Cybersecurity Challenges and Processes for Australia's Future Submarine

Keith F. Joiner
University of New South Wales Canberra at ADFA
Systems Capability Centre
Canberra, Australia
k.joiner@adfa.edu.au

Simon Reay Atkinson
University of Sydney
Centre for International Security Studies and SCSN
Sydney, Australia
simon.atkinson@sydney.edu.au

Elena Sitnikova
University of New South Wales Canberra at ADFA
Australian Centre for Cyber Security
Canberra, Australia
e.sitnikova@adfa.edu.au

***Abstract*— If Australia's Future Submarine Program is to deliver, it needs to rapidly develop a comprehensive Systems Security Engineering (SSE) and Cybersecurity Test and Evaluation (CT&E) Strategy that provisions Australian owned and operated infrastructure to design, build, demonstrate and sustain cyber-resilience in critical submarine systems. Failure to act swiftly creates significant program risk that can only be mitigated through costly design rework and in the near term will result in capability limitations. Submarine T&E Sites and Cyber Resiliency are interdependent and inter-related. The Program Director has committed to building land based test infrastructure, however a serious concern is that if there are any delays in the development of organic test capability, these will force the French designer and builder, Naval Group (formerly DCNS), to provision French sites solving the near term problem but adversely impacting Australia's ability to take long term ownership of Submarine cyber-resilience. Australia can exploit lessons learned from US DOD Cybersecurity initiatives to help mitigate Australia's Future Submarine Cybersecurity Risks.**

Cyber has become a supposedly cheap first-strike weapon of political choice by potential adversaries in a milieu placing insurgency, terrorism, international crime and state-based influences in close un-regulated proximity. The merging of electronic and cyber warfare means that no physical artefact such as a submarine, however unconnected or firewalled it may be, is immune to probing. The quantum attack surface (QAS) of the future submarine is as much in the past, as it is in its designs today and operations tomorrow. It must not only survive to be credible, but even before build is part of an offensive cyber capability for contemporary deterrence. Cybersecurity craft in the U.S. has determined that critical Defence systems, like submarines, nuclear weapons and space surveillance, require robust security systems engineering and Cybersecurity T&E to build and sustain robust cyber-resilient systems. The future submarine, and every current and future Australian DoD capability has cyber-resilience as a requirement, and there is an opportunity to ensure these requirements flow down through to design, build and test by leveraging the approaches used by the U.S. DoD. Secondly, this paper outlines the security systems engineering and Cybersecurity T&E challenge could be addressed by adopting U.S. DoD best practices to engineer, test and sustain cyber-resilient systems. Lessons learned from the U.S. DoD can be used to inform and refine Australia's Future Submarine Cybersecurity program.

Keywords- cybersecurity, cyber-resilience, future submarine design, land-based test sites, quantum attack surface, test and evaluation

I. INTRODUCTION

The Australian National Audit Office [11] gives an overview of Australia's future submarine and the decision to select the French Naval Group and Lockheed Martin as the designers of the Barracuda. Furthermore, Stanford in [48] covers the economic, technical, strategic and other risks of this Program and the choices made thus far, in a pending comprehensive public policy report and exposition. From a technical risk perspective, Joiner and Reay Atkinson in [33] summarised significant lessons learnt from the Collins Submarine program concerning inadequate test and evaluation and insufficient land-based testing capability (i.e., in [7], [43]). A concern of both of these reviews is the emerging deviation of the Submarine Program from lessons learnt, best practice and extant defence policy by seemingly not conducting preview test and evaluation of reference design classes to disclose technical and operational risks prior to design down-select and contract (i.e., in [31], [13], [10], [4]).

Concerns were raised about releases of the French-Indian submarine, after which Minister Pyne gave assurances about cybersecurity to be applied to French-Australian submarine planning [49]; [36]. Such cybersecurity risks and mitigation and contingency planning for the future submarine have not been outlined in any detail. They warrant a degree of public outline and reassurance, which this paper tries to provide. The increasing threat of cyber-enabled warfare for Australia has been reviewed extensively by Austin in [3], following instances of cyber espionage; including the Australian Secret Intelligence

Organisation building [22], [25]; and increasing instances of cyber-attack [41]. The Australian Government has focused its Department of Defence (DoD) on meeting the new threat [4], however, according to Joiner [32] much more could be done practically to leverage U.S. DoD initiatives in cybersecurity T&E. Proposals by Joiner, Sitnikova and Tutty [34] on how to engineer cyber-resilient systems in the Australian DoD has been followed more recently by an extensive exposition by Joiner and Tutty [35] examining how the U.S. DoD has undertaken at least six major initiatives to give more integration and information assurance to its complex and interconnected systems and how that may be leveraged by the Australian DoD. This paper extends on these broader works with research into how those initiatives can specifically apply to the Submarine Program. In particular, recent research into how to create 'trusted' supply chains for software-intensive systems will be overviewed [2], [51] and compared with public efforts thus far by the Submarine Program to shape Australian Industry involvement.

II. SOVEREIGN TESTING

When we talk about Sovereign Testing we are essentially introducing Knowledge Sovereignty, which may be considered as:

> *The independent authority of a state without interference from outside sources or bodies to abduce, conceive, deduce, design, induce, devise new ontologies and transfer info-technological skills, understanding, comprehension, expertise, proficiency, capacity, capability, learning, science and wisdom for its own socio-ethical purposes.* [58]

Critically Sovereign Testing connects with Knowledge Transfer as part of Knowledge Sovereignty; as distinct from but clearly connected with Sovereign IP and Sovereign Capability:

> *Knowledge Transfer 'goes beyond the translation of technical manuals from the French into Australian Books of Reference (ABRs) and engineering / data sheets. Without it there is no point to building in Australia. Without a sovereign capability over the asset, even the ability to support and maintain the programme is in jeopardy. The more so given the added risk in replacing the existing nuclear propulsion system with lead acid batteries and diesel engines, possibly in collaboration with the German manufacturer TKMS'. Without understanding the socio-cultural context in which the submarine was abduced, abstracted, conceptualised, deduced, designed, induced, modelled, built and operationalised, it will not be possible to de-risk Knowledge Transfer, or to successfully translate and sustain, build and maintain its operations in the Australian context.* [59]

