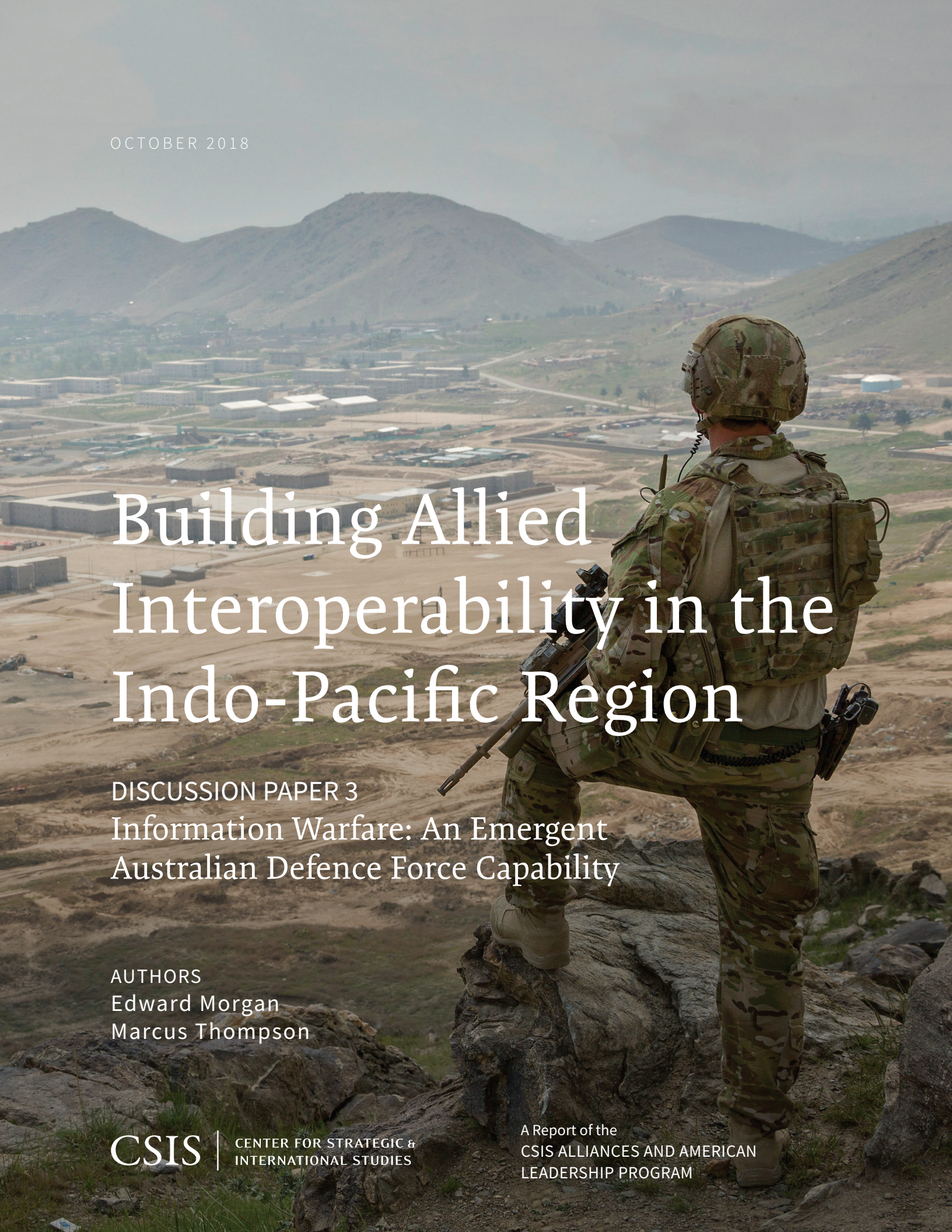


OCTOBER 2018

Building Allied Interoperability in the Indo-Pacific Region

DISCUSSION PAPER 3

Information Warfare: An Emergent Australian Defence Force Capability

AUTHORS
Edward Morgan
Marcus Thompson

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

A Report of the
CSIS ALLIANCES AND AMERICAN LEADERSHIP PROGRAM

OCTOBER 2018

Building Allied Interoperability in the Indo-Pacific Region

DISCUSSION PAPER 3
Information Warfare: An Emergent Australian Defence Force Capability

AUTHORS
Edward Morgan
Marcus Thompson

A Report of the CSIS Alliances and American Leadership Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in November 2015. Former U.S. deputy secretary of defense John J. Hamre has served as the Center's president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Acknowledgments
This report is made possible by the generous support of the governments of Australia and Japan.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Contents

"There is nothing new in cyber warfare; what it requires is the application of old or established military methods in a new warfighting environment.

The ADF must understand, and become masters of, the information environment."

Major General Marcus Thompson, Deputy Chief of Information Warfare, Australian Defence Force Headquarters, November 2017.[1]

[1] Remarks by Deputy Chief Information Warfare, Australian Defence Force (ADF), Major General Marcus Thompson, to the Military Communications and Information Systems Conference (MILCIS), November 17, 2017, Canberra, Australia. Elements of this article have drawn from that speech.

Foreword | Information Warfare and the Indo-Pacific: Fracture and Coherence

This paper forms part of a CSIS series on Indo-Pacific interoperability.

As such, it seeks to provide an account of the developing information warfare capabilities of one Indo-Pacific country, Australia.

Specifically, this paper seeks to account for the developing information warfare capabilities of the Australian Defence Force (ADF), one arm of the Australian government.

The Indo-Pacific is a region that is increasingly recognized as a geographically distinctive strategic system. However, the paper recognizes that individual countries in the Indo-Pacific can and will develop their strategic and military capabilities independently.

This paper therefore seeks to set out Australia's developing information warfare capabilities with a view to generating discussion between Indo-Pacific security partners and allies on the nature of information warfare in a modern context and the capabilities and frameworks required to meet this emergent challenge.

The timing for such discussion is significant:

- In 2018, the Australian government passed laws into its parliament restricting foreign ownership of Australian assets such as electricity grids, while also tightening laws against foreign interference.[2] Reports suggested the laws were aimed at China.[3]

- During the same period, 13 Russians were charged by U.S. courts with tampering with the 2016 U.S. federal elections.[4]

Both of these events were unprecedented in recent memory, and information capabilities sat at the heart of both.

---

[2] Parliament of Australia, *Security of Critical Infrastructure Act 2018*, https://www.legislation.gov.au/Details/C2018A00029; Parliament of Australia, *Foreign Influence Transparency Scheme Bill 2018*, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6018; Parliament of Australia, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018*, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6022.

[3] "China put on notice by Australia's anti-interference laws," *Bloomberg*, June 26, 2018, https://www.bloomberg.com/news/articles/2018-06-27/china-put-on-notice-by-australia-s-anti-interference-laws; "Australia passed sweeping foreign interference laws not-so-subtly targeted at China," *Business Insider*, June 28, 2018, https://www.businessinsider.com/australia-passed-foreign-interference-laws-amid-china-tensions-2018-6. The Australian prime minister denied the accusation: "Australia passes foreign interference laws amid China tension," BBC News, June 28, 2018, https://www.bbc.com/news/world-australia-44624270.

[4] "Russia-Trump inquiry: Russians charged over US 2016 election tampering," BBC News, February 17, 2018, https://www.bbc.com/news/world-us-canada-43092085.

Information capabilities possess the potential to disrupt or break an emergent strategic system like the Indo-Pacific, or to cohere it more tightly:

- The task for existing Indo-Pacific allies like Australia, Japan, and the United States is to bring their insights into alliance management to bear on the development of new relationships and partnerships in the Indo-Pacific information environment.

- This will require flexibility, creativity, and pragmatism to achieve. It will also require technical and material insight into the nature of the information environment as it might relate to warfare.

This paper seeks to develop the beginnings of such flexibility, creativity, and pragmatism. Its authors will welcome the feedback of peers on the proposals outlined within.

Washington, D.C.
October 2018

Executive Summary

The Australian Defence Force's (ADF) emergent information warfare (IW) capabilities exist within the framework of Australia's developing cyber policy at the strategic level. A lack of specific Australian guidance around the military use of information capabilities, including cyber, prompts three crucial questions:

What is IW for the ADF?

The ADF possesses a working description rather than a definition of IW as "the context for the provision and assurance of information to support friendly decision-making, whilst denying and degrading that of adversaries." The working description provides the ADF with doctrinal flexibility in the information environment (IE) at the same time as nation-states like Russia have integrated their information capabilities with their conventional forces. The ADF's working description of IW means the ADF can participate in the information "contest" wherever it occurs across the traditional spectrum of conflict.

