber 9/11' has already happened", *Forces Network* https://www.forces.net/news/british-army-chief-reflects-whether-cyber-911-has-already-happened

[4] Morgan and Thompson, *op. cit.*, p. 15. US Department of Defense, *Directive-type Memorandum (DTM)-18-005 – Authority for Support of Special Operations for Irregular Warfare (IW)*, 3 August, 2018, https://fas.org/irp/doddir/dod/dtm-18-005.pdf

I am creating this picture because I do not see that we are acting even remotely fast enough to keep tempo with the risks we see emerging.

If anything I am saying here is true, what are we to do?

I propose that we undertake a thorough examination of what the information environment does to warfighting. I don't mean here, to cry "the sky is falling" like Henny Penny and declare the last Defence White Paper redundant.

I mean, truly restructure our imagination and become our enemy trying to tear us apart. How will the information environment affect the ADF? Are my worries about force structure justified? Or should we just maintain radio silence and worry only about the submarines we know will be in our waters?

I think it is our duty to ask how the ADF can become like a swarm of 1941 Japanese torpedo bombers able to menace the legendary capabilities of all modern militaries. I think we should work through how the ADF can develop and train fighters to operate, metaphorically, low on fuel, across the open ocean of the cyber domain, to sink those menacing the ADF and who seek to do Australia harm.

Only this way will the ADF "red-team" its way to information warfare proficiency. Only this way, I believe, will the ADF become an adversary as skilled as any that we have to be prepared to fight in the information environment, during any phase of the competition-conflict spectrum.

This, at any rate for the ADF, is our job. I want you, in industry, academia and elsewhere, to help us do it.

Have we prepared the Australian public to understand the nature of war in the information environment? Or, is the Australian public's lack of awareness a risk to Australia's force-structure development for information warfare?

This brings me to my third and final question today. I want to talk to you about narrative. I don't mean "storytelling" in the general sense. I mean the precise account we give of ourselves as warfighters in the information domain to the Australian public we serve.

Why is this important?

Storytelling is as old as warfare. The relationship between what we say we are doing and the policy settings under which we are doing it, is essential in today's environment. We can't afford to imagine that the Australian public will be happy to be left with a "nothing to see here", or "sorry, way too classified" approach to information warfare.

I think our "story" has to go something like this:

1. **The nature of war is changing in the information age.** We have to get across what this means, urgently. It needs thinkers, planners and practitioners like those in this room, along with our excellent policy officials and strategists, to imagine ourselves to agility in the information age. Actively challenge your assumptions. We already know

that old verities are being replaced by new realities. We have to become masters at what this means and turn it to our advantage.

2. **Citizens and their digital capabilities can become proxies in the information domain in ways they do not understand.** Defending the Nation in the information environment is a collective responsibility. Therefore, cyber-security and information awareness is everyone's business. We need to educate the public and make sure they understand the new world we are in. We can't expect people to help us if they don't understand the problems we are trying to solve.

3. **The ADF is on the front line of the information battle**. When the ADF speaks about what it does in the information fight, we must be dependable to give a factual, credible account of itself and the challenges we face. We are the nation's first responders to military emergencies and we need to become trusted to respond and capable to deliver in information conflict, just as we are in every other domain or warfighting.

Information war bodes a new era of state-on-state conflict. It isn't just a different form of propaganda and it isn't just the "same old thing" as wars we've already seen. It is real, present, different, dynamic and evolving. Some illustratively suggest that it burns like napalm through our ancient expectations of armed conflict. It has already changed how we respond to conflicts and how we behave in them – look at the role of media in modern conflict, for example. The information domain on the warfighting side has started to mold our force-structure thinking, even if has done so less than I would like.

Unless the ADF takes a lead in explaining what information war is and becomes a natural leader in Australia's response to it, it will be impossible for policy makers to account for the money we need to spend to get our response to our new game up to scratch.

Secondly, the ADF needs to become the chief advocate of information warfare capabilities so Australia can build sovereign defence capabilities for the information environment. I don't just mean "plug and play" capabilities for information resilience to the tactical warfighter. I mean whole-of-force level capabilities that make Australia an information capability powerhouse in the Indo-Pacific and globally.

This matters because while we are learning to fight war in the information environment, mixing new forces with old, we will need to take a lead and set the tone for our security partners to follow.

For example – Australia is a privileged member of the five-eyes intelligence-sharing network and it is important that we remain so. But soon, nearly universal commercial encryption capabilities will mean all militaries will require good relations with host-countries to execute targeting procedures properly. We cannot afford to believe we are "elite" in our freedom of maneuver, even while we remain members of a privileged intelligence club. In the information domain as elsewhere, Australia will need to secure good, working-level human relationships with all our partners to become truly effective in the information fight. We may even need technical capabilities that enable fluent maneuver through multiple layers of encryption, reflecting the different levels of security relationship we have with multiple security partners.

Dynamism of this kind should inform our approach to information warfare policy. We should consider how we develop technical information capabilities that are truly Australian, which preserve and enhance our traditional security relationships, and which enable us to develop new partnerships that empower our warfighters.

Finally, the reason we need to get the story straight is that the characters in our domestic information story are changing. As I highlighted in a recent article with the Center for Strategic and International Studies in Washington, the changes in Australia's homeland security settings risk leaving the military without an information bed to lie in. The formation of the Department of Home Affairs, the Office of National Intelligence, and the statutory independence of the Australian Signals Directorate (within the Defence portfolio) are welcome events, much needed by Australia. But the ADF's cyber and information capability requirements will need to be considered against the powerful and entirely reasonable demands of each of these agencies into the future.

Each one of Australia's agencies charged with cyber and information security have specialized expertise in their fields, which differently shape their approach to the information environment.

So unless the ADF articulates its specific information environment needs, it may miss out on making its unique and critical contribution to the national security space which will involve information capabilities across the board.

The ADF has a story to tell and to put into the minds of its stakeholders. That story should help Australians reconfigure their understanding of conflict in the information age. This also means being able to frame our story so a teenager can "get it" when they look at an information warrior in the Australian Defence Force. The ADF's current information war concepts are too muddy for people quickly to grasp. Our story hasn't been clear, and sometimes it hasn't been there at all. We have to change this so everyone understands the nature of the information fight, and we in the ADF get better at it.

Conclusion – preparing for the future

In conclusion, I've set out three objectives here today which I think need addressing:

1. Australia's legal frameworks for conducting information war

2. The ADF's force-structure to fight and win war in the information age

3. The public narrative connected to information age warfare, including thinking through sovereign ADF capabilities in the information domain.

Each of those challenges is big in its own right. I am sounding a little "strident" because I sense at the moment that there is plenty of concern about this domain, but a lot less action than we need.

We have started, but we have to go further, and we need to move faster. I'm happy for you to come and overwhelm us with ideas, so we can return to you with capabilities. I would prefer to be flooded and learn to swim in the information environment than be slaked and die of thirst in it.

To join the dots for you, I need you as our stakeholders to talk back to us about the connection between warfighting and your domains; between law and your needs; and between your capability and the threats facing us. I need you to you use your imaginations and get your pens out to help us focus our own imagination. Only that way will we get ready for the next fight, where information will be central and may be the decisive feature of all our ways of doing battle.

I look forward to continuing this journey with you. We, in the ADF look forward to working with you as we become an agile and sophisticated defence force for warfighting in the information age.

Thank you. I'm open to questions.