Good morning ladies and gentlemen.

It’s a great pleasure to welcome you here this morning to the Information Warfare five-eyes principals’ forum.

I should also thank my team, and in particular Ms. Kendy Hau, for bringing me the idea of the conference and organizing it. Kendy has been exceptional in her leadership and has dared to ask questions others seem reluctant to confront. I bring to your attention the topic of the forum, “Redefining the boundaries: warfare in the digital age”:

Western democracies are already at war in the information domain despite a general struggle to detect the modern hallmarks of warfare. How can the ADF and its Allies posture to meet this new frontier in warfare? What leverages are the adversaries employing to win?

I will leave it to other speakers to address these three critical questions in detail. I would like for my own part to set an agenda for the conference by bringing my own perspective as Australia’s Head Information Warfare to the table.

I commenced this role in July 2017 which sees me, maybe, nearly halfway through my tour. I can tell you, things have changed a lot even in this short time. When I began my job, there was doubt in strategic circles about even naming the concept of “cyber” warfare out loud, let alone “information warfare”. But, our Department of Defence has been bold enough to give me the title Head Information Warfare and a Division to go with it. Both are new for Australia.

So, of course, I have had to go ahead and attempt to work out what all that means!
Fortunately, Australia has long had strong cyber capabilities. We have spoken out loud about it, one of the first Western nations to do so after the United Kingdom announced its intentions to develop offensive cyber capabilities in 2013.¹ Prime Minister Turnbull announced in April 2016 that Australia has an offensive cyber capability, following which Australia’s then Minister for Cyber explained that our cyber capabilities are for use against cyber criminals offshore.² Cyber has become part of warfare’s daily conversation.

But information warfare is another matter. Isn’t it something only other countries do, according to media reports? Isn’t “information war” a kind of Soviet-era propaganda, now globalized through the internet? Surely I could leave that to one side?

Well, as I grew into my role – and the more I looked at the Russian example in particular – the more comfortable I became with the concept of information warfare. More than that, I realized that we – the ADF, her allies and partners – are already part of a significant global struggle in the information environment.

This struggle uses the information environment as its centre, global populations as its pawns, and human infrastructure as its chessboard.

It is a terrifying picture when we draw it up. It is even more terrifying when we realise that we aren’t crying “the sky is falling” like Chicken Little or Henny Penny in the children’s tale. We are working out the scale of a global risk in which every person is involved, and in which the military has a distinct, critical role.

Today I want to address three questions that I think go to us identifying where the military sits in this picture. The questions are, simply:

1. What is the threat?
2. So, what should our response be? and
3. Now, what do we do next?

**What is the threat?**

Let me start with the threat. UK Chief of the General Staff, General Mark Carleton-Smith, said at the UK’s land-warfare conference in June this year that “a cyber 9-11 could already have happened and we wouldn’t even know about it.”³ His point was not that we should rest easy. It is

---

¹ “Cyber spy boss taking agency ‘out of the shadows’”, *The Australian*, October 25, 2018; “UK becomes first state to admit to offensive cyber attack capability,” *Financial Times*, September 29, 2013, [https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de](https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de)
instead that there is a probability – for some analysts, a high certainty – that mines to detonate in the cyber domain have already been laid.

Like the magnetic mines that killed the old British Dreadnoughts, these cyber mines threaten our way of life and the strategic certainties we currently hold dear. The Dreadnought symbolized the height of British naval power, and became a symbol of British naval decline. Cyber capabilities threaten to disrupt the quest for military superiority that has carried us into our current force structures. They equally threaten the conventional adjustments we have made to these force structures to try to maintain our capability edge.

If I needed an example to make my point, I would observe – as I did in a recent article with the Center for Strategic and International Studies in Washington – that the new combat systems of the indomitable Aegis-Class Destroyer recently delayed their rollout because of identified cyber vulnerabilities, a fact the US Navy wisely put on record. The US Navy has already developed sophisticated ways of being afloat and becoming cyber resilient. Here I name the impressive “Compile to Combat” or C2C4 models the US Navy is developing. But, the symbol of a grounded US combat fleet due to cyber paralysis tells us how deep this risk goes.

I congratulate the US Navy for its transparency, and for its snappy response to risks in the cyber domain. None of us can meaningfully address what remains in the dark. Equally we cannot get into the fight without concepts to match our capabilities.

The US Navy is leading the way. Always courageous!