Knowledge Transfer is essentially a quantum phenomenon; connecting past, present and future with the indivisible '*knowledge that is both socio and info-technological*' [60]. In this respect, we need to consider the impact of cyber as synthesising and combining both Socio and IT systems and being:

> *A technologically bounded, largely immeasurable, strongly scientific, stochastic control space (ITS); comprising virtual-media and the display of data dealing with the real communication of* [historical] *facts and the conceptualization of other plausible possibilities, themselves capable of generating strong physical and weaker more social effects and influencing them* '. [61]

Last year the Australian Chief of Navy and the Submarine Project Director committed to the necessary submarine land-based test sites that would commence build in South Australia in 2018 and complete in 2019 [14], [46]. Moreover, Vice Admiral Tim Barrett [14] outlined that a '*rolling build philosophy has been identified as a keystone of this program* … [that] *will ensure the regional superiority we pursue can be attained and endure*.' The importance of these land-based test sites to informed decisions and thus governance on the Submarine Program has been covered [33], [15]. For example, the broad aim of the Submarine Program used by Bradley *et al*. [15] to illustrate a complex systems governance model for the Program is similar to Barrett's [14] and it reiterates the key strategic role these test sites have in areas like sovereignty, early public confidence, evolving to meet new threats including cybersecurity, and ultimately avoiding another imported design 40 years from now:

> '*To maintain political, military and public trust that the FSM capability is continually evolving to meet the maritime threat with adequate efficiency.*' (p. 6)

The lessons learned in the U.S. [57] need not be relearned by Australia. Early, strategic investment in security systems engineering and Cybersecurity T&E improve program cost, schedule and performance. Conversely, failure to make those investments has adverse programmatic and mission impacts.

The land-based test sites are also a chance to reconnect this submarine program with best practice[1] Australian DoD test policy [31], [10] and the lessons learned from the Collins program [7], [43]. A serious concern with any delays in test capability is that the French designer and builder, Naval Group, will soon hold technical sway over knowledge transfer and so project direction, and it may suit their commercial purposes for such test sites to be deferred, so French sites retain knowledge sovereignty. Such an outcome would seriously impair a sovereign testing capability and lead to difficulties in knowledge transfer. It may also lead to the Australian DoD giving further deference – essentially creating a colonial mindset – so as to avoid political sensitivity. For example, difficulties in Knowledge Transfer for sovereign testing occurred on previous partially-French projects, like the Mu90 Lightweight Torpedo. The Torpedo was mistakenly thought to be off-the-shelf (2000-2004); yet took some 13 years to get properly tested for operational release. The last seven years of which occurred after full commitment to all production and delivery of Australian DoD war-stock [8], [9].

An illustration of independence in test and evaluation is at Figure 1, showing the importance of unfettered factual results being equally available to investors, technical authorities and operational managers.

[1] For example in [13], [16], [33], [35], [38]

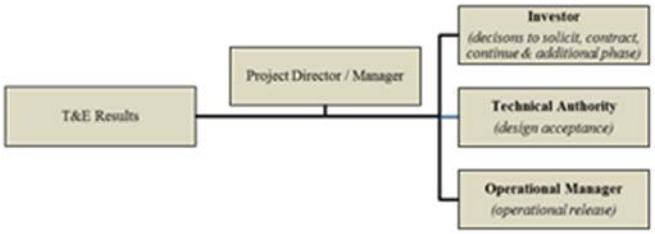

Figure1. Illustration of Independence in Test and Evaluation

Unfettered sovereign test results have been shown in Parliamentary evidence and ANAO review to have been essential in hindsight [4] both as part of Defence market testing (i.e., Land Project 121 down-select) and acceptance into initial service (i.e, Landing Helicopter Dock ships). If major capabilities outsource conduct of developmental and acceptance testing, safety assessments, usability trials and operating procedures to a contractor without adequate residential project staff and representative operators present, then the transfer of risk and delay in resolving risk is contrary to the very intent of the project in giving the tasks to the contractor in the first place [10].

If the French Naval Group undertake significant portions of the submarine systems virtual, constructive and live simulation testing in France, significant Knowledge Transfer issues will make the flow of results as shown in Figure 1 much harder. Similarly, if Lockheed Martin undertake the same simulation testing in the U.S. there are risks to test results making it unfettered to the stakeholders, especially if they use proprietary simulation models that have not been accredited by the U.S. DoD (i.e., F-35 aircraft) [4]. Constraints on travel budgets hampered representation of operators and technical experts on the Landing Helicopter Dock ship during safety and usability assessments and that program only involved travel from Canberra to Melbourne, much less than Cherbourg, France [10], [12]. Cybersecurity assessments for cooperative vulnerability and penetration testing further challenge outsourcing of such work without close cooperation between the DoD and contractors [16], [56]. Work by Fowler *et al*. [23] shows there are extant Australian DoD practices like systems safety that can be leveraged to cooperate with industry in independent cybersecurity, provided these practices are being followed and not overly outsourced. Also, Joiner and Tutty [35] outline U.S. DoD initiatives to efficiently manage independent cybersecurity testing through distributed simulation, experimentation exercises and through the test network infrastructure on which these are based.

