Cyber test and evaluation in a maritime context

Sub Lieutenant Luke Boswell, Royal Australian Navy
Sub Lieutenant James Keane, Royal Australian Navy
Sub Lieutenant Connor Mooney-Collett, Royal Australian Navy

Since the development of the Internet in the 1960s, modern states have become completely dependent on their ability to communicate in the global information domain. Cyberspace, a key component of this domain, is defined in the ADF's 'Defence strategic cyber operations policy 2010' as:

> Cyberspace is a component of the global information domain consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers, and their resident data (ADF, 2010).

At the same time, technology has changed the way that nations project influence and power. This has driven significant changes within all modern navies, including the Royal Australian Navy (RAN). However, the accelerating growth of cyberspace is dynamic and unpredictable, which means that navies (and others) must continue to adapt in order 'to effectively conduct maritime operations in the information age' (Kirk, 2016).

This article outlines the significance of the effective management of cyber, particularly for the RAN, developing an argument for cyber as a key component of operational testing and evaluation. After introducing the key concepts, the article explores the drivers of change within the RAN, which have been categorised into three significant technology shifts: integration, connectivity and dependence. The article then discusses the role of testing and evaluation in achieving cyber-worthy capabilities, and introduces two frameworks, before concluding with a number of recommendations.

The militarisation of cyber

The world has progressed from analogue to digital, radio to fibre, and from phone lines to data packets. But information has continued to

be captured, stored and transmitted. In the context of information warfare (IW), where 'decision superiority' is predicated on information advantage, cyber technologies both reduce the material resources required to develop and deliver effects, and increase the speed with which those threats can evolve. In this information domain, cyber-weapons can also be used to destroy or disable critical infrastructure, which previously was only vulnerable to physical damage.

However, it is rarely possible to identify the source of a cyber-attack with certainty. Therefore, building an accurate picture of the threat in cyberspace is complicated, not least because of the blurring between state and non-state actors. Also, malicious activity in cyberspace is not just contained to the intangible domain of information. The widespread embarrassment of cyber-related failures has spilled into the physical domains. Consider the destruction of nuclear centrifuges in an Iranian enrichment plant from the Stuxnet virus. An increasing amount of civilian infrastructure, such as telecommunications, banking and transportation systems, is also increasingly vulnerable.

Within modern militaries, the trend towards cheap, modular and flexible networked and reconfigurable systems has driven acquisition patterns, including in the RAN. For example, where a valve may have been controlled by a mechanical switch in the past, it is now controlled by an electronic switch connected to a computer. Unlike their predecessors, these new systems exist in cyberspace and hence are vulnerable to cyber-attack.

The role of testing and evaluation

A common misconception is that all vulnerabilities can be identified and addressed before a system is deployed. Most vulnerabilities can be mitigated through good design and extensive testing. However, there are variables which exist only while the system is operational, the most significant of these being human error. This, combined with regular configuration change, necessitates an operational approach to cyber testing and evaluation.

To achieve their intent, a malicious actor may take advantage of one or more vulnerabilities. Where an actor has both the intent and capability to exploit a vulnerability, this is known as a threat. A single vulnerability in isolation may be irrelevant in the same way an unlocked door may be of no interest to anyone. However, when combined with other vulnerabilities, it may be the crucial ingredient. Consider an unlocked vault inside the building with an unlocked door; this combination of vulnerabilities is potentially devastating. Therefore, it is essential to guide any search for vulnerabilities from an understanding of intent, which necessitates the testing of a system while it is operating normally, that is, configured as it is when deployed.

A common guide to cyber-security is Kerckhoff's principle, reproduced as Shannon's maxim, that 'one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them' (Shannon, 1949). The idea being that a system should be secure even if everything about the system, except the key, is public knowledge. Maintaining secrecy with respect to the design and configuration of a network is merely a layer of security, and not intrinsically any guarantee of its security. Hence, monitoring for malicious activity is not enough. It must be assumed that any system is capable of being compromised. Capabilities must, therefore, be engineered with the ability to recover from and continue functioning in a degraded information environment.