I also remain confident that each one of our Services – allied single Services, joint and coalition – will patch and manage cyber risk capably as we go forward. We are an inherently creative group of people. Our creativity has been spurred through combat. It carries the insights of nearly constant operational experience since 9/11. Many of you in this room are responsible for significant leadership and capability development in your respective militaries since that date, not least in the information world.

---


7 Semper fortis, the official motto of the United States Navy.
But 9/11 is a good focus point. As our US team mates know only too well, the 9/11 Commission into the attacks reported “four kinds of failures: in imagination, policy, capabilities, and management.” As an Australian, I would not presume to speak from the US experience. But I certainly want to learn from it.

So here is my question – will we truly grasp the threat of the cyber and information risk at the strategic level while we are addressing our own single service, domain-level risks?

What is this strategic level risk?

And, are we as military leaders at similar risk of a failure of imagination in cyber and the information environment as the one which caught the US, and the rest of the world, off guard nearly 20 years ago, that fateful September morning?

The evolution of 5G technology and growth of commercial encryption will mean our traditional targeting points for military operators must continue to evolve. Host-nation cooperation may become essential in correctly identifying legal targets, for any type of operation. This considerably complicates overseas operations, especially those in contested environments. And this is before we have even considered the challenges to safety, privacy and sovereignty these issues presented to countries like our own for whom the rule of law remains paramount.

We had better get these questions right. I agree with General Carleton-Smith when he says it’s likely the mines in the cyber domain may have already been set. I would go further and point out cyber is only one component of the information world. We need to get thinking about what this means, and fast.

We can start by pushing some boundaries. Let me do so here.

- I think we risk not seeing we are already in a state of conflict – or as some would argue, a state of war – in the information environment.
- A failure to acknowledge this will be at the heart of our vulnerability in this domain.

Information capabilities are sewn into the seams of every strategic capability we have. They are core to our strategic future.

Unless we realize we are already in a full-blown fight in the information domain, we may end up being beaten before we get out of conventional war’s older, perhaps rickety bed.

So what should our response be?

Some of my staff in the Information Warfare Division are certain of where things are at. One of them recently stated to me that “we’re currently at risk in the ADF of burning tomorrow’s money to solve yesterday’s security problems.”

---

I am on the record as saying that “the ADF will be involved in the information contest wherever it occurs in peace or war.” For reasons to do with Australia’s current legislation, I could not say, “the ADF will be involved in information warfare” because, for the meantime, Australia does not possess a legal or conceptual definition of what information warfare is.

I contend here that we need one. To be precise, we need:

- A clear **conceptual definition** of information warfare so our warfighters can plan with it.
- And we need a clear **legal definition** of information warfare so our warfighters can be protected when they engage in conflicts in the information environment.

Regarding law, I consider Australia currently has a gap in the authorities and powers related to its military operations— the *Defence Act 1903* – and the *Intelligence Services Act 2001* – under which Australia’s intelligence activities are legally authorized. These are roughly analogous to the United States’ *Title 10* authorities for the use of military force and its *Title 50* authorities for the use of intelligence capabilities. They are similar in kind also to the United Kingdom’s *Defence (Transfer of Functions) Act 1964* and the UK *Intelligence Services Act 1994*.

Even if these are only rough approximations of similar allied legal frameworks, they make a combined point:

1. **Information capabilities, and conflict using them, straddle the legal areas of both intelligence collection and responses to malicious, offensive, state-sponsored acts.**

2. **It can therefore become difficult to account for information capabilities’ use as warfare, as espionage, or as a combination of the two.**

What will our planners do, for example, when we need to mount an offensive cyber-attack to prevent a major domestic urban catastrophe such as the shutdown of critical infrastructure? What if that cyber-attack means the near-certain loss of human life to neutralize the attack’s source? How would we account for proportionality in a lethal cyber-strike?

It’s easy to get bogged down in conundrums like these. Only they aren’t theoretical. The capability march in the information domain has already begun.

Analysts propose that nation-states like Russia have already integrated their information capabilities into their conventional ones. British-based scholar Keir Giles pointed out in his 2016

---


Handbook of Russian Information Warfare that this “reflects enduring principles of the Russian approach to competition between states, extensively updated and renewed as part of Russia’s recent preparations for conflict in conditions of overall conventional inferiority.” Vladimir Putin explained why Russia has focused on information capabilities – because they are less expensive.