Representative land-based test sites across all submarine systems should be in Australia and under Australian DoD control as soon as possible if the design work is to be successfully exported in an enduring way and so as to enable knowledge sovereignty and provide for timely and informed decision making and taking [62]. Such test sites significantly de-risk the Program by helping to maintain public support, and enabling fully representative technical and operational participation throughout the rolling complex software-intensive systems development in safety, usability [55], reliability, maintainability, availability and cybersecurity assessments. Cybersecurity has traditionally been considered as one of the 'ilities" with tests focussed on mandatory compliance and responses to incidents during the operational phase of land-based tests as a reactive process [37], rather than developing social trusts and assurances. Perspectives on how to "build security in" can establish a common language to use in designing the software-intensive systems making risk trade-offs throughout project's acquisition lifecycles, thus minimizing the number of systems vulnerabilities and reducing time for land-based tests. Moreover, early investment in representative land-based sites can expected to add some up-front cost to the submarine program because they entail high fidelity virtual and bench-level representations of the submarine systems in progressive upgrade ahead of all future boats.

As observed by the U.S DOD [57], the return on investment in test infrastructure can drive down acquisition costs, because the Technical Debt, typically incurred because of flawed engineering and deferred testing, can be dramatically reduced. Australian controlled land-based test sites will have additional workforce and National Security benefits. Land-based test infrastructure provides fertile ground to grow and enhance Australia's Cybersecurity Workforce. From a National Security perspective, this infrastructure enables Australia to adopt agile, iterative and incremental acquisition and testing approaches that ultimately enhance Australia's ability to keep pace with adversaries in Cyberspace.

Despite these lessons learned, land-based test sites are likely to face enormous pressure to be scaled back, as they did on the Collins Program, in favour of foreign test sites and the actual build. Such pressure is likely to be a system-by-system argument, where for example, propulsion and power systems may get an Australian test site, but sonar, weapons, combat and communication systems remain foreign. Any such parsing of the submarine systems puts enormous risk on the higher-order aim of the Submarine program and on the actual submarines to resolve operational and technical issues in-build and in-the-water rather than beforehand and to become truly an Australian Sovereign Capability. Another unfortunate risk is that the key technical and operational personnel now advising on the test site proposals are posted with their families to Cherbourg and the U.S. to oversee the design, potentially for the next fifteen years, and comprehensive early test sites would significantly compete with that overseas program for funding, attention and influence.

In developing these land-based test sites to enable live, virtual and constructive distributed simulations [35], it is crucial that the simulations are accredited for intended use, as is required in the U.S. DoD [19]. While such accreditation seems a significant non-recurring expense, if the complex adaptive software elements and interconnectedness of the submarine exhibits emergent properties, as many modern defence systems are, then the quid pro quo of the test sites will be the wherewithal to begin software verification much earlier and continue into life as detailed by Hecht [28], Normann [40] , and Cofer [17].

III. Cyber Warfare Threat and Opportunity

Cyber is becoming the cheap first-strike weapon of political choice by potential adversaries in a kind of merging of insurgency, terrorism, international crime and state-based influences [29], [35]. The merging of electronic warfare and cyber-warfare means that no platform, however unconnected or

firewalled it may be, is immune to probing within its systems [32]. The future submarine must not only survive and be credible in this Information Age, but actually ought to be a potential purveyor of offensive cyber like that described by the Australian Prime Minister [41], so that it remains a contemporary deterrence.

Cyber first and foremost is connected to the socio, meaning interfering with the socio-functioning of the system, for example by cyber-attacks, creates an instability in the synthetic ecology which interferes with the human psyche; creating further instability and uncertainty [60]. Sovereign Testing of the entire quantum attack surface is therefore fundamental to Knowledge Transfer and cybersecurity, without which Australia will not have Knowledge Sovereignty over the future submarine.

Cyber-power is relatively cheap, available and largely anonymous, such that it is attractive for peacetime as it is for war [47], especially for deterrence by smaller powers in the Asia-Pacific region [29]. These attributes also make cyber-power attractive to non-state actors [4], [45] such as cyber criminals, terrorists, hackers, and proxy actors engaged or supported by numerous foreign governments [29, p.126], [44, p.5]. Heinl [29] forecasts that within a few years most states in the Asia-Pacific will develop some form of offensive cyber program. While Australia often relies on deterrence by alliances, kinetic military power like that referred to by Hashim [27] can be unusable in cyber warfare because attribution is slow and difficult [1], [21], [24], cyber-effects are hard to contain, and the adversaries may be globally dispersed [18]. For Australia's major military platforms like the future submarine, which operate throughout the Asia-Pacific region, they will be a cyber-warfare target starting from the first supply of software-intensive componentry for the test sites. The quantum attack surface for the Submarine Program will be defined throughout its entire life by resupplies and software updates and every contractor and subcontractor with access.

Defence acquisitions have sought to reduce costs and risks while improving interoperability for coalitions by utilising commercial components, especially computer components and software applications. As such, most defence platforms probably have a larger cyber-attack surface than they realise [50.] The increased use of commercial hardware and software to perform essential functions for mission critical systems have increased Australia's vulnerability to cyber-threats. Commercial components can be exposed to supply chain attacks as well as malicious tampering. Because re-use of commercial hardware and software is encouraged by international standards for interoperability [26], [35], [42], vulnerabilities are even more-likely to be discovered. Weapons Systems which use commercial hardware and software are extensively interconnected with other platforms [2], which increases the quantum attack surface and cyber risks.

Improving the dynamic (as in continuous and ongoing) cyber-resilience of defence platforms has three main threads:

- improved security systems engineering and Cybersecurity T&E so as to design and build in cyber-resiliency [16], [32], [34] [57];
- trusted cyber supply chains as covered in the next section of this paper [2], [51]; and
- trusted cyber-security modules or other resident cyber-threat adaptive sub-systems [23], [51].