Cyber in the maritime domain

Warships are not beyond the reach of cyberspace, even at sea, and the RAN is obviously no exception. The implications of a cyber-attack stretch beyond the operational to the potential reputational impact on the RAN and its strategic alliances. When cooperating with other forces in a joint or combined task force, it will be essential that Australia's capability does not represent a potential vulnerability, and therefore a risk to the broader mission and other forces.

Increasing demand for more flexible maritime capability has driven changes within the RAN, which are broadly categorised as three significant technology shifts, namely the adoption of integrated architecture, increasing connectivity to external systems, and a deeper dependence on defence industry for logistics support. Each of these has contributed to the breaking down

of information 'silos', which results in greater interdependence between systems. Even though these shifts are a result of technological progress, they each represent sources of cyber risk to the RAN.

Integration

Many systems aboard modern warships are connected to each other and integrated into a single architecture. This is a result of the shift from federated towards integrated architectures. The most significant reasons for this are that integrated architectures are cheaper, more modular and reconfigurable in a way that allows for more capable platforms to be developed. However, this flexibility also represents a source of cyber risk due to vulnerabilities being difficult to find or potential adverse interactions between systems. This is because it is impractical to precisely define the relationships and interactions between systems during design. The greater degree of connectedness between the systems in an integrated architecture also means that vulnerabilities in one system can propagate to another.

The management of cyber risk must be considered throughout the whole capability lifecycle and not just during the acquisition phase. Securing a poorly designed system can be prohibitively expensive. Every time a system is added, its software modified, or the network itself reconfigured, there is an opportunity for new vulnerabilities to arise. For example, consider the installation of new washing machines with automated alarms being integrated into a ship's monitoring network. If the washing machine software is poor quality, it may contain a vulnerability which could adversely affect the ship's monitoring system. Establishing requirements for cyber-security has, among other benefits, the additional outcome of improving the quality of software that is developed. It is precisely the flexible nature of interactions between systems that increases the cyber risk a warship is exposed to.

Connectivity

The operational environment is inherently connected, with both joint and combined forces routinely operating together. To support this operational environment, maritime capability is becoming increasingly connected to systems in the sea, air, land and space domains. In addition, terrestrial networks have an increasing support and operational role on ship activities. Every transmission to and from a ship presents an opportunity for a hostile actor to either disrupt, deny, degrade, destroy or deceive the ship. This is because there is potential for a skilled actor to manipulate the electromagnetic spectrum or other transmission medium in a way that adversely affects the ability of the ship to perform its mission effectively.

Dependence

An increased dependence on support from external organisations has resulted from accelerating RAN acquisition of complex capability while simultaneously reducing the uniformed footprint. Core functions that were previously undertaken by the RAN, such as maintenance and logistics, are now being fulfilled through external organisations. These services are increasingly being transacted in cyberspace as Defence brings products and services online. For example, 'WebForms' are rapidly taking the place of paper to facilitate storing, processing and tracking of information. This progress is necessary to support additional capability with reduced manning, and it facilitates an increased volume and quality of communication between and within Defence units and external organisations. However, the impact of these services needs to be considered from a cyber security perspective to understand the risks that the RAN is exposed to.

By facilitating the breaking down of information 'silos', technological adoption facilitates an increased flow of information between support organisations. However, this greater degree of interconnectivity means that any vulnerabilities in one system can more readily propagate to and compromise other systems in the network. Consequently, the security of information now stored in cyberspace needs to be considered as there is increased dependence on connected systems and as integrated organisations are trusted to manage their cyber domain with integrity.

IW continues to play a significant role in the maritime context, especially as the RAN has moved

into cyberspace with more integrated, connected and dependent capability. It follows that the RAN must be proactive in its pursuit of measures to manage risks in cyberspace. The avenue proposed by this article for effective cyber defence is for cyber security to be introduced through Navy engineering and, specifically, for cyber testing and evaluation to be implemented as part of the seaworthiness framework to address the challenges associated with operating in the 21st century.

