The Changing Operational Security Landscape for Sensitive National Capabilities

Martin White

The Australian Defence Force and Australian security community maintain many sensitive national capabilities that are subject to extensive security protections to prevent information disclosure. Often, the operational models of these capabilities are based on the assumption that they will not be discovered. This assumption is becoming tenuous. The frequency of public information disclosures of sensitive national capabilities is high, and technology has evolved to give Australia's strategic competitors greater ability to gain intelligence on these sensitive national capabilities. This article will consider the shared operational security features of two of Australia's most sensitive military capabilities—submarines and Special Forces. It contends that Australian policymakers must be more specific in designating the information they wish to protect, and take additional measures to do so, noting that operational security is becoming a more transitory concept rather than something that can be achieved into perpetuity.

National security information disclosures or 'hacking' incidents are an almost weekly occurrence in Australia and elsewhere, even against the most sensitive and highly protected military capabilities. A serious 'compromise' of highly sensitive submarine data in 2016[1] was just one of many previous and subsequent disclosures of Australia's most sensitive national secrets. Hacking is just one means through which information is becoming more accessible, and protecting specific information from unintended disclosure is now an enormous challenge.

Various Australian defence commentators have assessed that 'unconventional' forces, particularly submarines and Special Forces, will offer a relative advantage against sophisticated potential adversaries in future conflict.[2] This is because these unconventional forces may be harder

[1] Andrew Greene, 'French Submarine Builder Information Leak Could Be Result of Hacking, Indian Defence Minister Says', *ABC News*, 24 August 2016, <www.abc.net.au/news/2016-08-24/french-submarine-data-leak-'could-be-result-of-hacking'/7782256> [Accessed 1 August 2018].

[2] Ian Langford, *Australian Special Operations: Principles and Considerations* (Canberra: Australian Army, 2014), 10, argued that Special Forces must use unorthodox methods that are unsuitable for other parts of the military. Also see Andrew Davies, Peter Jennings and Benjamin Schreer, *A Versatile Force: The Future of Australia's Special Operations Capability* (Canberra: Australian Strategic Policy Institute, April 2014), 5.

for an adversary to detect and subsequently defeat.[3] When it comes to operational security, submarine forces and Special Forces appear to have similar challenges. Both have traditionally sought high levels of operational security and information protection, through sophisticated communications security, identity protection for personnel, cover stories for missions, and compartmentalisation of capabilities and operations.[4] However, protection is becoming more difficult. Operational security measures must now mitigate threats and vulnerabilities including 'insider threats', deliberate leaks to media, signals intelligence interception and more sensitive collection sensors, poor security practices, use of social media by families and friends, and hacking. Aggregation of routine data or access to metadata can exacerbate vulnerability.[5] Information protection for nationally significant military capabilities is now more difficult and may now only be temporary. Levels of vulnerability may vary across different theatres of operation and across different missions. Strategic competitors have many ways to obtain such information. The most operationally secure organisations will be those that consciously identify and protect their most important information. These organisations must also be prepared for deliberate and inadvertent information disclosures, since failure to prevent all information disclosures can no longer be considered an appropriate or realistic benchmark.

This article calls for the Australian Defence Force and the broader Australian security community to adopt more deliberate and collaborative efforts to ensure operational security in the face of these increasing challenges. This article will contend that for the most sensitive national security capabilities, Australian policymakers must prioritise clearly what information is of greatest importance and which can be effectively protected. In the future, not all information can be protected, and the security community must be prepared for information and operational security disclosures. This article will further argue that nationally sensitive military units must understand the range of threats that can be used to disclose key information—as technological advancement has opened more vectors for the compromise of operational security.[6]

[3] Andrew Davies, 'The Strategic Role of Submarines in the 21st Century', *The Strategist*, Australian Strategic Policy Institute, 26 October 2017, <www.aspistrategist.org.au/the-strategic-role-of-submarines-in-the-21st-century/> [Accessed 10 January 2019].