Trusted cyber-threat adaptive modules have been the subject of recent review by the U.S. DoD's Defense Science Board [51], as these offer the ability to preserve cost-effective use of commercial off-the-shelf componentry but monitor and correct the use of such componentry with Defence-only add-ins to the architecture. The Board's proposal is as follows (p. 93):

'Further work remains in optimizing methods for hardware- and software-based integrity validation, autonomous assessment of subsystem compromise, and autonomous adaptation, including the restoration or shutdown of subsystems. It may be useful to develop so-called trusted "sidecar" modules that can easily integrate with various vehicle platforms under meaningful size, weight, and power constraints. These modules could execute out-of-band system-integrity assessments as well as host and restore the known good subsystem images. Such sidecars could also hold slight variations in subsystem images, to increase the likelihood of resistance to any specific attack. As well, a sidecar architecture could facilitate between-mission updates. Autonomous systems, especially those unable to communicate with humans, require the ability to defend themselves autonomously. Even for autonomous subsystems that are components of larger systems with humans in the loop, the timescale required to respond to cyber-attack can be far too short to allow human involvement.'

IV. Cybersecurity Acquisition and Test Planning for Submarine

The U.S. DoD's revised acquisition policy with cybersecurity integrated was issued in January 2015 and is comprehensive [16], [38]. The policy is underpinned by a clear and comprehensive Cybersecurity T&E Guide [52] that is readily available on-line. According to Joiner and Tutty [35], the *'early heart of the process for developing projects or project proposals is the Program Protection Plan, which links the traditional efforts in security, requirements and T&E with the new cybersecurity assurance requirements and activities.*' A program protection plan is normally a requirement of the U.S. DoD prior to market testing and design development, since it assesses the criticality of each of the systems, assigns security levels and then guides the necessary levels of cybersecurity assessment of the industry being solicited for the design [16], [52]. This year the Submarine Program has been soliciting Australian industry involvement in every state in Australia and guidance would seem overdue against U.S. DoD norms on the cybersecurity assessment processes that industry will need to undertake, depending on the systems they will design and build, and on the cybersecurity acquisition strategy. A list of tasks necessary to recover cybersecurity protections for the Submarine Program to the best practice documented in [52], would include the following, where page numbers given are from the U.S. DoD guidebook for ease of reference:

- For the Submarine's likely information systems, categorise the systems (p. 9) in accordance with the U.S. risk management framework (RMF – Step 1), so that it can, as is US policy, be put in the Submarine's T&E Master Plan (TEMP).
- Read-across the information system categorisation above to any extant Australian Defence ICT policy and provide

that read-across for the TEMP as an Annex to guide U.S. contractors and sub-contractors in perpetuity of the Program.

- Examine the extant Submarine Program security plan and determine what, if any improvements can be made to the cybersecurity aspects (p. 12).

- Select the cybersecurity controls appropriate to the categorised information systems (RMF – Step 2), especially any supply-chain trusted-systems controls. Provide options here for Defence approval with broad categorisation of the risks between options. For the System Threat Assessment Report (STAR) input, use appropriate representation from the Defence Intelligence Agencies.

- Compile a list of the cybersecurity requirements (p. 21) for amendment of the Submarine's Functional Performance Specification.

- Develop a security assessment plan (p. 12), especially guiding how contractors and sub-contractors will be assessed. Where the physical security assessment plans already exist, augment these with the necessary cybersecurity assessment elements focused especially on any accreditations necessary should such assessments need to be outsourced.

- Look at the elements of a Program Protection Plan (p. 13) and determine where in Australian Defence, for the Program, such management and security coverage is, or will occur. Provide that read-across for the TEMP as an Annex to guide contractors and sub-contractors in perpetuity of the Program. Alternatively, publish a Submarine Program Protection Plan.

- Develop the Cybersecurity Strategy (p. 13), including the cybersecurity T&E metrics [54].

All the above tasks would precede any cybersecurity verification planning and are essential inputs to all land-based test sites and design costings. Use of the U.S. DoD guidebook for such planning is warranted not only because it is best practice, but because the U.S. combat system being designed into the future submarine warrants the same protections it would in the U.S. DoD. Furthermore, Joiner and Tutty in [35, p. 20] assess that, '*With over fifty percent of Australian DoD acquisitions procured from the U.S., it is no longer appropriate or sensible for the Australian DoD to invent its own such guidebooks or the majority of such planning processes.*'

The US DoD has been implementing this approach for Cybersecurity T&E for some time. There are many lessons learned based upon Cybersecurity Testing accomplished at the National Cyber Range (NCR) [57]. The NCR provisions representative Cybersecurity T&E infrastructure, similar to what will be needed by Australia, to deliver testing as a "Service" to meet customer requirements. Each test event provides actionable recommendations for hardening IT and weapon systems and improving operational tactics, techniques, and procedures. Key lessons learned from NCR Testing include:

- Start small and grow.

- Cybersecurity Testing is an important engineering and design tool.

- The Cyber Table Top is an effective tool to understand mission risks and prioritize testing.

- Focus Cybersecurity Testing on the mission.

- Cybersecurity Testing must be executed with key IT staff, incident responders, Network Defenders, and Cyber Protection Teams.

The processes in the U.S. DoD Cybersecurity T&E Guidebook are only intended for the DoD level. Much work has been done by the International Council of Systems Engineers (INCOSE) to produce an industry standard for security systems engineering, now published as NIST 800-160, that embodies cybersecurity and interleaves it with standard system engineering practices [39]. The recent work by Nejib *et al*. [39] to produce a relatively simple industry matrix of cybersecurity planning and activities against standard system engineering practices has further simplified the task for DoDs to set statements of work when contracting and for major Defence primes to inculcate and be readily compliant with U.S. DoD cybersecurity processes. This recent cybersecurity matrix framework and the NIST 800-160 standard are recommended for the Submarine Program.