Testing and evaluation towards cyber-worthiness

The concept of 'cyber-worthiness' may be considered a cyberspace analogy to 'seaworthiness'. The implication being that RAN capability must be prepared to meet potential adversaries in cyberspace to continue the fight at sea. Accordingly, cyber-worthy should be included within existing policy alongside fitness for service, safety, and environmental compliance. This would ensure that cyber is considered at every stage of the capability lifecycle and as part of the Sea Release Assurance Framework. To achieve this, operational test and evaluation needs to be the primary driver for ensuring that RAN maritime capability is cyber-worthy.

As an analogy to seaworthiness, a ship that is cyber-worthy can operate effectively even while in a contested, degraded or operationally limited information environment. For maritime capability which depends on cyberspace to operate effectively, this would suggest that the ship (and its supporting elements) is resilient to adverse conditions in cyberspace. Therefore, cyber-worthiness could be seen as the process which assures that maritime capability is cyber-worthy; that is, well-suited for operations, and resilient to adverse conditions within cyberspace.

Paul Kirk asserts that a key challenge for the implementation of the RAN's 'Information warfare: Master Plan 2030' with respect to cyber has been an absence of clear strategy and end-states (Kirk, 2016, p. 5). So the concept of cyber-worthiness and its incorporation into existing policy would seem to be the right way to respond to this challenge. This would require that 'objective quality evidence', specific for cyber, be developed as part of the Sea Release Assurance Framework, with the evolution of operational test and evaluation the natural candidate to drive this strategy.

The role of operational testing and evaluation in cyber-worthiness

Commenting on the importance of operational testing, the US Department of Operational Testing and Evaluation has asserted that:

> The cyber threat has become as real a threat to US military forces as the missile, artillery, aviation and electronic warfare…. Real-world cyber adversaries regularly demonstrate their ability to compromise systems and inflict damage. Operational testing must examine system performance in the presence of a realistic cyber threat (cited in Joiner, undated).

It follows that the tools of operational testing and evaluation, such as penetration testing and security audits, need to be employed to ensure that the capability is cyber-worthy. Existing RAN policy was originally developed for assets with long development times, defined operating envelopes, and long in-service life. However, the policy obviously now needs to be adapted to evolving technology, such as a process outlined at Figure 1.

The below is a simplistic illustration of the process used to evaluate an individual capability in a realistic environment. These steps are explained further as follows:

- **Understand requirements.** Develop the cyberspace context the system operates in. Examples include what systems are integrated, and what role the system has in supporting the mission.
- **Characterise attack surface.** Understand the interface between integrated systems

Figure 1: Operational test and evaluation process for cyber (Christensen, 2016)

and the potential methods an adversary could use to penetrate the system.

- **Identify vulnerabilities.** Analyse the system for potential failure modes or conditions which an adversary may use to their advantage.
- **Conduct penetration testing.** Interrogate the system to exploit vulnerabilities.
- **Operational assessment.** Evaluate test results to assess the ability of the system to resist realistic cyber threat.

Christensen's model represents a good reference for the RAN to develop its own process. However, establishing a process to evaluate individual capability is only the first step towards cyber-worthiness. In addition, there must be an overarching strategy or framework to guide its implementation.

The 'five pillars' framework

Symantec, a leader in commercial anti-virus software, has suggested a 'five pillars' framework to encourage organisations to revisit their security posture and move their focus towards cyber-resilience (see Figure 2). This framework explicitly avoids prescriptive behaviour, such as checklists, but instead promotes a risk-aware approach through evaluations based on a realistic picture of the threat environment as built and understood through active cyber intelligence (Kirk, 2016). This is where operational testing and evaluation would represent a natural fit for driving such an approach to cyber-worthiness within the RAN.