Popular literature meantime brims with titles such as The Perfect Weapon. War, Sabotage and Fear in the Cyber Age; and Like War. The Weaponisation of Social Media.

It’s hard to miss the fact that “war” has emerged as the strongest frame for contest in the information environment. We have lost the time to speculate on this. We now have to chase the problem down. It is at our doorstep.

Let me propose three ways we can do this together, as FVEY partners, with tangible effect:

1. **Firstly, lets clarify our legal definitions:** Australia is facing a problem in its legal accounts of information warfare. If you, our partners, have solved yours, tell us how. We need to hear from you. If you haven’t solved it, let’s solve it together.

2. **Secondly, let’s develop our conceptual frameworks:** I recently described some beginnings of ADF concepts of cyber warfare. This is only a beginning. I’d like to see us, as five-eye allies, work together to develop concepts of information war – detailed, tested, workable operational and strategic concepts. We are in this battle together.

3. **Thirdly, let’s tell the public our story:** As members of liberal democracies, this is critical! If we can’t explain to our public how we are going to defend them, we probably can’t win the information battle. Much of our work is classified and will remain so. But the world is immersed in the information age. So, we could do worse than explain the information warfare threat to the public we are duty-bound to protect. That would simply mean having a tech-savvy population make the link between our strategic efforts and our military spending.

It’s easy to forget that narrative is as old as warfare. We need to get both right to win at the strategic level.

---


13 As described by President Vladimir Putin, “We must take into account the plans and directions of development of the armed forces of other countries... Our responses must be based on intellectual superiority, they will be asymmetric, and less expensive.” (Vladimir Putin, “Солдат есть звание высокое и почетное” (‘Soldier’ is an honorable and respected rank), excerpts from annual Address to the Federal Assembly of the Russian Federation, Krasnaya zvezda, May 11, 2006, [http://old.redstar.ru/2006/05/11_05/1_01.html](http://old.redstar.ru/2006/05/11_05/1_01.html)

Now, what do we do next?

The question of what we do next in dealing with this threat has a lot to do with gaps we see in this field.

I propose we move on four lines-of-effort, together, as five-eye partners:

1. **Let’s make it clear to all our stakeholders that information warfare is real and its impact is “already”**. I’ve already said we need a public narrative to account for our military activities. But I sense that we have an additional job. Our stakeholders need to know how information warfare is different for the military than for other agencies. Spy-agencies and police-forces have different remits to ours. What belongs to our militaries in the information domain? What do we have to protect as militaries? What do our militaries have to become experts at in the information fight? Reciprocally, what belongs to other agencies and areas? How will we share, if at all? Clarity and purpose will be needed in all these areas. Otherwise we risk information “smoke” as an excuse for bad spending. None of us can afford this.

2. **Let’s emphasize the nature of the information fight. It is both cognitive and technical, and inherent to modern warfare.** The human mind remains the key to the information battle. Our technical systems support human minds making decisions during the battle and preparing for it. We have to shape both minds and machines, make both resilient, and get both ready for a conflict with information as a new decisive point in warfare. Have we agreed as five-eye allies yet on the dimensions of the information fight, so we can put them into doctrine for our soldiers, sailors, airmen, airwomen, and Marines? If we haven’t, let’s set a timeline and get on with it. Additionally, let’s make sure we get the “information vernacular” right between our allied forces right, so we can hand off operations to one another seamlessly. Language is key to information’s power. We should remember that while we build as allies.

3. **Thirdly, lets recognize and message that the information fight has already begun, it is strategic, and we will always be in it.** We are now in a state of constant competition in the information environment. Some of this is can be labelled as war, some of it cannot. We need to define that. If we need to change our legal definitions and interpretations, then let’s do that. The US Congress has already started this discussion, asking the US President to “develop a policy for determining when an action carried out in cyberspace constitutes an act of war against the United States.” Similar discussions probably need to occur in all of our countries. We need to make it pointedly clear that our nation-state capabilities are at risk of being slowed, or stopped, by cyber and information capabilities. That is before a single shot has been fired. If that isn’t a strategic level risk, I don’t know what is.

4. **Finally, let’s work out how information war plays in the grey zone.** The US Congress recently authorized US special forces to support foreign forces working

---

against “hybrid” war or “grey zone” conflict. 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. As Five-eye allies we should start working out now what these authorities means 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. So, we should link discussions of conceptual ambiguity – such as “hybrid” and “grey” wars – to the tests of strategic, operational or tactical necessity for our military forces. If information capabilities are needed to deter or counter threats at any level of war, we should provision our forces to act on their own terms in any zone whenever our capability is menaced.