[4] Australian Defence Force, Operations Series: Australian Defence Force Publication (ADFP) 45—*Special Operations* (Canberra: Australian Defence Force Warfare Centre, 1997), para 440, 610.

[5] A former Central Intelligence Agency Chief claimed, "We kill people based on metadata"; see David Cole, 'We Kill People Based on Metadata', in *The New York Review of Books*, 10 May 2014, <www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata> [Accessed 1 August 2018].

[6] This information is often labelled 'Essential Elements of Friendly Information'. Commonwealth of Australia, Operations Series: Australian Defence Doctrine Publication (ADDP) 3.13—*Information Activities*, Edition 3 (Canberra: Defence Publishing Service, 2013), para 1.46.

Not All Information Can Be Protected

Australian Defence Doctrine Publication (ADDP) 3.13 describes operational security as:

> A command function (that) denies the adversary access to Essential Elements of Friendly Information. This prevents effective analysis of friendly activities, dispositions, intentions, capabilities and vulnerabilities.[7]

Most military doctrinal definitions of operational security are consistent with this one. But such definitions may now lack the nuance necessary in an Internet-enabled and information-overloaded environment. For example, ADDP 3.13 does not highlight that sophisticated cryptographic security may not reduce the likelihood that a military unit may be geo-located through their communications, or may not fully mask the identity of the unit. Further, operational security doctrine rarely refers to the transient nature of operational security. As uncomfortable as it may be to admit, it is likely that at many points in the future there will be more information compromised or publicly released. Indeed, the previously classified ADDP 3.13, which was released through a freedom of information request, is itself an example.[8] If a sophisticated strategic competitor or an opportunistic insider prioritises the collection or release of information on a specific Australian national security capability, a significant amount of data might be compromised.

Australia's submarines and Special Forces capabilities arguably represent two of the nation's most sensitive military-related capabilities. Understanding their shared challenges offers a view of contemporary operational security issues.

Submarines are central to Australia's defence policy, and the future submarine project is one of Australia's most expensive procurements. One commentator argued, "it is hard to imagine a more precious national security secret than the performance parameters of Australia's new $50bn submarine fleet".[9] Former Chief of Navy, Vice Admiral David Shackleton, argued:

> Submarines and their crews depend on secrecy for their survival. They represent an extreme expression of what it means to be clandestine … Our submarine secrets had better be kept safe.[10]

There are few military capabilities that are more nationally sensitive than submarines. However, Vice Admiral Shackleton seems to place impossibly high criteria on information protection and operational security for the future submarine, at a time when information relating to the submarine capability

[7] Ibid.

[8] Department of Defence, *FOI 330/13/14*, Canberra, 22 April 2014, pp. 1-2.

[9] Cameron Stewart, 'Loose Lips Sink Ships', *The Australian*, 7 September 2016, p. 11.

[10] David Shackleton, 'Australia's Future Submarine: Why Security Matters', *Lowy Interpreter*, Lowy Institute, 30 August 2016, <www.lowyinterpreter.org/the-interpreter/australias-future-submarines-why-combat-system-matters> [Accessed 1 August 2018].

has already been shown to be at risk and when information disclosures have been historically frequent. Others have predicted emerging risk for submarine operational security.[11] Indeed, there are many examples in history of submarine information being compromised, often publicly—for example, the World War Two intelligence collected on Japanese submarine locations,[12] US intelligence analyst Ronald Pelton selling information relating to US submarines and their operations to the Soviet Union,[13] and Able Seaman William McNeilly's public disclosures associated with the safety and security of the Royal Navy's Trident capability.[14] The 2017 Chinese seizure of the US underwater drone off the Philippines demonstrated a new vector to gain submarine intelligence.[15] Further, actions of ex-military personnel seeking recognition of operational service have resulted in other information disclosures; the admission of an Australian submarine intelligence gathering mission against Soviet targets being one example.[16] It is not unusual for submarine operational information to be conceded or lost.