The five pillars represent key functions to manage cyber risk through a continual process of refinement, as explained as follows:

- **Identify.** Conduct an infrastructure and information assessment to establish a baseline understanding of known security vulnerabilities.
- **Protect.** Develop and implement safeguards for critical infrastructure and services to limit or contain the impact of an attack. How up to date measures are for a system in its current configuration is a measure of how well the system is protected.
- **Detect.** Develop and implement processes to identify an attack in progress (real time), assess the systems that are affected (near-real time) and ensure appropriate and timely response. To achieve this, networks should be continuously monitored and relevant activity logged as indicators of a potential attack or for future analysis.
- **Respond.** The ability to respond to a cyber-attack and remediate effects is a measure of cyber-worthiness. This requires the ability to understand the likely effects of cyber-attack and develop a plan to coordinate a response.
- **Recover.** Develop and implement plans to restore data and services that may have been impacted during a cyber-attack.

This section has developed the concept of cyber-worthiness and argued for operational testing and evaluation as a key driver towards its implementation. Regardless of the path taken, the costs for delay or inaction are great. Therefore, the following section outlines three specific recommendations for RAN consideration.

Integrating cyber operational testing and evaluation

The RAN has adopted increasingly complex technological capabilities, however, its adoption of industry best practices has not kept pace. This is a type of technical debt, where the interest is unnecessary cyber risk exposure and the opportunity cost of poor technology utilisation.

In 2014, the Australian Signals Directorate published a document titled 'Strategies to mitigate targeted cyber intrusions', which outlined specific recommendations to combat elementary threats in cyberspace (Australian Signals Directorate, 2014). In addition to implementing those recommendations, this article suggests the RAN should consider the following.

Figure 2: The 'five pillars' framework to evaluate individual capability (Symantec, 2014)

Establish RAN cyber capability

The RAN needs to develop its own cyber capability, which should include the concept of 'cyber-worthiness'. The reasons are three-fold. Firstly, effectively combating cyber demands a deep technical understanding not only of the technology but also the operating environment. This complexity cannot be outsourced to another department or organisation. Secondly, the RAN is ultimately accountable to deliver seaworthy material. This requires that decision-makers at every level of the command chain be aware of cyber. Responsibility cannot be outsourced because, like safety, it is the responsibility of everyone to practise good security. To achieve this, the RAN needs to ensure adequate training and develop a cyber-aware culture. Finally, cyber specialists must be embedded, or at least made available, within acquisition and sustainment projects, in order to facilitate a process of certification and accreditation of cyber-worthy material.

Integrate cyber-worthy into the seaworthiness framework

The seaworthiness framework is the natural place to integrate the concept of cyber-worthiness. Cyber-security must be as fundamental as ship stability or safety. Ideally, requirements for cyber-worthiness would be established early in the acquisition and design processes. However, existing capability must also be considered where it is vulnerable to cyber-attack. Addressing issues proactively, before they are realised, is far cheaper than the alternative.

Some consider cyberspace to be the realm of specialists with techniques that are difficult to understand and apply. However, there are established and readily adopted controls which do not require expert skills. These practices have analogies such as key control or monitoring logs. Essentially, good cyber-security is largely the diligent application of basic controls to manage risk (Kirk, 2016).

Collaborate with existing leaders to develop RAN policy

RAN policy is sparse on cyber at an unclassified level. Where cyber is employed, it is through specialists or by an external organisation. However, this is an unsustainable model to deliver capability that is cyber-worthy. While specialists and external organisations can provide support in critical areas, they cannot be responsible for the entire RAN. Moreover, while much of the discussion on cyber is classified, this article has argued that to establish cyber-worthiness as a process, underlying every maritime capability, knowledge needs to be embedded in Navy's people.

To that end, the RAN must collaborate with existing leaders in cyber to develop its policy. The RAN has a unique operating environment but appropriating experience elsewhere would assist in developing relevant policy and practices. Industry generally has adapted quickly to cyberspace, and expertise already exists within Australia Government departments. The US Department of Defense has also been supportive of RAAF efforts on the Joint Strike Fighter project. The RAN should leverage these and other relationships to gain access to additional expertise. The importance of such collaboration has been summarised as:

> As our dependence on information networks increases, it will take a team to eliminate vulnerabilities and counter the ever-growing threats to the network. We can succeed in securing it by building strong partnerships between and within the private and public sectors, encouraging information sharing and collaboration, and creating and leveraging the technology that affords us the opportunity to secure cyberspace (Alexander, 2013).