V. Trusted Cyber Supply Chains and Anti-Tamper for Submarine

Cybersecurity craft in the U.S. has found that the most critical of Defense systems, like submarines, nuclear weapons and space surveillance, require to be 'trusted systems', meaning that their computer and software components, applications and architectures need to be designed, assembled, tested and refreshed using personnel, companies and procedures that are, and remain, highly-trusted suppliers [51]. Trust in this regard moves beyond a tick-box, IT, rule-based approach and introduces notions such as assurance and shared awareness, necessary to enable sûréte, more than commodified (often privatised) notions of security. This returns to Knowledge Sovereignty, in which Trust (as distinct from blind faith) may be:

> *A function of the Likelihood of a person or system being able to comprehend, explain, understand by logic (where understanding by logic can be described as Intelligibility, taken to be a function of comprehension: explainable and understandable by logic) and deal with a set of outcomes or events, or:*
>
> *Trust is a function of the Likelihood of a person or system being able to intelligibly deal with a set of outcomes or events.* [63]

In addition the DOD Program Protection Planning Guidance includes the requirement to plan for and implement Software Assurance, Anti-Tamper and manage Supply Chain Risks for critical components. Australia has a precious few chip, processor, board and software manufacturers for Defence Industry, all who should be key for our future submarine, including for the test sites.

The Australian DoD has outsourced most of its repair and maintenance to a cost-effective hub and spoke acquisition and sustainment model [20]. Unfortunately, this model provides an increase in the quantum attack surface of Defence materiel since

according to Ferguson '*the lower down the supply chain the sub-contractor is, the less it is directly affected by Defence's policy and processes.'* According to Alberts *et al*. [2], '*while supplier, vendor, and contracts relationships provide cost savings and flexibility to the DoD, they also come with risk.*' With cybersecurity, one-off assessments of suppliers of software-intensive componentry and applications is no longer adequate and the assurance cost will be in perpetuity of the componentry and application use, since the vulnerability against continuously emerging threats mean an assured system and supplier of today is vulnerable tomorrow. Some strong policies exist on people, processes and technology used on Australian DoD ICT networks, however software-intensive platforms and capabilities that are not ICT networks have no similar controls [5], [6]. All acquisitions need to have cyber planning resources available, especially something as developmental, forward-deployed and deterrent as the Submarine Program.

Earlier it was noted there was no public evidence yet of the necessary industry engagement to establish cyber-trusted supply chains, certainly for the imminent test sites. The Australian DoD may need to urgently, assuredly (on the bases of trust development) and systematically scrutinise cybersecurity protections resident in Naval Group and Lockheed Martin. This will involve providing DoD strategic cybersecurity requirements and acquisition strategy to address Anti-Tamper and supply-chain risk management options in the redesigns — all of which is also fundamental to enabling Knowledge Transfer and establishing Knowledge Sovereignty over the future submarine. Naval Group and Lockheed Martin are unlikely to be commercially motivated to adjust extant supply chains, or subject them to new scrutiny, in order to establish a robust and independent cybersecurity test framework for Australia. They should not therefore be given untested and unfettered technical deference to Australian Knowledge Sovereignty in this key future threat area before trusts are established.

VI. Recommendations

The following recommendations for the Australian Submarine Program derive from this research:

- Provision representative land-based test sites across all submarine systems to be established in Australia and under Australian DoD control as soon as possible if the design work is to be successfully exported in an enduring way and so as to enable Knowledge Sovereignty and timely and informed decisions on the program.
- Automate land-based test sites to create efficiencies in submarine development, deployment, and redeployment [57].
- Test sites should be used to significantly de-risk the Program by helping to build trusts, maintain public support, and enabling fully-representative technical and operational participation throughout the rolling development in safety, usability, sûréte, cybersecurity, reliability, maintainability and availability assessments.
- Test Sites will also improve overall cost schedule and performance and position Australia for long term sustainment.
- Apply the U.S. acquisition guidebooks for cybersecurity [52] as these protections are apropos to the U.S. DoD combat system being used and they represent best practice.
- Implement the list of cybersecurity planning tasks given earlier that are necessary to recover cybersecurity protections for the Submarine Program to the best practice [52].
- Include targeted Australian ICT industry in the cybersecurity acquisition strategy.
- Exploit Cybersecurity Testing and an Engineering and Design Tool to improve Cyber resilience. [57].
- Execute Cyber Table Top exercises as a tool to understand mission risks and prioritize testing [57].
- Use the recently developed industry cybersecurity matrix framework [39] and the NIST 800-160 standard for all the supply chain options as a fundamental requirement of integrating cybersecurity into the systems engineering.
- Link the new land-based test facilities and laboratories, wherever they are, to the U.S. T&E networks with appropriate training and assurances so as to enable distributed live, virtual and constructive experimentation and cybersecurity vulnerability assessments and penetration testing of every software-intensive system on the submarine to the latest U.S. DoD cybersecurity threat levels [30], [35].
- Linked/distributed test facilities will enable agile development and test, help Australia to reduce development, test, operations and sustainment costs and stay ahead of cyber adversaries [57].
- Independent review by cybersecurity and test professionals of all test concept strategies and plans.

VII. Conclusion

Australia's Future Submarine Project needs to progress sooner on two interrelated aspects or it will quickly risk fundamental design rework and associated capability limitations. First, the in-Australia footprint of the Submarine early work – namely design test sites, and second, the cyber-resilience of the critical systems – namely cybersecurity of the submarine design and development plans. The Submarine Project Director promised the first of these two aspects during last year's Submarine Institute Conference, while Minister Cristopher Pyne has given assurances about the latter when French submarine plans for another country may have been compromised. Australia's DoD committed at the 2016 conference to build the land-based test sites in 2018 and commission them in early 2019. A serious concern with any delays in test capability is that the French designer and builder, Naval Group, will soon hold technical sway over Knowledge Transfer and project direction. It may suit commercial purposes for such test sites to be deferred, so French sites pick up the slack. Such an outcome would seriously impair Knowledge Sovereignty, Knowledge Transfer and independent test capability in the difficulties of foreign release and likely lead to Australian deference so as to avoid political sensitivity.

