iWar conference keynote speech - the Missing 'I' in DIME

[Intro]

Thank you Kendy

Ladies and Gentleman

It's my great honour and privilege to welcome you to the 2019 iWar Forum.

This is an important occasion. And one, I hope, will become a standing event in our calendars each year.

In this room – inside our National Parliament – is an extraordinary brains trust.

A collective intellect with the capacity to think critically and creatively about the information warfare threats we face of today, and those we can only imagine tomorrow.

If you've found yourself lying awake at night contemplating how we – and I mean the collective 'we' of governments, militaries, businesses and organisations – defend ourselves, and compete in an ever-expanding information environment, you've come to the right place.

I've made no secret of the issues that keep me up at night – and it's not the performance of the Wallabies at the Rugby World Cup.

There are three questions constantly on my mind:

- How do we have a meaningful conversation with the public about a contested environment they may know very little about?
- How do we build national resilience towards malign influence and activities in the New Information Environment?
- And lastly, what is the role of the Australian Defence Force (the ADF) in a whole of government response?

Over the next two days I'd like us to think critically and creatively about how we as liberal democracies respond to asymmetric warfare actions that exploit the interconnected nature of the information environment.

We need to imagine the actions of our competitors before they've been conceived.

Whether we like it or not, we're in an era characterised by continuous contest in the information environment.

And contest demands of us the kind of thinking that is only made possible through the sharing of knowledge.

That brings me to the theme of this year's conference - '**The missing I in DIME'** – which my team has posed to start the tough conversations we need to have.

I'm not being deliberately ironic.

But rather, I'm presenting a challenge that I believe we're all facing.

Information needs a champion.

The seams of our democratic system are vulnerable to exploitation in the information environment.

I'm sure it won't surprise any of you to know that Australians (like citizens of most liberal democracies) are concerned about the increasing threat of cyber-attacks.

In fact, a recent Lowy Institute Poll[1] showed increases from the previous year in the Australian public's concern over cyber attacks from other countries (up from 57% to 62%), and concerns regarding foreign interference in Australian politics (up from 41% to 49%).

The Poll also showed the number of Australians who feel 'very safe about world events' has almost halved over the past ten years (from 35% to 18%)[2].

It's a pattern we've seen play out all over the world.

So what do we do about it?

The next two days will be about asking, and - I hope - finding answers to fundamental questions about our ability to compete and contest in the INFORMATION ENVIRONMENT and the grey zone.

We may need to look at how we conceptualise the threshold of conflict in this contemporary battlespace, and ultimately, if we have a strategy for the information fight?

The answers to these questions will define the prospects for our sovereignty and prosperity over the next 20 years.

There is a great deal of hard work being done across the Five Eyes to develop the capability for agile responses to threats in the information environment. We will hear about that work over the next couple of days.

But I want to take a moment to reflect on some important developments which go to the heart of this conversation.

---

[1] https://www.lowyinstitute.org/the-interpreter/cyber-threats-go-beyond-hackers-and-scams-democracy-itself

[2] https://lowyinstitutepoll.lowyinstitute.org/themes/security-and-defence/

[Context]

At the recent Australian Strategic Policy Institute's 'War in 2025' conference, our Chief of Defence Force, General Angus Campbell, posed a number of questions about Australia's vulnerability to political warfare[3].

These were questions that needed to be asked.

As the information environment constantly evolves around us, we are left pondering how to delineate responsibilities across government to enable us to be agile in response to an information war.

Chair of the Australian Parliamentary Joint Committee on Intelligence and Security Mr Andrew Hastie[4], a former Army officer, noted the geo-strategic landscape in which Australia operates has changed. Both General Campbell and Mr Hastie urged stakeholders, like you here today, to avoid a costly failure of imagination about the nature of contemporary competition and conflict.

From a strategic perspective, perhaps the fundamental question is - have we imagined ourselves into the mindset of our competitors, to understand the range of options they consider appropriate and legitimate?

Or are we posturing our defence capability and national security architecture for a fantasy conflict, one that bears no resemblance to the reality of contemporary threats?

So let me try to anchor these ideas in a real-world context….

[Skripal poisoning and response]

I take you back to the 4th of March 2018, to Salisbury in the UK. Former Russian military intelligence officer Sergei Skripal and his daughter Yulia were poisoned with Novichok, a nerve agent that emerged from the Soviet Union's chemical weapons labs[5].

During their investigations, the UK East Stratcom Taskforce identified more than 150 disinformation narratives emerging from the pro-Kremlin propaganda apparatus[6]. Each one was designed to distract from and distort Russian involvement in the attempted assassination. Russian state media and its Ministry of Foreign Affairs operated in tandem[7], asserting that claims of Russian culpability were in fact due to Russophobia.