The disclosure of information on Special Forces is similarly not historically unusual. It is hard to imagine that there was any important information from the British Special Air Service resolution of the 1980 Iranian embassy siege in London that was not released into the public domain soon after the incident.[17] In 2012 newspapers published an article purporting to be about Australian Special Forces' operations in Africa.[18] In the same year, US Navy Seals were reportedly punished for providing technical details of Special Forces methods to a video game developer.[19] Photography on social media

[11] Davies, 'The Strategic Role of Submarines in the 21st Century'.

[12] Wilfred Jay Holmes, *Double Edged Secrets: U.S. Naval Intelligence Operations in the Pacific* (Annapolis: Naval Institute Press, 1979), pp. 212-13.

[13] Olga Khazan, 'The Creepy, Long-Standing Practice of Undersea Cable Tapping', *The Atlantic*, 16 July 2013, <www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/> [Accessed 1 January 2018].

[14] William McNeilly, 'Trident Whistleblower: Nuclear "Disaster Waiting to Happen"', *Wikileaks*, 17 May 2015, <wikileaks.org/trident-safety/> [Accessed 1 January 2018].

[15] Katie Hunt and Steven Jiang, 'China: Seized Underwater Drone "Tip of Iceberg" When It Comes to US Surveillance', *CNN*, 19 December 2016, <edition.cnn.com/2016/12/18/politics/china-us-underwater-vehicle-south-china-sea/> [Accessed 1 January 2018].

[16] Brendan Nicholson, 'Secret Spy Missions Forced to the Surface', *The Age*, 8 September 2006, <www.theage.com.au/news/national/secret-spy-missions-forced-to-the-surface/2006/09/07/1157222265317.html> [Accessed 1 January 2018].

[17] Phil Davison, 'John McAleese: Leader of the SAS Team That Ended the 1980 Siege of the Iranian Embassy in London', in *The Independent*, 30 August 2011, <www.independent.co.uk/news/obituaries/john-mcaleese-leader-of-the-sas-team-that-ended-the-1980-seige-of-the-iranian-embassy-in-london-2345827.html> [Accessed 1 August 2018].

[18] Raphael Epstein and Dylan Welch, 'Secret SAS Squadron Sent to Spy in Africa', *Sydney Morning Herald*, 13 March 2012, <www.smh.com.au/federal-politics/political-news/secret-sas-squadron-sent-to-spy-in-africa-20120312-1uwjs.html> [Accessed 1 August 2018].

[19] Associated Press in Washington, 'US Navy Seals Punished for Giving Secrets to Medal of Honour Game', *The Guardian*, 10 November 2012, <www.theguardian.com/world/2012/nov/09/navy-seals-breach-video-game> [Accessed 1 August 2018].

from an assumed United States mission in Libya was reported.[20] Significant information was disclosed by participants in the mission to kill Osama bin Laden in Pakistan.[21]

Special Forces and submarines are not the only highly sensitive national capabilities that are at risk from information disclosures, both deliberate and unintended. The ‘Five Eyes’ signals intelligence and electronic warfare enterprise is another sensitive area at persistent risk. Signals intelligence has been highly classified for many decades, but compromise has been regular. The Edward Snowden and Chelsea Manning information releases through Wikileaks and other sources were recent instances in a history of signals intelligence disclosures. The Snowden and Manning cases made specific capabilities, collection priorities and reports public.[22] Desmond Ball’s renowned Australian book from the 1980s, *The Ties That Bind*, offered extensive assessments of highly sensitive facilities such as Pine Gap.[23]

Simply put, sensitive information compromise cannot be characterised as unusual.

In the submarines and Special Forces cases, security measures (including legislative protections), limited but did not prevent ongoing disclosures. Beyond these examples, it is common for information to be compromised or released without authorisation, including by external organisations supporting operations, personnel management or capability development. The challenge of protecting military secrets in an Australian culture where transparency is valued comparatively highly is an added pressure.