These are four areas that I see each of us as partners needing to get right. I’m certain that we’re some way to doing this in each case. But we can go further, and my sense is we need to move faster.

Conclusion – Lest We Forget

I have set out this morning a number of key issues for information warfare. They are issues we see in Australia, and I know that we share many of them as five-eye partners. We may share all of them. Let’s use these next two days to work out what the issues are. Then, let’s galvanize our collective thinking when we return home to secure agreements, and collaborate wherever we can. We must establish a broad surface of defense as five-eye information allies to succeed.

In closing, let me recall a story as to why getting this wrong could be catastrophic. Many of you know it well:

- In World War 2, the British Navy was stretched to breaking point due to the global reach of the conflict. Britain hinged its defence of Singapore and the Malay Peninsula on a small, 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. These ships were the pride of the Royal Navy.

- On the morning of 10 December 1941, three days after Pearl Harbor, a large force of Japanese bombers were hunting Britain’s Force Z. A small scout plane spotted them at 1015 h. At 1113 h, eight Japanese Nell torpedo bombers targeted the Repulse and scored one minor, but insignificant, hit. Regrouping, 17 Japanese planes formed into two attack groups of 8 and 9 torpedo bombers, then swarmed the Repulse and Prince of Wales respectively.

---


18 See https://richardedwards.info/2014/12/10/118/
Of the nine planes attacking the *Prince of Wales*, one delivered a single, catastrophic hit. The ship took on 2,400 tons of water, listed dangerously to port and began mangling internally. She struggled on for another hour before 26 Betty Bombers of the Japanese Kanoya Air Group arrived at 1220 h and finished her off. The bombers sent three torpedoes into *Wales*’ starboard side.

Meanwhile, the *Repulse* was forced to cease its successful evasive maneuvers from the Japanese air force to assist the stricken *Wales*. *Repulse* had dodged 19 torpedoes that deadly hour. She looked likely to survive. But turning to help *Wales*, *Repulse* was caught in the pincer movement of the Japanese aircraft and took a torpedo in the starboard side. *Repulse* took three more torpedoes in the next few minutes. *Repulse* was now on her death-bed with *Wales*.

Within half an hour, the pride of the British Navy had been sent to the bottom of the ocean. The naval defence of the Malay Peninsula was all but over.

How did this happen?

The Royal Navy already knew about the threat airpower posed to ships, not least from their own offensive capabilities. The Royal Navy had launched the first all-aircraft, ship-to-ship naval attack in history at Taranto in 1940.19 They sank half of Italy’s capital ships that day. Pearl Harbor had already happened, albeit only three days before *Wales*’ and *Repulse*’ last. The world had seen what this new arm of war could do.

But tragically, on board the *HMS Prince of Wales*, the renowned Commander of Force Z, Admiral Sir Tom Phillips, refused to call for air support at Malaya in favor of keeping radio silence.20 He had favored the element of surprise throughout that fateful voyage.

It was a thoughtful but devastating choice.

What defeated the Royal Navy that day was arguably being unprepared for a dose of its own strategic wit, this time better prosecuted by Japan across open ocean. Taranto one year earlier had been an attack in shallow water. The Japanese planes completed their mission, nearly without fuel, across wide seas. Phillips had underestimated his enemy, like many British naval commanders of his time.21 Singapore fell only two months later, including the 8th Australian Division.

Imagination, tenacity and Japan’s sharp strategic purpose ended wartime Britain in Asia.

It is not a risk to say we face analogous problems today. Our countries are outstanding in the cyber domain. Arguably, we invented it.

---


As allies, we are aware of the cyber and information war threat. We talk about it constantly.

But have we truly imagined our way – as warriors and leaders – into an information warfare future?

Are we at risk of congratulating ourselves on shallow water cyber and information operations when the deep blue ocean of the cyber and information future awaits us?

Finally, have we communicated to each other effectively about the threat, breaking our modern radio silence so we can defeat an already skilled, increasingly capable enemy?

I set these questions to you as peers and team mates. It is for us to solve them as allies.

I look forward to working with you over the next two days to keep building the bridge to our future. We can’t afford to be found wanting.

Thank you.