Conclusion

With cyber-attacks on Australia and Australians increasing, even crossing into the physical domains, it is evident that the RAN is not immune. Technology shifts in the maritime domain have driven new and advanced capabilities, which have increased integration, connectivity and dependence on cyberspace, representing a significant risk. It follows that a modern warship is vulnerable to these risks, even at sea.

This article has argued for the concept of 'cyber-worthy' to be included in existing RAN policy, alongside fitness for service, safety, and environmental compliance. It has also argued that operational testing and evaluation should be the key driver of cyber-worthiness.

Employing the tools of operational testing and evaluation, such as regular penetration testing and security audits, provides the best way to manage this risk.

Two frameworks have been presented which explicitly avoid promoting prescriptive behaviour but instead deliver a risk-aware approach. The article has also suggested three specific recommendations for RAN consideration, namely that the RAN develops its own cyber capability, that cyber-worthiness be integrated into the seaworthiness framework, and that the RAN collaborates with best-practice leaders to develop its policy for cyber-worthiness.

Cyberspace represents a serious threat. However, as Australia and like-minded countries increasingly rely on cyberspace to enhance its warfighting capability, the opportunity arises to manage the risks of operating in cyberspace and, indeed, to turn Australia's command of the new battlespace to its benefit.

Sub Lieutenant Luke Boswell joined the RAN in February 2016 and is currently serving as an Assistant Weapons Electrical Engineering Officer on HMAS Adelaide. He is under training to be a professional engineer within the RAN, after graduating from The University of Melbourne with a Bachelor of Science and Master of Engineering degrees. While at university, he was President of the Electrical Engineering Student Society.

Sub Lieutenant James Keane joined the RAN while studying a Bachelor of Engineering (Honours) in Naval Architecture at the Australian Maritime College (AMC). He was president of the AMC Autonomous Technologies Society and involved in a number of maritime automation projects, with the results of his research published, including in China and the US. He is currently completing Engineering Officer training while serving as Assistant Marine Engineering Officer on HMAS Leeuwin.

Sub Lieutenant Connor Mooney-Collett joined the RAN in June 2014 and is currently serving as an Assistant Weapons Electrical Engineering Officer on HMAS Stuart. He studied a Bachelor of Engineering (Electrical) at the University of Queensland, where he was a member of the Electrical Engineering Student Society and worked on a number of computing and electronics project teams.

References

Alexander, K., (2013), 'Commander of US Cyber Command and National Security Agency Director, General Keith Alexander, to Keynote Day One of Black Hat USA 2013', *PR Newswire* [website], 14 May 2013, available at <http://www.prnewswire.com/news-releases/commander-of-us-cyber-command-and-national-security-agency-director-general-keith-alexander-to-keynote-day-one-of-black-hat-usa-2013-207361951.html> accessed 18 November 2016.

ArsTechnica (2016), 'Cisco confirms NSA-linked zeroday targeted its firewalls for years', *ArsTechnica* [website], available at <http://arstechnica.com/security/2016/08/cisco-confirms-nsa-linked-zeroday-targeted-its-firewalls-for-years/> accessed 4 October 2016.

Australian Broadcasting Corporation (2013), 'Brandis confident ASIO "dealt with" hacking attack', *ABC* [website], 29 May 2013, available at <http://www.abc.net.au/news/2013-05-29/brandis-briefed-by-asio-on-china-hacking-claims/4719886> accessed 4 October 2016.

Australian Broadcasting Corporation (2016), 'Turnbull confirms weather bureau cyber attack', *ABC* [website], 21 April 2016, available at <http://www.abc.net.au/news/2016-04-21/australia-admits-it-can-launch-cyber-attacks-turnbull/7343620> accessed 4 October 2016.