This article will now turn to information compromise without the knowledge of the information owner—perhaps an even greater risk to operational security.

[20] Tom Wyke, ‘US Special Forces Photographed for the First Time on a Secret Mission in Libya But Were Embarrassingly Told to Leave by Local Commanders Shortly after Landing’, *Daily Mail*, 18 December 2015, <www.dailymail.co.uk/news/article-3365394/US-Special-Forces-photographed-time-secret-mission-Libya-embarrassingly-told-leave-local-commanders-shortly-arriving.html> [Accessed 1 August 2018].

[21] Associated Press, ‘Navy Seal “Who Shot bin Laden” Hits Back at Critics’, *The Telegraph*, 15 November 2014, <www.telegraph.co.uk/news/worldnews/al-qaeda/11232830/Navy-Seal-who-shot-bin-Laden-hits-back-at-critics.html> [Accessed 1 August 2018].

[22] For example, see Bruce Schneier, ‘Code Names for NSA Exploit Tools’, Web-blog, 23 October 2013, <www.schneier.com/blog/archives/2013/10/code_names_for.html> [Accessed 23 July 2014].

[23] Jeffrey Richelson and Desmond Ball, *The Ties That Bind: International Cooperation Between the United Kingdom, the United States of America, Canada, Australia and New Zealand* (New York: Harper-Collins, 1986).

Technology, and the Art and Science of Keeping Secrets

Australian defence policy has long articulated the goal of the Australian Defence Force maintaining a regional technological advantage.[24] Submarines and Special Forces are at the forefront of this long-standing policy, operating some of the most sophisticated military equipment available on global markets. This has clearly been an advantage in recent operations, and the maintenance of technologically sophisticated submarines and Special Forces will undoubtedly remain a high priority for the Australian Government.

Military technological sophistication and a broad range of missions required of Australian submarines and Special Forces has brought some less desirable technological attributes, with an increased electronic signature being a prime example. Electronic signatures represent additional vulnerabilities that strategic competitors can exploit to compromise sensitive Australian security information. This could in future reduce the viability of traditional mission types such as Special Reconnaissance.[25] Technological evolution should be comprehensively and deliberately considered in determining the Australian Defence Force approach to operational security.

In his extensive commentary on submarines, Dr Norman Friedman regularly reminded readers that covertness is relative, particularly when submarines operate in waters that are closely observed.[26] Clandestine operations by Special Forces are similarly relative. Submarines and Special Forces have a growing number of equipment types with a prominent electronic signature, particularly for communications. Personnel from both capability areas also rely on communications in a private capacity. But there is no ‘peacetime’ for the most sensitive capabilities, with strategic competitors collecting signatures from satellite and radio systems, counter-improvised explosive device technology, military information technology systems, mobile telephony and Internet use, beacons, and social media without interruption. Use of some or all of these electronic systems will be necessary for submarines and Special Forces elements to achieve their designated mission, particularly when operating in conjunction with conventional forces, or when decision-makers need information such as high resolution imagery.

[24] Department of Defence, *2016 Defence White Paper* (Canberra: Commonwealth of Australia, 2016), 100.

[25] US Department of Defense, Joint Publication (JP) 3-05—*Special Operations* (Washington DC: Department of Defense, 16 July 2014), II-5 – II-6, x, describes Special Reconnaissance as “surveillance and reconnaissance actions normally conducted in a clandestine or covert manner, to collect information of strategic or operational significance, employing military capabilities not normally found in conventional forces”.

[26] Norman Friedman, ‘Submarines and Their Future’, Defense Media Network, 20 December 2012, <www.defensemedianetwork.com/stories/submarines-and-their-future/> [Accessed 26 January 2019].