Russia's propaganda machine consistently rebutted accusations of Russian culpability, however the UK mobilised a coordinated response that provided the public, the media and the international community with a clear attribution linking Russian military intelligence to the attempt on the lives of the Skripals.

---

[3] https://www.aspistrategist.org.au/adf-chief-west-faces-a-new-threat-from-political-warfare/
[4] https://www.smh.com.au/politics/federal/we-must-see-china-the-opportunities-and-the-threats-with-clear-eyes-20190807-p52eon.html
[5] https://www.bbc.com/news/uk-43315636
[6] https://euvsdisinfo.eu/conspiracy-mania-marks-one-year-anniversary-of-the-skripal-poisoning/
[7] https://euvsdisinfo.eu/behind-the-smokescreen-who-are-the-actors-spreading-disinformation-on-ex-spy-poisoning/

UK Prime Minister at the time, Theresa May, responded to Russia's "sarcasm, contempt and defiance" with a message that surprised Russia[8]; expelling 23 undeclared Russian intelligence agents, cutting off high-level diplomatic engagements, and strengthening powers to detain foreign intelligence operatives at the UK border.

Most powerfully, she lined up like-minded states around the world to hit back at Russia with coordinated expulsions. A range of allies (including Australia) acted in solidarity with the UK by expelling more than 100 undeclared Russian intelligence officers posted as diplomats[9].

This impressive response from the UK Government got me thinking about two questions.

- If a similar incident occurred in Australia, or any of the countries represented here today, do we have the appropriate whole-of-government structures in place to operate swiftly and effectively in our messaging?

And

- Are roles and responsibilities sufficiently clearly delineated across our Governments to allow our national security architecture to respond not just to the incident itself…..but also to how our response is framed….by the international media, by our own population, and by competitors – all of whom would be scrutinising our response?

While this is a Five Eyes forum, there are lessons to be learnt from other nations such as Sweden[10] and Finland[11]. Both nations have developed their own sovereign capabilities to mitigate the risks of political warfare, capabilities appropriate to their specific circumstances. Faced with the looming threat of Russian interference in their domestic politics, and military movements on their borders, both have developed whole-of-nation responses to information warfare.

The Swedish Civil Contingencies Agency has been responsible for preparing the Swedish population to defend against disinformation. The agency has trained Sweden's public service to identify and counter influence activity, developing a manual on crisis communications that is considered to represent best practice[12] in the field. The Swedish government also distributed a pamphlet on preparing for war and national disaster to every household in the country[13] following incursions into Swedish air space and maritime territory by Russian military aircraft and submarines.

---

[8] https://www.theguardian.com/uk-news/2018/mar/14/may-expels-23-russian-diplomats-response-spy-poisoning

[9] https://www.theguardian.com/uk-news/2018/mar/26/four-eu-states-set-to-expel-russian-diplomats-over-skripal-attack

[10] http://www.gmfus.org/blog/2018/09/07/sweden-preparing-wolf-not-crying-wolf-anticipating-and-tracking-influence

[11] https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/

[12] https://rib.msb.se/filer/pdf/28698.pdf

[13] https://www.theguardian.com/world/2018/may/21/sweden-distributes-be-prepared-for-war-cyber-terror-attack-leaflet-to-every-home

An impressive example of a nation building security and resilience concurrently.

Finland sees education as the first line of defence. It hosts the European Centre of Excellence for Countering Hybrid Threats, which develops best practice in responding to grey zone warfare[14]. In Finnish schools and adult education centres, a national program teaches students, citizens, journalists and politicians how to spot Russian disinformation [15]. The results are impressive. Finland tops the rankings for media literacy across European and Scandinavian nations.

There is a psychological element to these approaches.

I've said a number of times that citizens have become unwitting combatants in cyberspace.

Both Sweden and Finland recognise the importance of its society in whole-of-nation responses to information warfare. Their citizens are appropriately armed for the fight. Both nations want to make clear to competitors that their populations are actively mobilised in the defence of national sovereignty.

[Urgency of vulnerabilities]

I want to emphasise that the questions I'm posing today are not rhetorical. Only last month the outgoing Director General of ASIO, our domestic intelligence agency, Duncan Lewis, described foreign interference as an "existential threat"[16] to the nation.

We're not talking in abstract hypotheticals.

It's no surprise that Australia, as a modern liberal democracy, has high rates of internet penetration and social media use. This connectivity is vital to our economy and, these days, is essential to our way of life.

But there are a range of actors with the motivation and capability to contest our information environment, as well as those of our allies and regional security partners. These actors target us in the information environment.

And they erode trust.

- Trust in our institutions
- Trust in our values
- Trust in each other.