What threat is the ADF facing from IW?

The ADF faces a four-fold threat in IW, emanating from (1) nation-states who seek to integrate IW capabilities into their conventional combined forces; (2) non-state actors such as terrorist organizations or insurgent groups; (3) "grey-zone" threats from state and non-state actors in the information environment; and (4) the ADF's inexperience operating in the IE, which generates avoidable, but potentially lethal, IE errors. The ADF faces the additional risk of not integrating its tactical and strategic-level IW capabilities at a time when Australia's national security infrastructure is undergoing significant organizational and legal changes.

How will the ADF address the IW threat?

The ADF will address the IW threat through its newly established Information Warfare Division (IWD) which will lead ADF IW capability development across five focus areas: (1) IW and joint warfighting; (2) C4 systems and information; (3) the cognitive dimension of information capabilities; (4) people and personnel; and (5) international engagement. These support ADF cyberspace operations spanning offensive cyber, active cyber defense, passive cyber defense, and cyber self-defense. Respectively these focuses help the ADF integrate with Australian government agencies, international allies, and a broad range of security partners in the IE.

The Australian government's urgent priority on the ADF's IW capability development is reflected in IW's funding of 0.18 percent of Australia's gross domestic product over 10 years. This compels the ADF's IW capability development but will need to occur alongside the ADF's evolution of its warfare theory to ensure the ADF's IW capability remains within its moral and legal traditions. This may include the re-examination of the laws of armed conflict in the light of new uses of emergent information technology in warfare.

The Question of Strategic Interests

The question of Australia's strategic interests must lie at the heart of Australia's discussion of information warfare.

There are a number of reasons for this.

Firstly, "information warfare" is a relatively new term in its modern incarnation. While information has always played a crucial part of warfare, the modern terminology associated with it is frequently linked to digital capabilities and, more specifically, to "cyber warfare."

Thus, for Australia to have a coherent conversation about the role of information in modern warfare, it will need to define where "information" in the twenty-first century is situated across the normal spectrum of conflict.

Secondly, Australia has already mapped out its strategic interests across a number of *Defence White Papers* and most recently in the *2017 Foreign Policy White Paper*.[5]

Australia's defense interests, as stated succinctly in the *2016 Defence White Paper*, are:

1. A secure, resilient Australia, with secure northern approaches and proximate sea lines of communication.
2. A secure nearer region, encompassing maritime Southeast Asia and the South Pacific.
3. A stable Indo-Pacific and a rules-based global order.[6]

Information warfare—or the use of information in a digital or information age for warfare purposes—sits across all these Strategic Defence Interests. It also sits integrated with the Strategic Defence Objectives which support them.[7]

[5] Australian Government, *2017 Foreign Policy White Paper*, https://www.fpwhitepaper.gov.au/foreign-policy-white-paper. For the most recent *Defence White Paper*, see: Australian Government, 2016 Defence White Paper, http://www.defence.gov.au/WhitePaper/.
[6] Australian Government, *2016 Defence White Paper*, p. 68. http://www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf.
[7] Ibid.

Australia's *Foreign Policy White Paper*, similarly, sets out the challenges of Australia's foreign policy objectives in the following way:

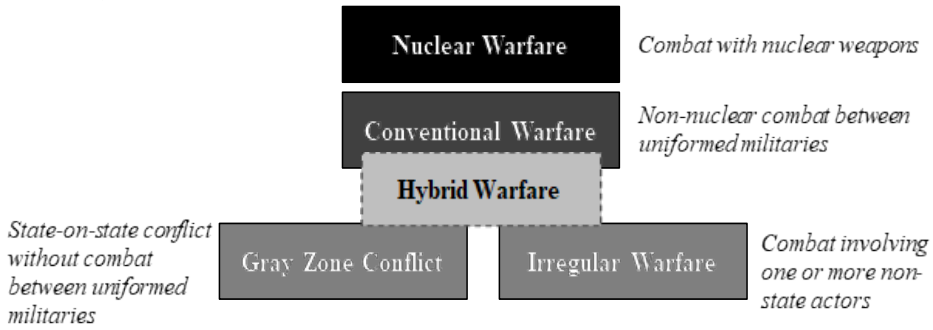
1. Promote an open, inclusive, and prosperous Indo-Pacific region in which the rights of all states are respected.
2. Deliver more opportunities for Australian businesses globally and stand against protectionism.
3. Ensure Australians remain safe, secure, and free in the face of threats such as terrorism.
4. Promote and protect the international rules that support stability and prosperity and enable cooperation to tackle global challenges.
5. Step up support for a more resilient Pacific and Timor-Leste.[8]

Information and its use in acquiring national power objectives could sit across, or integrated into, any of these frames of strategic reference.[9]

Figure 1: Spectrum of Conflict Diagrams

The issue of where information capabilities sit on the traditional spectrum of conflict is vexed but arguably simple. The proliferation of information capabilities means they could be framed anywhere within traditional and non-traditional settings. The two diagrams below express a traditional and "unconventional" view of the so-called spectrum of conflict.

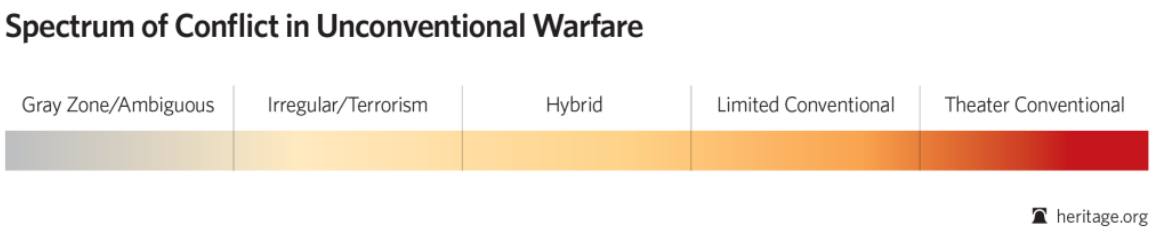
1. **The traditional spectrum of conflict**, with "hybrid" warfare sitting positioned between them. Information capabilities span all five of these boxes comfortably, in different proportions according to context.



Source: Zack Cooper and Andrew Shearer, "Thinking clearly about China's layered Indo-Pacific strategy," Bulletin of the Atomic Scientists 73:5 (September 2017): p. 308.

[8] Australian Government, *2017 Foreign Policy White Paper*, p. 3, https://www.fpwhitepaper.gov.au/foreign-policy-white-paper.
[9] Cyber can arguably sit within any context of conflict dependent on where the conflict is being waged. Discussion on the traditional "spectrum of conflict" and cyber is ongoing. See: Thomas Ricks, "The future of war: cyber is expanding the Clausewitzian spectrum of conflict," *Foreign Policy*, November 13, 2014, https://foreignpolicy.com/2014/11/13/the-future-of-war-cyber-is-expanding-the-clausewitzian-spectrum-of-conflict/; Matthew J. Flynn, "The cyber spectrum of conflict," http://newconflict.org/spectrum%20of%20conflict.html; Bonnie Adkins, "The Spectrum of cyber conflict from hacking to information warfare: what is law enforcement's role?" diss., Air Command and Staff College, Air University, 2001, http://www.dtic.mil/dtic/tr/fulltext/u2/a406949.pdf.

2. **The spectrum of conflict in unconventional warfare** presents a similar but linear picture. Information capabilities, again, can sit across all of these and in different levels of intensity.



Source: Frank Hoffman, "The contemporary spectrum of conflict. Protracted gray-zone, ambiguous, and hybrid modes of war," The Heritage Foundation, 2016 Index of Military Strength, https://index.heritage.org/military/2016/essays/contemporary-spectrum-of-conflict/.

We think information capabilities are "unmapped" in a contemporary environment. Most attempts to do so fall short of the dependencies the military, other parts of government, and society are coming to accept as normal for information capabilities, cyber especially.

We therefore consider information capabilities as "emergent," still seeking both language and concepts to become normative for discussions of warfare.

Additional to these two key strategic documents, Australia possesses two cyber-specific documents relevant to the discussion of information warfare. They are Australia's International Cyber Engagement Strategy, released in 2016, and Australia's Cyber Security Strategy, whose first update was released in 2017.[10] These set out Australia's cyber interests in terms coherent with the core strategic documents of both the Australian Department of Defence and the Australian Department of Foreign Affairs and Trade's (DFAT):

[10] Australian Government, "Australia's International Cyber Engagement Strategy," http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html; "Australia's Cyber Security Strategy First Annual Update," https://cybersecuritystrategy.pmc.gov.au/first-annual-update/.