The second concern for project progress is cybersecurity preparations. Cyber is becoming the cheap first-strike weapon of

choice by potential adversaries in a kind of merging of insurgency, terrorism, international crime and state-based influences. The merging of electronic warfare and cyber-warfare means that no platform, however unconnected or firewalled it may be, is immune to probing within its systems. The future submarine must not only survive and be credible in this Information Age, but actually ought to be a potential purveyor of offensive cyber if it is to be our contemporary deterrence. It therefore has to respond dynamically to a quantum attack surface as relevant to its past designs, current builds, and future operations. Cybersecurity craft in the U.S. has found that the most critical of Defence systems, like submarines, nuclear weapons and space surveillance, require to be 'trusted systems', meaning that their computer and software components, applications and architectures need to be designed, assembled, tested and refreshed using personnel, companies and procedures that are, and remain, highly-trusted suppliers. Moreover, recent work in the U.S. may enable trusted 'sidecar' cyber-threat adaptive embedded components to give greater cybersecurity assurance while retaining cost effective use of commercial computers and software.

Australia has a precious few chip, processor, board and software manufacturers for Defence Industry, all who should be key for our future submarine, including for the test sites. The future submarine's high-level requirements would undoubtedly have cyber-resilience as a key feature, but there is no evidence of this flowing through to the key cybersecurity plans like those usual at this stage in a U.S. project (i.e. Project Protection Plan). Nor is there evidence of the necessary industry engagement to establish a cyber-trusted supply chains in time for the test sites or to independently assure Naval Group's and Lockheed Martin's redesigns. Again, these Defence Primes are unlikely to be commercially motivated to adjust extant supply chains, or subject them to new scrutiny, in order to provide for Knowledge Transfer (and so Knowledge Sovereignty) and establish a robust and independent cybersecurity test framework for Australia. They should not therefore be given untested and unfettered technical deference in this key future threat area fundamental to defending Australia's sovereignty.

ACKNOWLEDGMENT

This research was greatly assisted by Mr Pete Christensen from the MITRE Corporation following his three-year assignment as the Director of the U.S. DoD National Cyber Range [57]. The research was also assisted by a number of students undertaking postgraduate coursework in cybersecurity, in particular Mr Kenan Erem, Mr Thomas Coughlin, Mr Christopher Leedham and Ms Anne Coull.

REFERENCES

---

[1] Adres, R. B., 2012. 'The emerging structure of strategic cyber offense, cyber defense, and cyber deterrence,' p. 92 chapter in Reveron, D.S. editor, 2012. Cyberspace and national security threats, opportunities, and power in a virtual world, Georgetown Uni Press, Washington, DC.

[2] Alberts, C.; Haller, J.; Wallen, C.; Woody, C., 2017. 'Assessing DoD System Acquisition Supply Chain Risk Management,' CrossTalk, 30(3), pp. 4-8.

[3] Austin, G. (2016). Australia rearmed! Future needs for cyber-enabled warfare. Discussion Paper No. 1 of the Australian Centre for Cyber Security at University of New South Wales, Canberra, released publically on 19 January 2016. Retrieved from https://www.unsw.adfa.edu.au/australiancentre-for-cyber-security/news/australia-rearmed

[4] Australian DoD, 2016. Defence White Paper 2016. p. 50 & pp. 81-82 www.defence.gov.au.

[5] Australian DoD, 2017a. Defence Procurement Policy Manual, available at http://www.defence.gov.au/casg/multimedia/DPPM_(4_May_2017-9-7937.pdf.

[6] Australian DoD, 2017b. Defence Security Manual, available at http://www.defence.gov.au/DSVS/resources/DSM/PUBLIC%20%DSM%20Part%201.0.pdf.

[7] Australian National Audit Office (ANAO), 2002. Audit Report No. 30: 2001–02 Test and Evaluation of Major Defence Equipment Acquisitions, Canberra, ANAO

[8] Australian National Audit Office, 2010. Report No. 37 2009-10: Lightweight Torpedo Replacement Project - Department of Defence. Canberra: ANAO.

[9] Australian National Audit Office, 2013. Report No. 26 2012-13: Remediation of Lightweight Torpedo Replacement Project. Canberra: ANAO.

[10] Australian National Audit Office, 2015. Report No. 9 2015–16: Test and Evaluation of Major Defence Equipment Acquisitions. Canberra: ANAO.

[11] Australian National Audit Office, 2016. Report No.48 2016–17, Performance Audit, Future Submarine—Competitive Evaluation Process. Canberra, ANAO.

[12] Australian Parliament, 2016. Joint Parliamentary Committee for Accounts and Audit (JCPAA) hearing with Defence and the Australian National Audit Office, accessed on 3 March 2016 at http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/Reports_Nos_52_3_an d_9 with video viewed at http://parlview.aph.gov.au/mediaPlayer.php?videoID=296010&operation_mode=parlview

[13] Australian Senate, (2012). Senate Inquiry into Defence Procurement., Chapter 12, Canberra: Australian Parliament House.

[14] Barrett, T., 2016. An expanded submarine fleet: Meeting the challenges, Chief of Navy Address to the 8th Biennial Conference of the Submarine Institute of Australia, 15 November, Shine Dome, Canberra

[15] Bradley, J. M.; Joiner, K. F.; Efatmaneshnik, M.; Keating, C. B., 2017. 'Evaluating Australia's most complex system-of-systems, the future submarine: A case for using new Complex Systems Governance,' proceedings 27th Annual INCOSE International Symposium (IS 2017), Adelaide, Australia, July 15-20.

[16] Brown, C., Christensen, P., McNeil, J., & Messerschmidt, L., 2015. 'Using the developmental evaluation framework to right size cyber T&E test data and infrastructure requirements.' ITEA Journal, 36, 26–34.

[17] Cofer, D., 2015. 'Taming the complexity beast,' ITEA Journal, 36, pp. 313-318.

[18] Demchak, C., 2012. 'Cybered conflict, cyber power, and security resilience as a strategy,' p. 120, chapter in Reveron, D. S. editor, 2012. Cyberspace and national security threats, opportunities, and power in a virtual world, Georgetown University Press, Washington, DC.