The challenge is that all electronic systems have signatures and vulnerabilities, and these signatures and vulnerabilities are well known or easily known to strategic competitors. Signatures and vulnerabilities are also more exposed as the size of a capability is increased—for example, when growing from a fleet of six to twelve submarines. Consequently, there are many countries able to collect, analyse, geo-locate or disrupt signatures and communications, including when forces are training or operating in Australia. Such threats to Australian communications have been outlined previously, but the threat posed in 'peacetime' during domestic training could be better understood and mitigated by most military and security forces.[27] As technology evolves, operational security for 'operations' and for 'training' cannot be treated as separate issues; nor can 'personal' communications and 'work' communications.

'Radio silence' is a long-standing doctrinal method to reduce a tactical unit's electronic signature. However, radio silence will rarely be a viable option with modern equipment, particularly when submarines or Special Forces operate in advance of larger forces or gather intelligence for others. Further, some contemporary equipment will transmit or relay signals without user awareness. Military commanders must assess the cost-benefit trade off of whether or not to use certain military equipment (if indeed they have the choice). They must also determine if a mission or a capability has sufficient operational security and an appropriate electronic signature. Such an assessment can only be made if there is detailed knowledge of the signatures associated with technologically sophisticated communications devices. Such knowledge is also important to ensure that personnel involved in nationally sensitive military forces do not believe they are operating in a 'low signature' mode when in fact their signature can be readily identified.

There is no 'peacetime' for intelligence collection, because it is outside periods of conflict that the opportunity for significant intelligence targeting is present. This includes strategic competitors collecting on Australian forces in Australian-based training areas. Digital and Internet technology offers strategic competitors the opportunity to conduct inexpensive intelligence collection on sensitive capabilities and personnel at great range from a designated target. The cost of such collection will reduce further as technology such as commercial miniature satellites evolves.[28]

It may be argued that information is now so freely available that submarines and Special Forces can 'hide' many of their signatures in the clutter and the

[27] Martin White, 'Operational Security in the Digital Age: Who is Being Targeted?', *Australian Army Journal*, vol. XI, no. 2 (Summer 2014), pp. 11-12.

[28] For example, some commercial satellite systems will provide services such as high resolution pictures of any point on the Earth's surface between 55 degrees North and 55 degrees South within 90 minutes—see 'Earth Observation: Anywhere and Everywhere', *The Economist*, Technology Quarterly, 27 August – 2 September 2016, pp. 6-7.

dross of information. The global penetration of WIFI networks is a good example of where there is now a higher signature threshold than existed in the past. This elevated baseline signature threshold presents an opportunity for operational security risk mitigation. However, to do this effectively, military planners and commanders (and defence policymakers) must understand their own signature, and understand the environment that they will operate in. Mobile telephony, for example, may appear a desirable means of communications for a particular mission, but not if all communications on a particular mobile network are being collected or analysed.[29] Protection within information clutter may work if no one is looking for particular signatures, but submarines and Special Forces will remain a high information priority for any strategic competitor. A level of collaboration between submarines and Special Forces elements to determine emerging opportunities and risks may be beneficial in the future.

In summary, submarines and Special Forces may improve their ability to credibly protect their most important information and most sensitive operations by deliberately considering two things. First, they must expect more frequent disclosure of nationally sensitive information. The challenge of maintaining a secret grows over time, especially if a capability gets larger in terms of numbers of platforms or personnel. Second, they must comprehend that more technologically sophisticated capabilities means many signatures and many ways to collect information. Operational missions will become harder to credibly protect. Electronic signatures now mean that deployed locations may be difficult or impossible to fully protect. The strategic trend of 'information availability'—information becoming far easier to obtain—is exacerbating these problems because there are so many different ways to obtain that information, particularly through emerging technology. In combination, these factors mean that the successful achievement of operational security is more challenging than it has been in the past.

With these factors in mind, this paper now turns to considering how defence policymakers might mitigate the growing challenge of maintaining operational security for Australia's most sensitive capabilities.