Australia's Cyber Policy Documents		
Focus Area	**Australia's International Cyber Engagement Strategy**	**Australia's Cyber Security Strategy (2016, updated 2017)**
1	Maximise the opportunity for economic growth and prosperity through digital trade.	A national cyber partnership between government, researchers, and business including regular meetings to strengthen leadership and tackle emerging issues.
2	Stronger cybercrime prevention, prosecution, and cooperation, with a focus on the Indo-Pacific.	Stronger cyber defences to better detect, deter, and respond to threats and anticipate risks.
3	A stable and peaceful online environment.	Global responsibility and influence to champion a secure, open, and free internet while building capacity to crack down on cyber criminals and shut safe havens for cybercrime.
4	An open, free, and secure internet achieved through a multi-stakeholder approach to internet governance and cooperation.	Growth and innovation to support the Australian cybersecurity sector to grow and prosper and ensure all Australian businesses can operate securely online.
5	Human rights apply online as they do offline.	A cyber smart nation to grow a highly skilled cybersecurity workforce and ensure all Australians are aware of the risks and benefits of being online.
6	Digital technologies are used to achieve sustainable development and inclusive economic growth in the Indo-Pacific.	
	Source: Australian Government, "Australia's International Cyber Engagement Strategy," http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html.	Source: Australian Government, "Australia's Cyber Security Strategy First Annual Update," https://cybersecuritystrategy.pmc.gov.au/first-annual-update/.

As can be seen from comparing these documents, Australia's top-level strategic planning documents are coherent across a spectrum of cybersecurity and economic growth, especially regarding a focus on developing technologies.

These documents also make clear that Australia has already advanced strongly in understanding the question of information capabilities as elements of national power. This means that for the question of "information warfare" to be addressed, an account is first required of what this form of "warfare" is and how it relates to conflict as that is traditionally understood.

This paper will set this out across three key areas:

1. What is “information warfare” for the ADF?
2. What threat is the ADF and/or Australia facing from information warfare?
3. How will the ADF address the information warfare threat?

The paper addresses the final question in terms of the ADF’s strategic focus areas for information warfare as well as the beginnings of the ADF’s core concepts for its information warfare capability development.

Section 1 | What Is Information Warfare for the ADF?

A definition of information warfare is difficult to come by. This is in part due to what we will describe as the "emergent" character of the modern information environment. The proliferation of digital information systems is relatively recent and with it has come an intense discussion of the competition being played out using digital information systems. These span military, economic, and diplomatic spheres.

It is also because, historically, the relationship between the term "warfare" and "information" has arguably never been as close as it is today. While the use of information as part of war is as old as war itself—for deception, persuasion, and battlefield communication, among other things—the near-universal use of modern, digitized "information systems" for military decisionmaking has amplified the importance of information's fidelity in the battlespace. This, in turn, has led to increased demands for what is referred to as "information assurance" and the security of the systems modern militaries use to prosecute their actions.

A U.S. Definition of Information Warfare and Its Context

One succinct U.S. definition of "information warfare" is:

> Information warfare is conflict between two or more groups in the information environment.[11]

The information environment is defined elsewhere by the U.S. Department of Defense's Joint Publication (JP) 1-02 as:

> The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.[12]

Western countries may have struggled to find a definition for the term "information warfare" due to their tradition of identifying information activities during war as "information operations" (IO), which support a particular war. Put differently, the deliberate strategic military use of information has been described as a subset of a larger strategic engagement where lethal, or "kinetic," activity takes place. Thus, the United States describes IO as:

> The integrated employment during military operations of information-related capabilities (IRCs), in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-

[11] Isaac Porsche et al., *Redefining Information Warfare Boundaries for an Army in a Wireless World*, (Washington, D.C.: RAND Corporation, 2013), p. 14. The article refers to Dan Kuehl of the National Defense University as offering similar definition, "Military offensive and defensive actions to control/exploit the [information] environment."

[12] "U.S. Dictionary of Military and Associated Terms," U.S. Joint Publication (JP) 1-02, p. 110, https://fas.org/irp/doddir/dod/jp1_02.pdf. The U.S. 2018 Joint Doctrine Note on strategy describes an "Information Instrument" as comprised of "the infrastructure, capabilities, and processes by which a state or non-state gathers, analyses, disseminates, and exploits information." These are "crucial foundational and institutional dimensions of power." US Department of Defense, *Joint Doctrine Note. Strategy*, 25 April, 2018, p. II-6, http://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_18.pdf?ver=2018-04-25-150439-540 . The Joint Doctrine Note helps understand the complexity of the definition problem, since the abstract of an "Information Instrument" still requires multiple physical and non-physical parts to compose it, in "infrastructure, capabilities and processes." A singular definition of "information warfare" becomes harder to construct because its core instrument is complex and abstract. Concerning complexity, its parts can belong to peacetime capabilities at the same time as they belong to an instrument of war. The infrastructure used to deliver a cyberattack, for example, can simultaneously be used for peacetime purposes. This complicates targeting and attribution, among other things.

> making of adversaries and potential adversaries while protecting our own. IO integrates the application of force and the employment of information with the goal of affecting the perception and will of adversaries.[13]

Importantly, the U.S. definitions do not describe IO as a lethal activity except by analogy to "fires" in traditional warfighting domains:

> The integration of IRCs for effect can be compared to fire support coordination, in which a targeting methodology synchronizes and employs various capabilities to generate desired effects. It is the integration and synchronization of IRCs that enables desired effects in and through the IE at specified times and locations.[14]

Meta-questions of integration and synchronization remain the emphasis of U.S. doctrinal discussion about the use of information in its modern conflict settings. This suggests that the concept of warfare in the information environment has some distance to travel before being reconciled to traditional frameworks for authorized lethal military activity.

The ADF's Description of Information Warfare and Some Global Context

The ADF has not, to date, settled on a definition of information warfare as much as a working description of it. In unpublished material, it is as follows:

> The contest for the provision and assurance of information to support friendly decision-making, whilst denying and degrading that of adversaries.[15]

The ADF's description of information warfare is significant for deliberately avoiding the definition of "combat" or "conflict" in the information environment, describing it instead as a contest which can take place in any situation across the spectrum of war or peace.

The ADF's reticence to leap to a definition is in part connected to the U.S. settings described above. The ADF has traditionally described information activities as part of information operations, aligning thus with the United States and NATO countries.[16] The ADF has not traditionally described itself as conducting information "war", and its new journey into information capabilities for warfare is taking place as policy-makers and planners seek clearer ways to characterize the use of such capabilities in conflict settings.

---

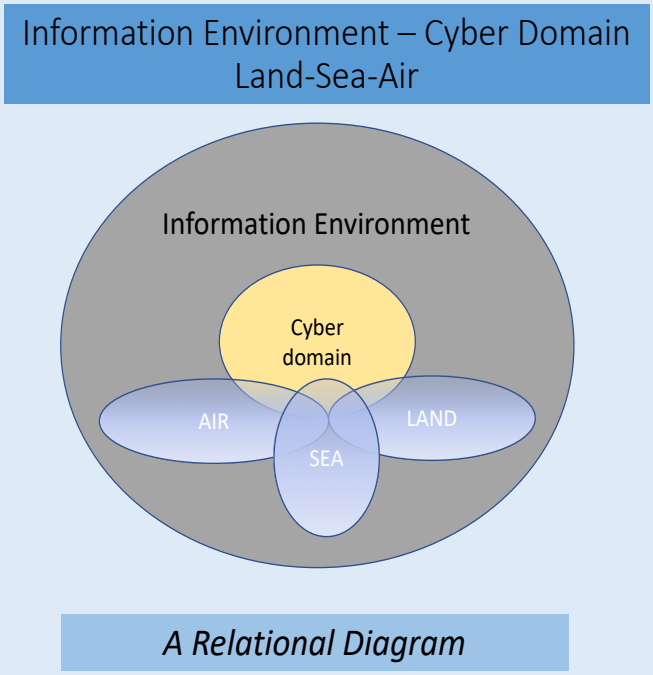
[13] U.S. Department of Defense, "Strategy for Operations in the Information Environment," June 2016, p. 3, https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf. See also U.S. Department of Defense, Directive 3600.01, Information Operations, May 2, 2013, https://fas.org/irp/doddir/dod/d3600_01.pdf.
[14] U.S. Department of Defense, "Strategy for Operations in the Information Environment," p. 3.
[15] ADF description of information warfare taken from unclassified, unpublished 2017 ADF information warfare documents from the Australian Department of Defence.
[16] See: "Operation Series: Information Activities," *Australian Defence Doctrine Publication* 3.13 (ADDP 3.13), 2013, http://www.defence.gov.au/FOI/Docs/Disclosures/330_1314_Document.pdf; NATO, "Allied Joint Doctrine for Information Operations," Allied Joint Publication (AJP-3.10), November 2009, https://info.publicintelligence.net/NATO-IO.pdf.