[19] Elele, J. N.; Hall, D. H.; Davis, M. E.; Turner, D.; Faird, A.; & Madry, J., 2016. 'M&S Requirements and VV&A Requirements: What's the Relationship?' ITEA Journal, 37, pp. 333-341.

[20] Ferguson, G., 2012. 'Product innovation success in the Australian defence industry – an exploratory study,' The University of Adelaide, available https://digital.library.adelaide.edu.au/dspace/bitstream/2440/79198/8/02whole.pdf.

[21] Fidler, D. P., 2012. 'Inter arma silent leges Redux? The Law of Armed Conflict and Cyber Conflict,' p.76, chapter in Reveron, D. S. editor, 2012. Cyberspace and national security threats, opportunities, and power in a virtual world, Georgetown University Press, Washington, DC.

[22] Fitsanakis, J., 2013, Chinese hackers stole blueprints of Australian spy agencies new HQ. Intelnews, 28 May, available https://intelnews.org/2013/05/28/01-1267/.

[23] Fowler, S.; Sweetman, C.; Ravindran, S.; Joiner, K. F.; & Sitnikova, E., 2017. 'Developing cyber-security policies that penetrate Australian defence acquisitions,' Australian Defence Force Journal, Issue 202, July.

[24] Geers, K.; Kindlund, D.; Moran, N.; Rachwald, R., 2017. World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks, Fireeye Corporation, available https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf.

[25] Grubb, B., 2013. 'Blueprints for new ASIO headquarters 'stolen',' The Sydney Morning Herald, May 28, available http://www.smh.com.au/it-pro/security-it/blueprints-for-new-asio-headquarters-stolen-20130527-2n7kz.html.

[26] Hardung, B.; Kozlow, T.; Kruger, A., 2004. 'Reuse of software in distributed embedded automotive systems.' Proceedings of the 4th ACM international conference on embedded software, ACM, pp. 203-210.

[27] Hashim, A., 2013, 'Warfare in New Domains: The Future of Asymmetric Operations and Information Warfare,' 15th Asia Pacific Programme for Senior Military Officers—The Future of War, RSIS Singapore, 5 August.

[28] Hecht, M. 2015. 'Verification of software intensive system reliability and availability through testing and modeling,' ITEA Journal, 36, pp. 304-312.

[29] Heinl, C.H., 2016. 'The Potential Military Impact of Emerging Technologies in the Asia-Pacific Region: A focus on cyber capabilities,' in Emerging Critical Technologies and Security in the Asia-Pacific, R.A. Bitzinger, Editor, Palgrave Macmillan: Hampshire, UK.

[30] Hudgins, G., 2017. 'Successful Distributed and Cyber Testing with TENA and JMETC,' U.S. DoD public briefing by the Test Resource Management Centre, available at http://www.dtic.mil/ndia/2017/test/BestPracticesHudgins.pdf

[31] Joiner, K. F. 2015. 'How New Test and Evaluation Policy is Being Used to De-risk Project Approvals through Preview T&E', ITEA Journal; 36, pp. 288-297

[32] Joiner, K., 2017. 'How Australia can catch up to U.S. cyber resilience by understanding that cyber survivability test and evaluation drives defense investment,' Information Security Journal: A Global Perspective, Vol. 26, Issue 2, 2017

[33] Joiner, K. F. & Atkinson, S.R., 2016. 'Australia's Future Submarine: Shaping Early Adaptive Designs through Test and Evaluation.' Australian Journal of Multi-Disciplinary Engineering, Engineers Australia, pp. 1-23, DOI: 10.1080/14488388.2016.1238025.

[34] Joiner, K., Sitnikova, E., and Tutty, M.G., 2016. 'Structuring defence cyber-survivability T&E to research best practice in cyber-resilient systems', paper presented at Systems Engineering Test and Evaluation Conference, Melbourne.

[35] Joiner, K. F. & Tutty, M. G., 2017 'A tale of two allied Defence Departments: New assurance initiatives for managing increasing system complexity, interconnectedness, and vulnerability' Australian Journal of Multi-Disciplinary Engineering, Engineers Australia, unpublished.

[36] Keany, F., 2016. 'French shipbuilder DCNS learned of submarine breach via the media, Pyne accuses Xenophon staffer of leak.' ABC News, 15th December, available http://www.abc.net.au/news/2016-12-15/submarine-french-company-unaware-of-breach-until-media-reports/8122548

[37] Murphy, T.; Leiby, L. D.; Glaeser, K.; & Freeman, L., 2015. 'How Scientific Test and Analysis Techniques Can Assist the Chief Developmental Tester,' ITEA Journal, 36, pp. 96-101.

[38] Mead, N.R; Woody C.C; "Cyber Security Engineering: A Practitional Approach for Systems and Software Assurance" , 2017 Pearson Education, ISBN-13:970-0-134-18980.

[39] Nejib, P.; Beyer, D.; & Yakabovicz, E., 2017. 'Systems Security Engineering: What Every System Engineer Needs to Know,' 27th Annual INCOSE International Symposium (IS 2017), Adelaide, Australia, July 15-20.

[40] Normann, B., 2015. 'Continuous system monitoring as a test tool for complex systems of systems,' ITEA Journal, 36, pp. 298-303.

[41] Pearce, R., 2016. 'Cyber deterrant: PM talks up Australia's offensive capabilities.' Computerworld, https://www.computerworld.com.au/article/598443.

[42] Pretschner, A.; Broy, M.; Kruger, I. H.; Stauner, T., 2007. 'Software engineering for automotive systems: A roadmap,' Future of Software Engineering, IEEE Computer Society, pp. 55-71.

[43] RAND Corporation, 2011. Learning from Experience, Volume IV – Lessons from Australia's Collins Class Submarine Program. Santa Monica, CA: RAND Corporation on Behalf of Australian Department of Defence. www.dtic.mil/dtic/tr/fulltext/u2/a552686.pdf.