Adapting to Reality

The growing technological sophistication of regional and global actors means that they can monitor sensitive Australian military capabilities increasingly effectively. This means that a belief that sensitive capabilities can protect all of their information, all of the time is no longer tenable. Regular information disclosures and technological evolution means trying to

[29] NATO assessed this was the case in Afghanistan, with extensive collection by Pakistan intelligence—see 'Afghanistan War Logs: Taliban Sympathisers Listening into Top-Secret Phone Calls of US-Led Coalition', *The Guardian*, 26 July 2010.

protect all information to an equal degree may result in the most important information being equally compromised. Impossibly high operational security objectives must be rebuffed. At the same time, policymakers must plan for a future where more is known about sensitive capabilities and missions. Efforts should be based on a clear understanding of operational security and information protection priorities, and should account for the new digital realities of information collection, signature understanding and the 'off duty' mobile and online presence of personnel. Education and deliberate planning for all threats to operational security is necessary. Some options to ensure that submarines and Special Forces remain optimised for contemporary conflict are as follows.

First, acknowledging that submarines and Special Forces will always produce and hold specific information on capabilities and operations that will remain highly sensitive, often over long periods of time, the Australian Defence Force may choose to take additional practical steps to protect these 'Crown Jewels'. Such steps may involve: (1) a deliberate reduction or complete removal of information related to sensitive capabilities from military information technology networks (information technology reliance has already been proven to be particularly risky); (2) limitations on the numbers of personnel exposed to specific information; (3) conscious decisions to not employ specific capabilities on certain operations and training (or even a 'war stocks' methodology of only using specific equipment in the event of a significant military requirement), and; (4) a more robust layering of information to offer levels of protection for the most sensitive information.

Second, the number and scope of 'Essential Elements of Friendly Information' may need to be deliberately constrained, to ensure that designated information can actually be protected. For example, a force element may be unable to mask the signature of its headquarters location from a future adversary. Consequently, the location or identity of that headquarters would be problematic to protect, because it will be quickly compromised, and therefore practically cannot be considered to be an 'Essential Element of Friendly Information'. Realising that this planning disclosure is likely necessitates a different approach to the deployment of that headquarters, such as spreading it over different locations, or not deploying it forward at all. It may also lead to a different assessment of whether a force element can be considered 'clandestine' during a particular mission or a particular phase of an operation.

Third, there should be a consistent Australian Defence Force (or even Australian security community) approach to identity protection for personnel involved in the most sensitive capabilities. Identity protection has long been a central feature of operational security for nationally sensitive capabilities.[30]

[30] Air Marshal Mark Binskin, *Senate Estimates Brief: Operations 05: Australian Defence Force Battle Casualties: Killed and Wounded as at 06 May 2013*, Canberra, p. 3.

Technological evolution, and the data collection behaviour of technology giants such as Google and Facebook and countries such as China, has meant that identity protection is now much more difficult. The limited ability for personnel to control the information that family, friends and foreign military partners place on communications mediums such as social media adds further concern.[31] Furthermore, information placed on the Internet is there forever. Submarines and Special Forces will, in the future, select personnel for service who have extensive histories on social media and the broader Internet. Ensuring that an identity protection strategy remains credible and achievable, through measures such as adequate protection for personal information databases, will need to start with acknowledging these realities.

Fourth, this article argues that doctrinal and political recognition of the often ephemeral nature of operational security may be useful. With technology offering more ways for a strategic competitor to gain specific information, the longer a secret exists, and the more people who are aware of the secret, the higher the likelihood of its compromise over time. This means protection for certain information may need to be seen as only viable for limited time periods and for specific locations. Operational security assessments need to be made after specific missions or training serials. This may lead to a more rapid declassification of compromised information in order to ensure that the classification system remains credible and meaningful. Adoption of new ‘Essential Elements of Friendly Information’ would need to be carefully considered, particularly if there is a high likelihood of their compromise.