Figure 2: The Information Environment, Cyber, and Traditional Warfighting Domains

The question of whether the information environment is a "domain" of warfighting or whether it contains other domains within it has been widely discussed.[17]

For the purposes of this paper, the ADF describes the relationship between the information environment and the traditional warfighting domains in the following way:

The ADF's Understanding of the Traditional Domains of Warfighting in Relation to Cyber and the Information Environment.



Of note:

1. Cyber is considered a domain in which warfighting occurs, which interlinks with the traditional warfighting domains of air, land, and sea.
2. The information environment encompasses all domains because of its pervasiveness. This is an appropriate frame of reference because information-related capabilities are not limited to cyber capabilities, and they exist outside the military context in which the ADF uses them.

U.S. doctrine describes cyberspace as "*a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.*"[18]

[17] For academic discussion, see, inter alia: G. Alexander Crowther, "National Defense and the Cyber Domain," The Heritage Foundation, Oct 5, 2017, https://www.heritage.org/military-strength/national-defense-and-the-cyber-domain; David Aucsmith,"Cyberspace Is a Domain of War," War in Cyberspace, May 26, 2012, https://cyberbelli.com/2012/05/26/cyberspace-is-a-domain-of-war/; and Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society*, vol. 8, no. 2 (2012): 321–336, http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf.

As one Russian theorist recently put it:

> A new type of war has emerged, in which armed warfare has given up its decisive place in the achievement of the military and political objectives of war to another kind of warfare – information warfare.[19]

Vladimir Kvachkov's remark is arguably overstated, in that it seems unlikely conventional military conflict will be decisively replaced by the capabilities of the information environment. However, Russia's experience of modern cyber warfare has taken much from its own defeats in the information environment. Reflecting on Russia's experience in the First Chechen War, Russian Chief of the General Staff Viktor Samsonov stated in 1996 that:

> [The] high effectiveness of [Chechen] information warfare systems . . . made it possible to disorganize the system of state administration, hit strategically important installations and groupings of forces, and affect the mentality and moral spirit of the population. In other words, the effect of using these means is comparable with the damage resulting from the effect of weapons of mass destruction.[20]

This suggests that Russia's experience of defeat at the hands of a skillful cyber enemy is what propelled Russia onto the stage as a modern actor in the information environment. This is in addition to Russia's historical doctrine, which contains strong precedent for Russia's developing information warfare capabilities.[21]

Russia's use of information capabilities progressed rapidly in light of its experience in Chechnya in the 1990s. Several open-source commentators have suggested that Russia has now effectively integrated its information-related capabilities with mainstream conventional military capabilities. Evidence of this was seen in Russia's successful attacks on Estonia in 2007, Georgia in 2008, Kyrgyzstan in 2009, and Ukraine in 2014.[22] Russia's experimentation with and use of cyber capabilities, in tandem with conventional military operations, has provided early indication of the potency of offensive cyber as a weapon of war.[23]

---

[18] U.S. Department of Defense Dictionary, U.S. Department of Defense, p.59 http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf; and Cyberspace Operations, Joint Publication 3-12, June 8, 2018, Glossary 4 (GL-4), https://fas.org/irp/doddir/dod/jp3_12.pdf.

[19] Vladimir Kvachkov, *Russia's Special Purpose Forces* (Moscow: Voyennaya Literatura, 2004).

[20] General Viktor Samsonov, Chief of the Russian General Staff, cited in T. Thomas, *Manipulating the Mass Consciousness: Russian and Chechen Information War Tactics in the 2nd Chechen-Russian Conflict*, Foreign Military Studies Office, 2003.

[21] For a good description of Russian doctrine in information warfare see: Michael Connell and Sarah Volger, *Russia's Approach to Cyber Warfare*, CNA, March 2017, https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf. Connell and Volger's article notes that for Russia, "cyber is regarded as a mechanism for enabling the state to dominate the information landscape, which is regarded as a warfare domain in its own right" (p. 3). It further cites Russian Federation military doctrine, which is clear in its intent around information war: "the prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favorable response from the world community to the utilization of military force," from The Military Doctrine of the Russian Federation, February 5, 2010, (translated), http://carnegieendowment.org/files/2010russia_military_doctrine.pdf.

[22] Connell and Volger, *Russia's Approach to Cyber Warfare*, 13-22. See also for excellent discussion on Russian information warfare: Keir Giles, *Handbook of Russian Information Warfare* (Rome: NATO Defence College, Fellowship Monograph, 2016), https://krypt3ia.files.wordpress.com/2016/12/fm_9.pdf. Giles' account is detailed and extensive on Russia's information warfare approach, setting it also in its historical context. Russia's practice in its near region is discussed throughout, most notably in Georgia and the Ukraine.

[23] Tom O'Connor, "U.S. Military and NATO May Now Target Russia with Cyberweapons, Marking Huge Policy Change," *Newsweek*, December 13, 2017, http://www.newsweek.com/nato-may-target-russia-cyber-weapons-marking-huge-policy-change-747697. NATO's response to Russia is perhaps the most telling, with NATO shifting to permit cyber against Russia. This suggests the perception of the Russian threat has moved beyond theory to practice. Sergei Medvedev, "Offense-Defense Theory Analysis of Russian Cyber Capability," master's thesis, submitted to Naval Postgraduate School, Monterey, California, 2015,

Russia has also been accused of using information capabilities to tamper with the 2016 U.S. federal elections.[24] Such activities are argued to belong to a broader, integrated, and whole-of-nation strategy.[25] This makes sense due to the constraints on Russia's defense budget and the highly cost-effective complement that information capabilities provide to Russia's conventional military forces. The views imply that Russia is seeking to lead the way in the development of information capabilities to prosecute nation-state influence well beyond the military battlefield. For some, this means that "war" should now be a term extended to cover cyberattacks, with policy developed for to identify when such attacks constitute an act of war.[26] This includes the consideration of "intangible effects of significant scope, intensity, or duration" which are the result of such attacks.[27] Others have called for ideological "political warfare", as practiced by Marxist-Leninist States during the Cold War, to be re-described under a strategic concept of "comprehensive coercion."[28]

These remain for the meantime theoretical frameworks and Australia is some way from achieving a legal definition of information warfare. Such a definition might include conceptual and legal frameworks for countering coercion or responding proportionately to nation-states who direct cyberattacks, as one weapon of information war, at Australia.[29] Such a definition might also include the concept of war as that is traditionally considered in relation to any newly described legal term of "information warfare." It would certainly need to account for hostile actors' potential to interfere with information systems to generate direct lethal effects, such as the downing of aircraft.[30]

These discussions, and any legal developments in their regard, are of considerable interest to the ADF. But for the purposes of this paper, we note that the ADF continues to account for "contest" in the information environment rather than "conflict." Notwithstanding the ADF's information warfare capability is still in development, the ADF will continue to be involved in the information contest wherever it occurs in either peace or war.

---

https://calhoun.nps.edu/bitstream/handle/10945/45225/15Mar_Medvedev_Sergei.pdf;sequence=3. A conservative assessment of Russia's cyber activity suggests Russia's use of cyber is offensive, even though it sits within an "offense-defense" theory of international relations. E. Iasiello, "Are cyber weapons effective military tools", *Military and Strategic Affairs*, vol. 7, no. 1, March 2015, p. 36, http://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/SystemFiles/2_Iasiello.pdf. This estimate cedes that cyber will almost certainly become a weapon of state-on-state war, even though it isn't quite there yet.

[24] Warren Strobel et al., "US charges Russians with 2016 U.S. election tampering to boost Trump," Reuters, February 16 , 2018, https://www.reuters.com/article/us-usa-trump-russia-indictment/u-s-charges-russians-with-2016-u-s-election-tampering-to-boost-trump-idUSKCN1G022U. This is just one example among numerous reports.