Australian Centre for Cyber Security (2016), 'Proposal for an Australian Cyber Corps', *University of New South Wales at Australian Defence Force Academy* [website], available at <https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/publications/Australia%20cyber%20civil%20corps%20Draft%20concept.pdf> accessed 4 October 2016.

Australian Cyber Security Centre website available at <https://www.acsc.gov.au/> accessed 14 April 2017.

Australian Cyber Security Centre (2016), 'ACSC threat report 2016', *Australian Cyber Security Centre* [website], available at <https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf> accessed 17 November 2016.

Australian Defence Force (2010), 'Defence strategic cyber operations policy 2010: Australian Defence cyber operations lexicon', unclassified draft in possession of author(s).

Australian Signals Directorate website available at <https://www.asd.gov.au/> accessed 14 April 2017.

Australian Signals Directorate (2014), 'Strategies to mitigate targeted cyber intrusions', *Australian Signals Directorate* [website], available at <http://www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf> accessed 26 October 2016.

CERT Australia website available at <https://www.cert.gov.au/> accessed 14 April 2017.

Christensen, P., (2016), 'ZEIT8231 - course notes, systems development practices closely aligned to T&E', University of New South Wales at Australian Defence Force Academy, Canberra, held by author(s).

Department of the Prime Minister and Cabinet, 'Australia's cyber security strategy: enabling innovation, growth and prosperity', *Department of the Prime Minister and Cabinet* [website], 2016, available at <https://cybersecuritystrategy.dpmc.gov.au/> accessed 14 April 2017.

Engadget (2016), 'Critical security flaw found in Lenovo PCs ... again', *Engadget* [website], available at <https://www.engadget.com/2016/07/04/critical-security-flaw-found-in-lenovo-pcs-again/> accessed 4 October 2016.

Joiner, K., (undated), 'Integrating cyber survivability into future ADF platform development and acceptance', *University of New South Wales at the Australian Defence Force Academy* [website], available at <https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/Cyber-survivability%20TnE%20-%20Dr%20Joiner%20PPP.pdf> accessed 18 November 2016.

Kirk, P., (2016), 'Navy information warfare: developing an information warfare strategy for the Royal Australian Navy', Master's thesis at the University of New South Wales at Australian Defence Force Academy, abstract available at <https://oatd.org/oatd/record?record=oai%5C%3Aunsworks.unsw.edu.au%5C%3A1959.4%5C%2F56982> accessed 14 April 2017.

Lehmann, M., (2014), 'Chinese national interests and cyber capabilities: a 'red team' future', *Australian Defence Force Journal*, Issue No. 195, pp. 12-20.

Nguyen, N., (2015), 'Evolution of the battlefield: strategic and legal challenges to developing an effective cyber warfare policy', *Australian Defence Force Journal*, Issue No. 196, pp. 60-9.

Prime Minister Malcolm Turnbull, M., (2016), 'Cyber security strategy', *Prime Minister* [website], 21 April 2016, available at <https://www.pm.gov.au/media/2016-04-21/australias-cyber-security-strategy> accessed 14 April 2017.

Royal Australian Navy (2011), *Information warfare Master Plan 2030*, Defence Publishing Service: Canberra.

Shannon, Claude (1949), 'Communication theory of secrecy systems', *Bell System Technical Journal*, Vol. 28, No. 662.

Sydney Morning Herald (2016), 'Census cyber attacks likely from low-level hacktivists but origins may never be proved, experts say', *Sydney Morning Herald* [website], 11 August 2016, available at <http://www.smh.com.au/federal-politics/political-news/census-cyber-attacks-likely-from-lowlevel-hacktivists-but-origins-may-never-be-proved-experts-say-20160811-gqqkag.html> accessed 4 October 2016.

Symantec Corporation (2014), 'The cyber resilience blueprint: a new perspective on security', *Symantec* [website], available at <https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilience-blueprint-wp-0814.pdf> accessed 27 October 2016.

Thompson, M., (2012), 'The cyber threat to Australia', *Australian Defence Force Journal*, Issue No. 188, pp. 57-70.