[44] RAND Corporation, 2015. Perspective on 2015 DoD Cyber Strategy, September, available www.dtic.mil/get-tr-doc/pdf?AD=ADA621794.

[45] Reveron, D. S. editor, 2012. Cyberspace and national security threats, opportunities, and power in a virtual world, Georgetown University Press, Washington, DC.

[46] Sammut, G., 2016. 'The Future Submarine Program,' slide 11, Head of Future Submarine Program address to the 8th Biennial Conference of the Submarine Institute of Australia, 15 November, Shine Dome, Canberra

[47] Sheldon, J. B., 2012. 'Toward a theory of cyber power: Strategic purpose in peace and war,' chapter in Reveron, D. S. editor, p. 212, 2012. Cyberspace and national security threats, opportunities, and power in a virtual world, Georgetown University Press, Washington, DC.

[48] Stanford, J., 2017 (pending). Australia's Future Submarine: Reducing Costs and Risks, public policy report, Insight Economics Pty Ltd, September.

[49] Stewart, C., 2016. 'Our French submarine builder in massive leak scandal,' The Australian Newspaper, 29 August, available http://www.theaustralian.com.au/national-affairs/defence/our-french-submarine-builder-in-massive-leak-scandal/news-story/3fe0d25b7733873c44aaa0a4d42db39e.

[50] U.S. Defense Acquisition University (DAU), 2016. The Road Ahead for Defence Acquisition, available http://dau.dodlive.mil/2016/04/18/cybersecurity-the-road-ahead-for-defense-acquisition/.

[51] U.S. DoD Defense Science Board (DSB), 2016. Summer Study on Autonomy, June, pp.28-30, [viewed 24 Aug 2017] https://www.hsdl.org/?view&did=794641.

[52] U.S. DoD, 2015. Cybersecurity T&E Guidebook, Version 1.0, 1 July, available online in numerous locations.

[53] U.S. DoD, Directorate of Operational Test and Evaluation, 2016. Annual Report to Congress on DoD Programs, F35 Joint Strike Fighter, available at www.dote.osd.mil.

[54] U.S. DoD, Director of OT&E Memorandum, 2014. Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs, dated 1 August 2014

[55] Wickens, C. D.; J. Lee; Y. Liu; & S. D. Becker. 2014. An Introduction to Human Factors Engineering. 2nd Ed. New York: Pearson Prentice Hall.

[56] Zhu, L.; Staples, M.; & Nguyen, T., 2014. The need for software architecture evaluation in the acquisition of software-intensive systems. Fishermans Bend: Aerospace Division, Defence Science and Technology Organisation.

[57] Christensen, P., 2017. 'Cybersecurity Test and Evaluation: A Look Back, Some Lessons Learned, and a Look Forward!' ITEA Journal, Vol 38 #3, 221–228.

[58] Reay Atkinson, S., and J. J., Bogais. Socio-Ethics to Critical Thinking. in Royal Australian Navy Fleet Air Arm Tactical Forum 24 Aug. 2017. HMAS Albatross, Nowra, NSW: SARN.

[59] Reay Atkinson S., J.J., Bogais, & R. MacLeod, Future Submarine Systems and Cultural Awareness Systems Brief. CISS Think Piece., 2016. Dated 2 Sep 2016.

[60] Reay Atkinson, S., and J. J., Bogais. Quantum AI – Future Imperfect? in Data Centre Dynamics (DCD) Converged, 27 Jun. 2017. International Convention Centre, Sydney: SARN.

[61] Reay Atkinson, S., Cyber-: Envisaging New Frontiers of Possibility. UKDA Advanced Research & Assessmnent Group, 2009. Occasional Series, 03/09.

[62] Reay Atkinson, S., A., Vakarau Levula, N.H.M., Caldwell, R.T.,Wigand, L., Hossain, Signalling Decision Making and Taking in a Complex World,

in International Conference on Information Technology and Management Science (ICITMS 2014), 1-2 May. 2014, WIT Transactions on Engineering Sciences Hong Kong.

[63] Reay Atkinson, S., A.M., Maier, N.H.M., Caldwell, & P.J., Clarkson., Collaborative trust networks in engineering design adaptation, in International Conference of Engineering Design, ICED11. 2011: Technical University of Denmark, Lyngby.

BIOGRAPHY

Dr Keith Joiner, CSC, [Group Captain (Ret'd), PhD, MSc (Aerosystems), MMgmt, BEng(Aero), MIEAust, CPEng, MAIPM, CPPD] joined the Air Force in 1985 and became an aeronautical engineer, project manager and teacher over a 30-year career before joining the University of New South Wales in 2015 as a senior lecturer in test and evaluation. From 2010 to 2014 he was the Director-General of Test and Evaluation for the Australian Defence Force, where he was awarded a Conspicuous Service Cross.

Associate Professor Simon Reay Atkinson [Captain RANR, PhD, MPhil, Eur Ing, CPEng, FIET] is an Australian (RAN Captain and associate professor at the University of Sydney, RN Ret'd), He served on the staffs of Generals Eric K. Shinseki and David Petraeus and was twice mentioned in despatches: Bosnia (1996–1997) and Sierra-Leone (2000). A weapons system engineer, he has an MPhil in International Relations (majoring in Law and Economics) and a PhD in Engineering Design Adaptation (in Complex Adaptive Systems), from St Catherine's College, Cambridge.

Dr Elena Sitnikova [PhD, BE (Hons), CSSLP] is a researcher and academic within the Australian Centre for Cyber Security (ACCS) at the University of NSW at ADFA. Her main research interests are in critical infrastructure protection and cyber security, software and systems engineering, quality assurance and enterprise process capability improvement. Elena currently leads the critical infrastructure area, carrying out research projects in cyber security in Industrial Internet of Things (IIoT) and Intrusion Detection Systems (IDS) for SCADA and industrial control systems.