[25] Giles, *Handbook of Russian Information Warfare*, 3. Giles cites Russian President Vladimir Putin, "[T]he concept of information warfare 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." 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 (accessed 22 June 2016)). Emphasis ours. See also the excellent article: Dmitry (Dima) Adamsky, "From Moscow with coercion: Russian deterrence theory and strategic culture," *Journal of Strategic Studies*, 41:1-2, July 2017, p. 33-60, https://doi.org/10.1080/01402390.2017.1347872. Adamsky likewise emphasizes the integration of Russia's information capabilities with its nuclear and conventional capabilities but illuminates the Russian cultural context of Russian deterrence thinking (p. 35).

[26] See, for example, attempts in the U.S. Congress to define specific acts of cyber war. "Cyber War Act of 2016," https://www.rounds.senate.gov/imo/media/doc/Bill,%20NDAA%202017%20Related,%20Cyber%20Act%20of%20War.pdf.

[27] Ibid.

[28] Thomas G. Mahnken et al., *Countering Comprehensive Coercion: Competitive Strategies Against Authoritarian Political Warfare* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2018), esp. p. 3-42. For an excellent study, this outstanding work covers both Russia and China.

[29] Australia's 2018 foreign interference legislation might form part of such considerations. See footnote 2 above for references to this legislation.

[30] A fictional but compelling account of this potential is contained in P.W. Singer and August Cole's, *Ghost Fleet: A Novel of the Next World War*.

Section 2 | What Threat Is the ADF Facing from Information Warfare?

At the Australian National Press Club in October 2017, then Australian Minister Assisting the Prime Minister for Cyber Security, the Honourable Dan Tehan MP, declared there had been some 47,000 cyber "incidents" in Australia during the previous year.[31] This was a 15 percent increase in such events from the previous year. The minister gave no further definition of the nature or type of these attacks—not distinguishing, for example, between cyber intrusion and deliberate, mass denial of service events.

However, the scale of the numbers was the minister's point to drive home. If any proportion of these numbers was configured as an "attack" in the traditional sense of that word—a force emanating from another nation state with a view to degrading or destroying Australia's national capabilities—Australia had not been under such bombardment since World War II.

The ADF's allies have for some time been seeking language, concept, and capability to account for a potentially catastrophic cyber risk to their networked battle systems. At a recent conference in the United Kingdom, the UK chief of the general staff remarked that "a cyber 9/11 could already have happened, and we wouldn't even know about it."[32] The U.S. Navy recently chose temporarily not to certify its new Aegis Class upgrade—Aegis Baseline 9—based on classified cyber vulnerabilities.[33] These remarks by UK senior leadership, and the significant body-language of the U.S. Navy, amount to a tacit acknowledgement of the depth of cyber risk in an increasingly networked world.

Australian Air Vice-Marshal Warren McDonald recently noted that one of the most critical threats to the ADF is not external attack against the ADF and its systems, but the ADF's own members. McDonald observed that, during the ADF's 2017 combined coalition Exercise Talisman Sabre with the United States, ADF members had considerably let themselves and their colleagues down through poor cyber practices:

> The number of security breaches detected by our cyber Red Teams, on Talisman Sabre, was simply unacceptable. Very early in this exercise, locations of named individuals and the movements of units were discovered on an embarrassing scale. The most egregious act was the posting of a battle map on social media. No warrior would do that![34]

---

[31] Hon. Dan Tehan MP, National Press Club Address, "Silent Dangers – Launch of the Australian Cyber Security Centre's 2017 Threat Report," October 10, 2017, https://ministers.pmc.gov.au/tehan/2017/npc-launch-australian-cyber-security-centre-2017-threat-report.

[32] Reported remarks of General Mark Carleton-Smith at Royal United Services Institute (RUSI) Land Warfare Conference, June 19-20, 2018.

[33] "FY17 Navy Programs: Aegis Modernisation Program," Director, Operational Test and Evaluation, FY17 Annual Report, January 2018, p. 39, http://www.dote.osd.mil/pub/reports/FY2017/pdf/navy/2017aegis.pdf. "The Navy's Aegis Baseline 9.A and Aegis Ashore installation (Baseline 9.B) cybersecurity testing identified deficiencies, which are classified. The nature of these deficiencies is such that they could pose significant operational risk in a cyber-contested environment. The implementation of fixes to previous problems is not anticipated until ACB-16; therefore, the Navy and DOT&E cancelled cybersecurity testing of Baseline 9.C1, which will instead take place during ACB-16 operational testing."

[34] Remarks of Air Vice-Marshal Warren McDonald, Chief of Joint Capabilities, Australian Defence Force Headquarters, to the Air Power Symposium 2018, March 2018, Canberra, Australia.

McDonald's remarks were a sharp reminder to the ADF that not only has the world changed substantially because of information technologies, its war fighters must now move to keep pace with the changed nature of threat in the new information environment.

This suggests that the ADF is facing a fourfold "threat" with regard to the information environment:

1. Firstly, the ADF faces nation-states who seek to use information capabilities in warfare, and who integrate these into conventional combined forces. This has already happened to other nation-states, such as Russia when faced with Chechnya in the 1990s. There is no reason the ADF should not expect other nation-states to have calibrated themselves similarly, indeed comprehensively, in the information environment. The timescale of over 20 years since Russia's Chechnya experience suggests the ADF has been slow to respond to this reality.

2. Secondly, the ADF equally faces other actors—non-nation-states, or "non-state actors"—who use the information environment to procure significant advantage for themselves or their sponsors. This can include terrorist organisations, insurgent groups, and other actors seeking to exploit the information environment to their own ends. Such actors may be used by nation-states to effect state-directed ends.

3. Thirdly, and in some combination of the first two threats, the ADF may face so-called "grey-zone" threats. These are activities existing in the threshold between the traditional conditions of peace and war which are designed to destabilise or undermine a nation-state. Cyberattacks and disruptive social media influence form part of such grey-zone activities.[35] Discussion of these "grey-zone" activities has been most prominent in the United States, with Congress authorising a 2018 US Department of Defense directive to engage in "low-visibility, irregular warfare" operations by supporting foreign forces in such wars.[36] Australia's status as a key US ally means the ADF cannot afford to ignore this discussion nor the reality of the threats it seeks to address.[37]

4. Finally, and perhaps most tellingly, the ADF faces a threat of "self-harm" in the information environment. A health-check, such as what took place at Exercise Talisman Sabre in 2017, showed the ADF up in stark terms for its lack of cyber self-awareness and failures in basic cyber self-defense. Perhaps hopefully, the "Red-Team" at Talisman Sabre showed that Australia's offensive capabilities in the information environment are approaching where they need to be.

These four ADF vulnerabilities are a starting point for the ADF's reflections on how to meet the challenges of the new information environment.

---

[35] David Barno and Nora Banshael, "Fighting and winning in the "gray zone", *War On The Rocks,* May 19, 2015, https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/.

[36] 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.

[37] See, for example, "Responding to Russia: Deterring Russian Cyber and Grey Zone Activities," Transcript, *Center for Strategic and International Studies*, March 19, 2018, https://www.csis.org/analysis/responding-russia-deterring-russian-cyber-and-grey-zone-activities.

Integrating Strategic and Operational Levels in the Information Environment

At the present time, Australia is establishing three new statutory offices which will possess cyber amongst their responsibilities. These will sit alongside other Australian agencies who already possess such capabilities.

This means the ADF will need to continue coordinating its information capability efforts with Australia's whole-of-government agencies, noting the significant changes underway within Australia's nation security establishment. These changes include:

1. The new Office of National Intelligence (ONI), reporting to the prime minister and assuming an enlarged role of coordination between Australia's intelligence agencies.[38]
2. The establishment of the Australian Signals Directorate as an independent statutory agency within the Department of Defence, reporting directly to the minister for defence.[39]
3. The establishment of the Home Affairs Portfolio, reporting to the minister for home affairs and bringing together operational agencies and bodies related to Australia's federal law enforcement, national and transport security, criminal justice, emergency management, multicultural affairs, and immigration and border-related functions and agencies.[40]

Each of these is a welcome development which will individually and collectively assist Australia's information capability management, most notably in the cyber domain.[41]

A potential risk remains that Australia will be unable to identify what cyber and/or information capabilities belong, or should belong, to which government portfolio and in what relative proportion. Indeed, the ADF could fall foul of the simple error of being unable to articulate what its remit should be when seen against this newly announced order of information battle for the Australian government.