[14] https://www.hybridcoe.fi/
[15] https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/
[16] https://www.abc.net.au/news/2019-09-04/asio-chief-foreign-interference-more-of-a-threat-than-terrorism/11479796

Effects in the information environment can damage national interests. Dare I say sovereignty? They have the potential to damage the very foundations on which our societies are built.

[Evidence base]

Let's examine the evidence around how vulnerable we are in the information environment.

This is no small challenge.

We know that misinformation ripples across social networks at a pace that outstrips truth[17]. A recent study at MIT found that disinformation travels six times faster than the truth across Twitter[18]. As something of an academic snob, I'm not sure there's a PhD in that conclusion…..!

More than five million Australians use Twitter[19]. That's around one fifth of our population. To extrapolate that out, one fifth of the population can be reached, targeted and potentially influenced by a malign actor.

But that's just one slice of the population, and it's just one social media platform.

Personally, I've got a great deal of faith in the ability of many Australians to recognise disinformation when they see it. And even greater faith in today's digital savvy teenagers to question the source of the information they see, and vigorously prosecute fake news. My 21 year old daughter's willingness to question *everything and aeveryone* is a case in point…..

That doesn't change the fact that we are vulnerable.

As internet users, we've all been subjected to the results of Search Engine Optimisation – the buzz word for marketers and content developers around the world, spawning a generation of search engine experts.

Research[20] shows that the manipulation of search engine rankings can be so influential, they can nudge the voting preferences of undecided voters.

US Department of Justice investigations[21] reported that Russia's Internet Research Agency employs teams specifically to work on search engine optimisation.

In fact, research by the Alliance for Securing Democracy[22] has shown that this tactic was deployed following the attack on the Skripals in an effort to encourage conspiracy theories and to favourably re-shape the narrative around the attack to Russian interests. Concerningly, these techniques would be invisible to all but the most critical among us.

---

[17] https://science.sciencemag.org/content/359/6380/1146
[18] https://www.newscientist.com/article/2163226-fake-news-travels-six-times-faster-than-the-truth-on-twitter/
[19] https://www.socialmedianews.com.au/social-media-statistics-australia-august-2019/
[20] https://www.pnas.org/content/112/33/E4512
[21] https://www.justice.gov/opa/press-release/file/1102316/download
[22] https://securingdemocracy.gmfus.org/from-nord-stream-to-novichok-kremlin-propaganda-on-googles-front-page/

There are a number of features of the contemporary information environment that expose us to information warfare techniques and methods.

Social media has democratised the flow of information. Today, anyone can be a publisher, commentator, and/or an influencer. And with this enormous increase in the volume of information and communication, we all tailor our information flow to screen out noise.

We rely on trusted networks and sources[23]. We actively curate content, selectively adding metrics of approval – likes and shares – that drive the engagement of others.

These contemporary media consumption habits combined with information overload mean that networked citizens tend to lend credibility to information conveyed across their social networks rather than down from public institutions.

The veracity of a post is judged more on the number of followers and likes than it is on the content and credibility of the source.

This treatment of our individual information environments is significant as human perception is malleable, it is shaped by cognitive bias and emotional response[24]. The Cambridge Analytica experience highlighted the potential use of digital trace data – the footprints we leave behind as we interact with the web and social media – to build personality models that can provide greater precision and nuance in targeting propaganda and disinformation at social media audiences[25].

This approach – known as "psychographic"[26] messaging - means that disinformation by malign actors in the information environment can be targeted to specific audience segments indirectly, using an understanding of the bias inherent to their personality types and behavioural preferences.

Here malign actors are simply leveraging attention economy to exploit our less rational, more instinctive emotional responses. And they are not the only ones to do so.

It's no accident that the products we look at online then stalk us relentlessly across different web pages, and the online advertising we see aligns with the topic of our last Google search.

State and non-state actors are becoming increasingly adept at exploiting these behaviours to spread propaganda, deliver cognitive effects, and mobilise behavioural change.

And a range of sophisticated capabilities[27] will be available to state actors who invest in AI, big data and machine learning.

[Sovereign capability]

---

[23] https://theconversation.com/merchants-of-misinformation-are-all-over-the-internet-but-the-real-problem-lies-with-us-123177

[24] https://www.pnas.org/content/111/24/8788

[25] https://theconversation.com/how-cambridge-analyticas-facebook-targeting-model-really-worked-according-to-the-person-who-built-it-94078

[26] https://theconversation.com/psychographics-the-behavioural-analysis-that-helped-cambridge-analytica-know-voters-minds-93675

[27] https://warontherocks.com/2019/08/the-coming-automation-of-propaganda/

The informational element of Australia's statecraft needs a focus, a champion, so that we can assert our values, our national power, in the information environment.

The development of sovereign capability to contest in the information environment requires that the ADF, Australia's national security community and the Australian public have a shared understanding of our own vulnerabilities, of the threats arrayed against us, and a shared vision of the resilience with which we need to respond.