Fifth, there must be recognition of the likelihood of future information compromise. The significant number of unauthorised information disclosures over time across the most sensitive military capabilities in Australia and in other nations leads to a reasonable assessment that disclosures will occur consistently into the future. This does not mean tolerance of individuals breaching operational security (either through information disclosure or through poor electronic signature mitigation)—in fact, there should be an organisational willingness to take action to rebuke those in serious breach or deter potential future breaches. But the Australian Defence Force should rehearse its organisational actions in the event of a significant information compromise, perhaps as an annual training serial, so a response to an incident can occur most efficiently and deliberately. The downgrading of classification or deliberate public release of certain information should be considered. The limiting of access to the most sensitive organisational information, and the potential removal of information from some information technology networks will also be necessary.

[31] Amy Johnson, Celeste Lawson and Kate Ames, ‘“Use Your Common Sense, Don’t Be an Idiot”: Social Media Security Attitudes Amongst Partners of Australian Defence Force Personnel’, *Security Challenges*, vol. 14, no. 1 (2018), pp. 53-64.

Finally, the regular rotation and disposal of specific 'personal' and 'work' communications systems, or modifying of their communications signature parameters or waveforms, may be worth considering. While there are clear integration and cost challenges, the often-highly sensitive missions undertaken by submarines and Special Forces must be afforded the most protection, including through the mitigation of known electronic signatures.[32] A deliberate plan to dispose of certain communications devices or systems may mean the procurement of cheaper equipment in greater numbers. Furthermore, since electronic threats may be local, regional or global in nature, and strategic competitors will conduct intelligence collection through periods of non-conflict, submarine and Special Forces personnel should consider themselves and their information on an operational footing at all times, including through the conduct of adequate operational security planning for domestic training and in their personal lives. This may necessitate a shared and specific understanding of operational security threats across the national security community.

Conclusion

There are many shared operational security concerns for sensitive Australian military capabilities. This article focused on some of the shared interests of submarine forces and Special Forces. Clearly defined and consistent information protection requirements for sensitive capabilities, across the national security community, would appear to now be essential to ensure that adequate information protection is afforded where it is most required, and for a realistic view of operational security to be maintained.

The greatest risk to operational security arguably lies in the potential lack of understanding of where information vulnerabilities lie and when such information can be obtained, and in assuming that all information can be protected equally at all times. Disclosure of information across sensitive capabilities has been common and will occur more often in the future. Operational security should be considered a transient state of affairs, rather than something that is absolute or enduring. As uncomfortable as the concept may be for many, the Australian Defence Force should not find itself surprised by information disclosures in nationally sensitive capabilities in the future, but there are steps that can be taken to ensure that elements such as submarines and Special Forces maintain a level of operational and information security in the information age.

This paper does not advocate a laissez faire approach to operational security because the challenge is too great. It does argue that the Australian Defence Force (and broader Australian security community) approach to

[32] It is a fact that communication systems conversions have occurred in the past. See for example Tim Lohman, 'Defence to Overhaul Collins Class Submarine Comms', *Computerworld*, 16 April 2010, <www.computerworld.com.au/article/343394/defence_overhaul_collins_class_submarine_comms/> [Accessed 1 January 2018].

operational security must be a deliberate effort across sensitive capabilities. This effort must take full account of the growing technological sophistication of strategic competitors and potential adversaries, the likelihood of insider threats, the vulnerabilities associated with maintaining a technologically sophisticated force, and the key information age trend of 'information availability'. This paper also advocates a broader understanding of the often-prominent signatures associated with contemporary communications systems. Intelligence threats from strategic competitors are ever-present, including in Australia and on 'private' communications systems, and sensitive national capabilities will remain a high priority for foreign intelligence targeting. Unauthorised information disclosures must be anticipated, but deliberate actions can be taken to identify and then protect the most sensitive 'Crown Jewels'. This will ensure that units like submarines and Special Forces will remain operationally viable unconventional capabilities.

Martin White is a serving Australian Army officer with extensive operational and command experience. He is currently completing a PhD through La Trobe University, focused on Australian defence policy.