This risk should not be overstated, noting the ADF and Australia more broadly have considerable experience in multiagency cooperation both on and outside of operations, and also that the new ONI has a specific mandate to lead, coordinate, and integrate the agencies of Australia's national intelligence community as described in the legislation pertaining to ONI.[42]

The ADF will nonetheless remain conscious of the need to coordinate policies, processes, and procedures in the information environment to ensure that the strategic, operational, and tactical levels of war are properly accounted for in Australia's information capability settings. This is not least because the ADF recognizes its members will be on the "front line" of military information capability failure in deployed environments and at home.

---

[38] Australian Parliament, *Office of National Intelligence Bill 2018*, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6147.
[39] Australian Parliament, *Australian Signals Directorate Bill 2018*, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6047.
[40] Australian Department of Prime Minister and Cabinet, "Home Affairs Portfolio Established", December 20, 2017, https://www.pmc.gov.au/news-centre/pmc/home-affairs-portfolio-established.
[41] The majority of these changes find their source in the Australian *2017 Independent Intelligence Review*, https://www.pmc.gov.au/national-security/2017-independent-intelligence-review.
[42] Australian Parliament, *Office of National Intelligence Bill 2018*, esp. "Part 2. Division 2. Functions and Powers," p. 10-16, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6147.

Section 3 | How Will the ADF Address the Information Warfare Threat?

On July 1, 2017 the ADF established the "Information Warfare Division" within the Joint Capabilities Group of the Australian Department of Defence. The division forms part of the newly established Australian Defence Force Headquarters (ADFHQ) and is responsible for developing joint ADF capabilities to fight and win in the information environment.

The ADF's Information Warfare Division currently focuses across five areas in its capability development:

1. Information War and Joint Warfighting
2. C4 Systems and Information
3. The Cognitive Dimension of Information Capabilities
4. People and Personnel
5. International Engagement

These five focus areas, driven by consideration of the threat landscape, will help the ADF incorporate information-related capabilities into its order of battle. We describe each with a brief summary below.

Focus Areas for ADF Information Warfare Capability Development

INFORMATION WAR AND JOINT WARFIGHTING
The ADF has an obligation to integrate its joint warfighting capabilities with its capabilities in the information environment.

The ADF's Information Warfare Division inherits and integrates numerous existing ADF information-related capabilities. These include:

- Information Activities and Operations
- Joint Electronic Warfare
- Military Cyberspace Operations
- Space Operations
- Joint Intelligence, Command, Control, Communications, and Computing (C4)
- Battlespace Situational Awareness

A key task of the Information Warfare Division is to unify, coordinate, and integrate these previously dispersed capabilities into a single capability element of the ADF.

On the one hand, this means identifying what information-related capabilities are a legitimate and necessary element of Australia's warfighting capabilities. On the other, it means that ADF members must become trained and proficient in the use of systems related to information warfare. This is both in

response to "attacks" on the ADF, its members, and its systems; and in order to develop information capabilities that will have a distinctively military component to them.

This might include the development of systems that protect the ADF from cyberattacks of all varieties when the ADF is deployed. It will certainly include the development of resilient information technology architecture to defend Australia's military systems at home.

In sum, the ADF will use the information environment as a means through which to integrate with its own systems more closely, across multiple traditional domains and their capability sets.

The ADF has recently acquired the airborne electronic-attack "Growler" system as part of its air capability. This system must be able to integrate with ADF systems from other services as well as with partner forces in coalition.

To do this effectively, the ADF could approach the question of integration at a systems-level, rather than a platform-level. In doing so, the ADF would recognize that information-related capabilities potentially connect to every ADF platform. This would in turn frame the ADF in its entirety as an "information system." While helpful, such a description would of course fall short of capturing the full range and potential of the ADF's combat systems. It would only be a means to an end of visualizing the range and potential of the ADF's capabilities in the information environment.

Broadly, thinking differently about the ADF's capability may help identify the ADF's potential in the information environment. It could also inform the ADF's development of materiel, training, and operating concepts for this new area of capability.

C4 SYSTEMS AND INFORMATION

The integration of the ADF's command, control, communications, and computing (C4) functions is an essential cog in the ADF's warfighting capability.

The information environment has enhanced the ADF's realization of the need for an integrated fighting force, enabled and not hindered by the "seams" of its capabilities. By seams, we mean those areas where systems do not naturally integrate or work well with one another. C4 is one area where these seams can become more vulnerable if not planned for integration from the outset.

The ADF's establishment of a chief of Joint Capabilities is one step towards increased C4 integration. Appointed on July 1, 2017 as a service-chief equivalent, Australia's chief of Joint Capabilities is responsible, among other things, for the "stitching" of Australia's existing C4 capabilities and planning for their future integration.

The information environment brings the need for integration into sharp relief. If high-end systems cannot communicate with earlier-generation systems, for example, significant parts of Australia's combat and defensive potential is lost.

It is for this reason that the ADF's chief of Joint Capabilities is tasked with cohering these systems. This means both seeking effective "workarounds" to current systems that struggle to communicate, while seeking better ways to plan for joint ADF C4 in the Information Age.

The ADF recognizes that, like most leading Western militaries, it has a distance to travel to achieve better integration of its joint military effects—in capability, in doctrine, and in force-structure planning. The ADF also recognizes that the information environment will remain one measure of the ADF's ability to do this effectively.

THE COGNITIVE DIMENSION OF INFORMATION CAPABILITIES

The cognitive component of information warfare is critical to its mastery. In a world of technical information systems, the human mind remains a key target of information capabilities. This is either to interrupt or degrade commanders' human decisionmaking processes, central to a battle's direction, or to interfere with the technical systems commanders depend on to make such decisions during a conflict.

> For the ADF, war remains a "human endeavour," exactly as Clausewitz described.[43] For that reason, the ADF recognizes that information warfare is ultimately about imposing one's will on a human enemy, not on a machine. The ADF continues to hold that even in the so-called Information Age, war remains a contest of human wills, not primarily of machine capacity.

The ADF nonetheless recognizes that in the Information Age, the contest of human wills is being played out in an intensified way across the digital and electromagnetic spectrums. For this reason, the ADF will identify, design, and manage capabilities across the information environment to enhance its own ability to contest and win in these spectrums.

This includes making a distinction between "technical" and "non-technical" capabilities relevant to the information environment:

- By **technical information capabilities**, the ADF refers to the **electronic, digital, or machine-based systems**. Technical systems cover everything from algorithms to mechanical engines. They are distinguished by not having morally accountable autonomy.

- By **non-technical capabilities**, the ADF refers to human, and more specifically, **cognitive elements of information warfare capabilities**. Non-technical capabilities refer to the human-in-the-mix, either as the target of information capabilities or as their operator.

Artificial intelligence (AI) presents a challenge to this distinction since it promises to fuse human and machine. The ADF accepts that the challenge of AI is still unfolding.

One additional challenge for the ADF to deal with concerning the cognitive element of human capability is the different moral baselines of potential ADF adversaries and/or the different moral frameworks of potential coalition partners in the information environment.

Where, for example, a strategic competitor develops technical information capabilities which remove the "human in the loop" for targeting, will the ADF consider doing the same thing if that means remaining militarily or strategically competitive? Or will the ADF or her allies refuse to entertain developing such capabilities based on their own ethical and moral codes?

[43] "War is an act of violence to compel our opponent to fulfil our will," Carl von Clausewitz, *On War*, 1.2.

Questions such as these for the meantime remain unanswered. The ADF remains comfortable with their ongoing discussion, observing that such discussion remains central to the ADF's ability to account for the moral component of the ADF's warfighting abilities.

PEOPLE AND PERSONNEL

It is difficult to overstate the importance of the ADF having the right people for work in the information environment.

Alongside the fact that military professionals take many years to develop, the technical capabilities resident in the information environment will make technically competent individuals a vital asset for the ADF as it develops its information warfare capabilities.

It is clear that the ADF is not the only sector of the global economy in search of these skills.

For that reason, the ADF may have to develop a specific workforce-planning system for individuals in the information environment. Such a system would need to be credible and sustainable in terms of key features of that workforce, for example being global and not just local.

> Cyber experts in banking could second with the ADF for periods of time to work on complex mathematical problems. Conversely, the ADF may choose to send its developing cyber experts into advanced academic, technological, scientific, or economic sectors to learn new ways to interact with the changing information environment. These "digital cultural embeds" would be of significant value to the ADF in its workforce and technical capability development.
>
> Examples like these remain hypothetical for the meantime. But they indicate the sort of flexibility the ADF—and perhaps its partner militaries—might seek to develop to gain a "cyber edge" in modern warfare.