Within Information Warfare Division, we have completed a range of initiatives to modernise our capability:

- Designing a cyber worthiness and mission assurance framework for the joint force;

- Accelerating Force Structure Review workforce growth from 10 years to 4 years, complete by 2023 to meet the challenges created by an increasingly complicated operating environment;

- Increased investment in Information Warfare Facilities to ensure that they are future-proofed, ensuring that joint and inter-agency Cyber Warfare training, education, and operations needs can be accommodated;

- With our Five Eyes partners, we've stood up Accelerated Defensive Cyber Training for selected ADF personnel to rapidly grow the ADF cyber workforce. In two-years we've certified almost 100 Defensive Cyber Operators;

- Designed and implemented the Cyber Training Framework for Defence and created a sovereign joint cyber training continuum that will commence in 2021;

- Ensuring that conditions of service for Navy, Army and Air Force cyber operators are aligned;

- And, we're working towards improving the organisational structures, and command and control arrangements, for our cyber forces across the Defence portfolio.

But as you can see, this is all cyber and threats in the information environment are far broader than that.

Our focus now will be to take the hard-learnt lessons from building the ADF's cyber capability and transferring that to Electronic Warfare, Intelligence, and Influence Activities. The whole is always greater than the sum of its parts and our competitors have achieved advantage because they have understood this.

In my 2017 strategy I stated that Information Warfare is "the contest for the prevision and assurance of information to support friendly decision-making whilst denying and degrading that of adversaries". As you can see, this was very military focussed. Two years later – and

with a greater appreciation of the threat and challenges – I propose a broader boundary that demands greater coordination and response across departments and agencies.

Our sovereign capability will reflect Australia's unique circumstances and national interests, our regional positioning, the assertion of our values in the service of our interests, our preferred language to shape our messaging – but will align with the capabilities of our Five Eyes allies.

Authoritarian regimes, revisionist powers, extremist groups; these actors all want us to understand their disregard for the rule of law and the international rules-based order. There is an informational element to their strategy and tactics – each action conveys a message.

As Laura Rosenberger, Director of the Alliance for Securing Democracy puts it; "Borders and distances no longer protect against many of the threats democracies face, the battle is not just for territory but for minds"[28]. Democracies must develop resilience to such threats at the whole-of-nation level. This requires initiatives that are coordinated across government, and in partnership with the private sector and civil society.

The ADF can play a role in this, we can make a positive contribution. But we need to sit within a defined place within a whole-of-government structure, to have the appropriate mandate to make that contribution.

We need to galvanise international partnership between like-minded allies.

But first we need to have a clearly articulated mandate. What is that?

There are strict and entirely appropriate legal constraints of the use of the ADF in a domestic setting. But I do sense that there is a requirement for a detailed discussion to address the questions

- What is the role of the ADF in this space, and does its traditional bookends still make sense in the New Information Environment?

- Are the other departments, agencies and the public happy for its military to sit idly by in this contest?

Australia's focus on the Pacific step-up[29] requires us to project a clear vision for the region and our role in it.

We need to assert our values as strengths – democratic values and transparency, an independent and high-quality media. As Prime Minister Morrison recently said in Jakarta: "In an era of rapid change and uncertainty, we must know who we are, what we offer and what we're about."[30]

We need to reassure our own population that ADF operations continue to be framed:

---

[28] http://www.gmfus.org/publications/authoritarian-advance-how-authoritarian-regimes-upended-assumptions-about-democratic

[29] https://dfat.gov.au/geo/pacific/engagement/Pages/stepping-up-australias-pacific-engagement.aspx

[30] https://www.pm.gov.au/media/speech-singapore

- by ministerial authorisation;
- by rules of engagement reflecting our values and legal obligations; adherence to our international obligations;
- by domestic and international law;
- and, by the same moral and ethical baseline that makes the ADF the most trusted entity in Australia.

We must deploy capabilities that enhance our capacity for early warning and situational understanding. We need to promote a positive image of Australia's - and the ADF's - involvement in the region. And we need to disrupt and expose the information activities of malign actors.

To develop our capacity for contemporary information warfare, we need to be imaginative, we need to be agile and most critically we need to work together.

I come back to my original questions.

- How do we have a meaningful conversation with the public about a contested environment they may know very little about?
- How do we build national resilience towards malign influence and activities in the New Information Environment?
- And what is the role of the military in a whole of government response?

We have an impressive array of speakers and participants on the programme, and I urge you to immerse yourselves in the conversations around you.

Let's not be ignorant to the fundamental role of the I in DIME, nor afraid to consider how best to champion information as an instrument of national power.

I'll finish by again welcoming you to the Forum, and I'm looking forward to the discussion over the next couple of days.

Thank you.