For the meantime, the ADF will continue to develop a "mixed" cyber workforce—of civilians and military professionals—for its activities in the information environment. The ADF recognizes that a fusion of skills, training, education, development, and professional experience will create the best information warriors in years to come. This may mean, from time to time, "thinking outside the box" about how to develop and sustain the best information environment workforce.

INTERNATIONAL ENGAGEMENT

Deliberate international engagement with allies and security partners on the development of the ADF's information warfare capabilities is good health and good practice. Allies can draw strength from the information environment's emergent character by working closely with each other to solve its common but unforeseen problems. The ADF continues to operate most frequently with allies and security partners, setting a precedent for its information environment conduct.

Presently, Australia's closest allies and security partners exist in the "five-eyes" intelligence-sharing relationship between Australia, Canada, New Zealand, the United Kingdom, and the United States. These allies continue to develop their own information warfare doctrine while closely coordinating their strategic intent with one another. In certain cases, they may choose to pursue specific information technology and capability development with one another.

Every case of common technology or strategic coordination between allies can present a broader surface of information defense for allied security partners. It also highlights common strategic intent related to the emergent information environment. This can include, for example, the establishment or preservation of a legitimate rules-based order for capabilities in the information environment, especially as these are deployed or utilized by militaries.

The importance of allied and security-partner coordination against disruptive cyber activity was recently seen in the "NotPetya" cyberattack. Australia,[44] the United Kingdom,[45] and the United States[46] attributed the attack to Russia, describing it as state-sponsored by Russia. This was despite Russia's strong denials of any responsibility for NotPetya.[47] This coordination between security partners helped firm up the public perception that cyber behavior emanating from Russia breached accepted international norms and standards. The conversation continues, but the force of allied effort has become clear at the same time as the intensity of cyber disruption from nation-states and, almost certainly, non-state actors has heightened.

The ADF will continue to develop its information warfare capabilities in close coordination with its partner Australian agencies and those of its long-standing military allies. This will ensure coordination between the military and strategic levels of the ADF's capability development in the information environment.

The ADF will also partner with non-government organizations to develop its information-related capabilities. This includes universities, industry, and even local governments at home and across Australia's allies and security partners. The ADF recognizes that international engagement equally means multisector engagement internationally in a globally-connected age.

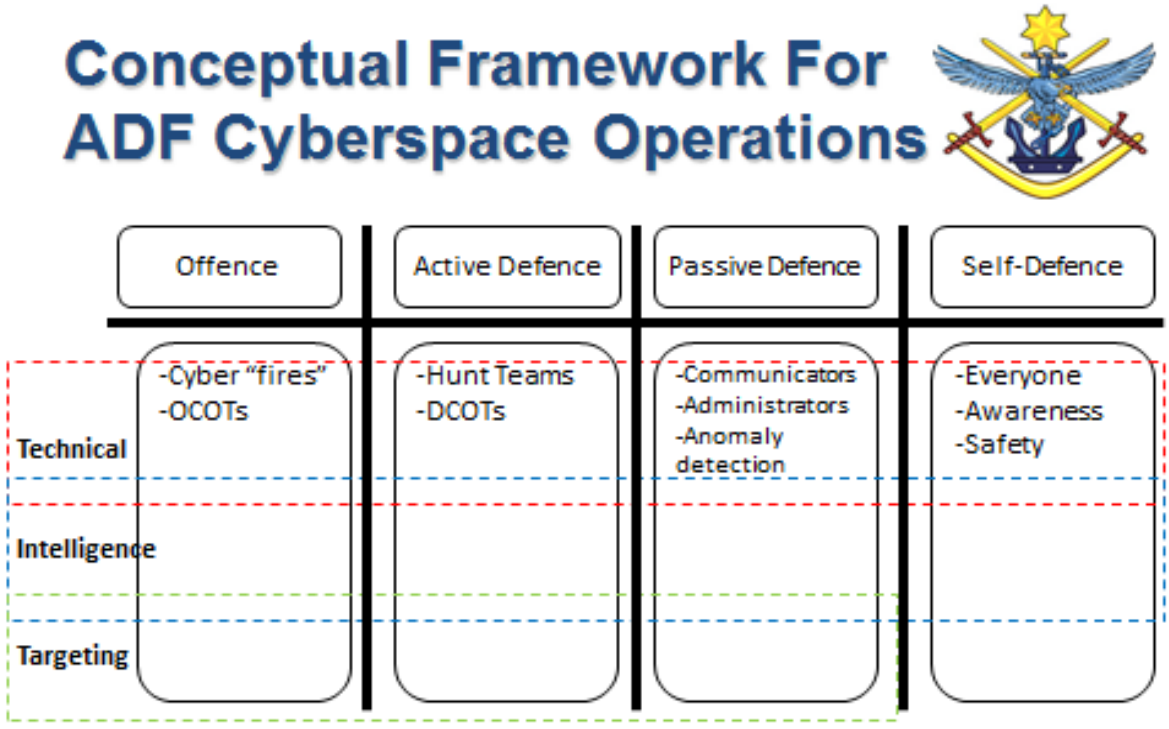
[44] Hon. Angus Taylor MP, "Australian Government attribution of the 'NotPetya' cyber incident to Russia," Minister for Law Enforcement and Cyber Security, February 16, 2018, http://minister.homeaffairs.gov.au/angustaylor/Pages/notpetya-russia.aspx. Minister Taylor's statement was made on behalf of the Australian government, noting, "Based on advice from Australian intelligence agencies, and through consultation with the United States and United Kingdom, the Australian Government has judged that Russian state sponsored actors were responsible for the incident."
[45] "Foreign Office Minister condemns Russia for NotPetya attacks," February 15, 2018, https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks. This UK report included a statement by Foreign Office Minister Lord Ahmad.
[46] "White House blames Russia for 'reckless' NotPetya cyberattack," *Reuters*, February 15, 2018, https://ca.reuters.com/article/technologyNews/idCAKCN1FZ2UJ-OCATC. This report cites White House Press Secretary Sarah Huckabee-Sanders unequivocally condemning Russia for the attacks.
[47] "Kremlin 'categorically' denies Russia behind NotPetya cyber-attack," *France24*, February 15, 2018, https://www.france24.com/en/20180215-kremlin-categorically-denies-russia-behind-notpetya-cyber-attack. Kremlin spokesperson Dmitry Peskov described the accusations as "unsubstantiated, groundless [and] nothing but a continuation of a Russophobic campaign that is not based on any evidence."

Section 4 | Four Pillars for ADF Concept Development in the Information Environment

The ADF's information capabilities must develop using sound concepts. The ADF has developed an early framework for this concept development. It provides an initial insight into the frames the ADF will use to develop its theory of conduct in the information environment.

The framework relates specifically to the ADF's cyber capabilities, as these remain for the meantime one of the easiest to "name" in the ADF's information tool kit. However, the baselines of the ADF's cyber defense framework will inform the other areas of its information capability development.

Figure 4: The ADF's Conceptual Framework for Cyber Operations



Source: Remarks by Deputy Chief Information Warfare, Australian Defence Force (ADF), Major General Marcus Thompson, to the Military Communications and Information Systems Conference (MILCIS), November 17, 2017, Canberra, Australia.

These four pillars cover the functions of offensive cyber, active cyber defense, passive cyber defense, and cyber self-defense. These reflect a normal order of battle for operational activities in military settings, detailed as follows:

> **Offensive cyber** means the ADF will attack the systems and capabilities of actors viewed as hostile to the ADF or its operations, to ensure missions are achieved and ADF personnel and systems are safe. These activities will remain highly classified and stand in best analogy to "fires" in traditional domains. These fires will occur in the cyber domain. The ADF's activities here will be legally authorized and cohere precisely with Australia's expressed national intent.
>
> **Active cyber defense** is conducted by specialists to elevate the cyber response via more technical capabilities that are operated by small numbers of highly-trained personnel. These professionals will be "hunt-teams" who are threat-focused but operating on friendly systems. Their role as specialists is in the defense of ADF systems, but not in attacking other systems.
>
> **Passive cyber defense** relates to all ADF communicators' and network administrators' management of ADF networks and mission systems. It means system operators will be trained and equipped to detect, triage, and resolve network or system anomalies in the information environment. It is basic cyber housekeeping for the ADF as a digitally-enabled, modern organization.
>
> **Cyber self-defense** involves all ADF members. It is the foundation for ADF cyberspace capabilities and will transform ADF culture to ensure every ADF member is fully-versed in cybersecurity norms and procedures. It means making cyber part of an ADF member's daily responsibilities, the new normal for everyone. Cyber safety should become as familiar as smartphone use is, and as easy as ensuring the door is locked before you leave the house.

Cyber self-defense means the ADF will aim never to repeat its information follies as exposed on Exercise Talisman Sabre 2017. It will see ADF members develop confidence in their knowledge and use of the information environment to the ADF's purposes.

The conceptual framework outlined above places boundaries around ADF activities and capabilities in cyberspace, which are distinguished from the way other government agencies use their cyber capabilities.

The framework also means the ADF's approach to cyber can be normalized with partner-militaries and within a whole-of-government approach in Australia. The ADF's decision to telegraph its basic conceptual framework in the cyber domain seeks to encourage security-partner participation across the broad range of stakeholders with whom the ADF will work as it develops its information capabilities.

The ADF will continue to test and adjust as it normalizes information partnership between current and future allies and security partners.

Conclusion

Financial Commitment for Capability Outcome

The ADF's enhanced journey into the modern information environment has been slow to start but is increasing in momentum.

The 2017 establishment of the Information Warfare Division in ADF Headquarters means the ADF now has a central driver for the development of its information capabilities.

This means that the ADF is well positioned to develop its military-specific information capabilities, which will complement and work in coordination with the other arms of Australia's developing capabilities for the information environment.

To grasp the significance of the ADF's journey, it is worth recognizing that in 2008 the ADF described information capabilities like cyber as an "emerging" priority.[48]

Information capabilities are now listed in the first of only six capability streams the government will prioritize to strengthen the future ADF.[49]

The *2016 Defence White Paper* states that across 10 years, the Australian government will provision capabilities resident within the ADF's Information Warfare Division—intelligence, surveillance, and reconnaissance; electronic warfare; space and cyber—with more than half of the budget for the ADF's future strike and air combat capabilities. Information capabilities will have half the budget for Australia's future land force, nearly a third of the money allocated for Australia's enormous expansion of its naval capabilities, and a third more spending than Australia's air and sea lift capabilities.[50]

This is a dramatic change in fortunes for Defence's information capabilities. Information capabilities have gone from being an "emergent" and relatively unfunded capability area to representing 0.18 percent of Australia's GDP spending seen over 10 years.

[48] Australian Government, *2009 Defence White Paper*, Department of Defence, 9.85-9.89, esp. 9.86; 9.97, et passim, http://www.defence.gov.au/whitepaper/2009/docs/defence_white_paper_2009.pdf. The paper describes "cyber" in some detail but notes it only as an emergent priority.
[49] Australian Government, *2016 Defence White Paper*, Department of Defence, 4.9, http://www.defence.gov.au/WhitePaper/. The *2016 Australian Defence White Paper* lists it first in its description of the future ADF.
[50] Ibid., p. 85.

Australia's Future Defense Capability Spending, Set Out by Capability Stream across 10 Years[51]

1. **Air and Sea Lift: 6 percent** of 10-year ADF investment
2. **ISR, EW, Space, and Cyber: 9 percent** of 10-year ADF investment
3. **Strike and Air Combat: 17 percent** of 10-year ADF investment
4. **Land Combat and Amphibious Warfare: 18 percent** of 10-year ADF investment
5. **Maritime and Anti-Submarine Warfare: 25 percent** of 10-year ADF investment
6. **Key Enablers: 25 percent** of 10-year ADF investment

This means **information capabilities for the ADF will account for up to 0.18 percent of Australia's GDP if Australia spends 2 percent of GDP on the Department of Defence by 2024**, its stated goal.

Source: Australian Government, 2016 Australian Defence White Paper, Department of Defence, Figure 3, p. 85, http://www.defence.gov.au/WhitePaper/.

Such financial commitment from the government towards the ADF's information warfare capabilities will certainly see the ADF better positioned to combat the increasingly rapid pace of change in the information environment. More critically, it will help the ADF identify how to deploy information capabilities in ways that maximize their potency for the ADF.

It also means the ADF has an increased serious obligation to return value to the Australian taxpayer for their level of spending and investment in this defense capability.

Ethics, Law, and Information War

In closing, it is worth reflecting on the fact that the ADF also has an obligation to continue developing its information warfare capabilities in terms of the codes of ethics that have always governed Australia's approach to warfare.

Australian theorist David Kilcullen recently told a London conference on future land warfare that autonomous systems have the same potential to transform the land domain as the Gatling gun did over 100 years ago.[52] In a similar vein, Australian Major-General Mick Ryan reminds us concerning artificial intelligence that "in the competitive environment of war, the race truly goes to the swift." The decisionmaking speed of AI has the potential to make the human person the slowest, and thus most redundant, on the battlefield.[53]

[51] Ibid. We have re-represented the *White Paper*'s original diagram here.
[52] Reported comments of Dr David Kilcullen, Royal United Services Institute (RUSI) Land Warfare Conference, London, June 19-20, 2018: "The ability for small squads to apply vertical [autonomous and robotic] systems rivals, in importance, the introduction of the light machine gun into the squad 100 years ago. In terms of reach and envelope, small and medium size drones significantly transform what [small squads] can do."
[53] Mick Ryan, "Integrating Humans and Machines," The Strategy Bridge, January 02, 2018, https://thestrategybridge.org/the-bridge/2018/1/2/integrating-humans-and-machines.

These are important observations. But, they also suggest one risk for the ADF—and any other military in this domain—is that it becomes too focused on the systems that assist it in conducting its fight, rather than the population on whose behalf it does so.

We have argued in this paper that the cyber domain is an emergent one. We suggest similarly that the human individuals on whose behalf the information environment is constructed will remain the centre of gravity of any conflict that takes place using the information environment.

For this reason, the ADF will need to continue to evolve its theory of warfare to account for rapidly developing information technology and information capabilities emerging from them. The reason for this is not simply that warfare will remain governed by ethically constraining laws, norms, and principles for Western countries. It is equally because the peace for which war is fought, more often than not, is heavily conditioned by the nature and conduct of the war that preceded it.

This is to articulate the requirement for an account of "just war" in the information environment. This should not be an unusual call. To fulfill it, however, will require creativity, commitment, and a depth of professional military insight. It may also require a succinct reappraisal of the laws of armed conflict and rules of engagement stemming from them in the light of information technology's new uses on the battlefield.

To begin such an undertaking will be another component of the ADF's journey into the information environment. It should be considered in no less important terms than the capability and concept development whose beginnings this paper has described.

About the Authors

Group Captain (Colonel) Edward Morgan is a Royal Australian Air Force Officer and Military Fellow at the Center for Strategic and International Studies (CSIS), Washington, D.C. He currently serves as strategy adviser in the Information Warfare Division at Australian Defence Force Headquarters in Canberra, Australia. He has previously worked as strategy adviser to the Royal Australian Air Force and in several strategy, enterprise planning, and policy roles across the Australian Department of Defence. He has also worked as a civilian at the state level in Australia, managing defence industry strategy and policy for the government of Victoria, Australia. Group Captain Morgan is a graduate of the University of Cambridge, UK (Ph.D., M.Phil.) and the University of Melbourne, Australia (B.A. Honors). He is fluent in French and German, has a working knowledge of Italian, and is fluent in two ancient languages (Latin and Ancient Greek).

Major General Marcus Thompson is currently Deputy Chief Information Warfare, Australian Defence Force Headquarters, where he is Head of the Information Warfare Division. Major General Thompson graduated from the Royal Military College, Duntroon, Australia in 1988 and was allocated to the Royal Australian Corps of Signals, Australian Army. He served in a variety of command, regimental and Special Operations appointments including Command of the 3rd Combat Signals Regiment; on secondment to the Department of the Prime Minister and Cabinet as the Senior Advisor Defence Policy and Operations; at Headquarters Special Operations as the Director General Special Operations Capability; and Commander 6th Combat Support Brigade. Major General Thompson was appointed a Member of the Order of Australia in the 2014 Queen's Birthday Honors List. He holds a Bachelor of Electrical Engineering with honors from the University of New South Wales, a Bachelor of Business from the Royal Melbourne Institute of Technology, a Masters Degree in Defence Studies from the University of Canberra, a Masters Degree in Strategic Studies from Deakin University, and a Ph.D. in Cyber Security from the University of New South Wales.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**