Scientific Research Publishing

World Journal of Engineering and Technology, 2018, 6, 696-712
http://www.scirp.org/journal/wjet
ISSN Online: 2331-4249
ISSN Print: 2331-4222

Cybersecurity for Allied Future Submarines

Keith F. Joiner[1], Simon Reay Atkinson[2], Pete Christensen[3], Elena Sitnikova[4]

[1]Systems Capability Centre, University of New South Wales Canberra at Australian Defence Force Academy, Canberra, Australia
[2]Centre for International Security Studies and Sydney Cyber Security Network, University of Sydney, Sydney, Australia
[3]The MITRE Corporation, McLean, VA, US
[4]Australian Centre for Cyber Security Canberra, University of New South Wales Canberra at Australian Defence Force Academy, Canberra, Australia
Email: k.joiner@adfa.edu.au, simon.atkinson@sydney.edu.au, pchris@mitre.org, e.sitnikova@adfa.edu.au

How to cite this paper: Joiner, K.F., Atkinson, S.R., Christensen, P. and Sitnikova, E. (2018) Cybersecurity for Allied Future Submarines. *World Journal of Engineering and Technology*, **6**, 696-712.
https://doi.org/10.4236/wjet.2018.64045

Received: August 3, 2018
Accepted: September 11, 2018
Published: September 14, 2018

Abstract

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 not even submarines, however unconnected or firewalled they may be, are immune. The quantum attack surface of submarines is as much in their past, as they are in their designs today and their operations tomorrow: they must survive to be credible and ideally they should even be a contemporary offensive cyber deterrent. Such critical defensive systems require robust security systems engineering and cybersecurity test and evaluation to build and sustain their cyber-resilience. This paper uses Australia's future submarine program [1][1] to outline key facets needed in a submarine program to achieve cyber resilience, including how to adapt U.S. Department of Defense (DoD) best practices to engineer, test and sustain cyber-resilient submarine systems. Strategies are needed that provision sovereign-owned and operated land-based test sites to design, build, demonstrate and sustain critical submarine systems. This work is most relevant to countries allied to the U.S. and importing submarine capabilities, such as within lesser European powers and also in the Indo-Pacific where both cyber warfare and submarines are proliferating.

Keywords

Cyber-Resilience, Future Submarine Design, Land-Based Test Sites, Quantum Attack Surface, Test and Evaluation

[1]The examination of the cybersecurity challenges and processes for the Australian Future Submarine Program was presented to the Submarine Institute of Australia's annual conferences in 2017 [1] and the Institute has kindly agreed for these aspects to be used herein for broader implications.

1. Introduction

The Australian National Audit Office [2] gives an overview of Australia's future submarine program and the decision to select the French Naval Group and Lockheed Martin as the designers of Australia's new Short-Fin Barracuda class. Furthermore, Stanford in [3] covers the economic, technical, strategic and other risks of this program and the choices made thus far, in a comprehensive and somewhat contrary public policy report and exposition. From a technical risk perspective, Joiner and Reay Atkinson [4] summarised significant lessons learnt from the Collins Submarine Program concerning inadequate test and evaluation and insufficient land-based testing capability (*i.e.* in [5] [6]). A concern of both of these reviews is the emerging risk of the Australian Submarine Program in not yet conducting preview test and evaluation of reference design classes to disclose technical and operational risks prior to design down-select and contract. This paper will use this risk context to illustrate the particular threat of cyber warfare to future submarines generally and early in their design, and then how best to leverage U.S. DoD cybersecurity test and evaluation processes for such an allied submarine design against these new threats.

Cybersecurity concerns were first raised publically in Australia about releases of the French-Indian submarine, after which Australia's Minister Pyne gave assurances about the cybersecurity to be applied to French-Australian submarine planning [7] [8]. Such cybersecurity risks and mitigation and contingency planning for Australia's future submarine program have not yet been outlined. The increasing threat of cyber-enabled warfare for Australia has been reviewed extensively by Austin [9], following instances of cyber espionage; including the Australian Secret Intelligence Organisation building [10] [11]; and increasing instances of cyber-attack [12]. This paper is not definitional; however cyber-attack is broadly used to include all the elements of an attack life-cycle as shown in **Figure 1**.

The Australian Government has focused its DoD on meeting the new threat [14]; however, according to Joiner [15] much more could be done practically to leverage U.S. DoD initiatives in cybersecurity T&E. Proposals by Joiner, Sitnikova and Tutty [16] on how to engineer cyber-resilient systems in the Australian DoD has been followed more recently by an extensive exposition by Joiner and Tutty [17] 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 future submarines. In particular, recent research

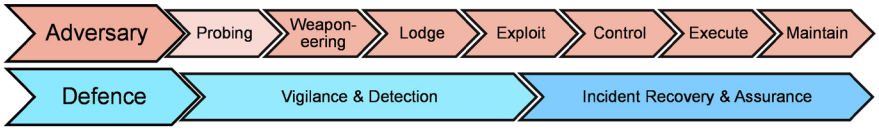

Figure 1. Illustration of attack life-cycle (adapted from [13]).

into how to create "*trusted*" supply chains for software-intensive systems will be overviewed [18] [19] [20] and compared with public efforts thus far by the Australian Submarine Program to shape sovereign industry involvement.

2. Sovereign Testing

Sovereign Testing essentially introduces the broader concept of 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 [21].

Critically Sovereign Testing connects with Knowledge Transfer as part of Knowledge Sovereignty; as distinct from, but clearly connected with, Sovereign Intellectual Property 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… 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* [22].

Knowledge Transfer is essentially a quantum phenomenon; connecting past, present and future with the indivisible "*knowledge that is both socio and info-technological*" [23]. In this respect, programs need to consider the impact of cyber as synthesising and combining both socio and info-technological systems and being:

A technologically bounded, largely immeasurable, strongly scientific, stochastic control space, 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* [24].

In 2016 the Australian Chief of Navy and his 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 [25] [26]. Moreover, Vice Admiral Tim Barrett [25] 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 Australian Submarine Program has been covered [4] [27]. For example, the

broad aim of the Submarine Program used by Bradley *et al*. [27] to illustrate a complex systems governance model for the Australian Program is similar to Barrett's [25] 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 for Australia in about 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 cybersecurity lessons learned in the U.S. [28] need not be relearned by Australia. Early, strategic investment in security systems engineering and cybersecurity test and evaluation improve program cost, schedule and performance. Conversely, failure to make those investments has adverse programmatic and mission impacts.

The proposed land-based test sites align the Australian submarine program with best practice (*i.e.* [4] [17] [28] [29] [30] [31]), Australian DoD test policy [32] [33] and the lessons learned from the Collins Program [5] [6]. A risk with any delays in test capability is that the foreign designers and builders may 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 foreign sites retain knowledge sovereignty. Such an outcome risks seriously impairing a sovereign testing capability and would almost certainly 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 a previous foreign project in 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 [34] [35].

Independence in test and evaluation is crucial in factual results being equally available and unfettered to investors, technical authorities and operational managers. Unfettered sovereign test results have been shown in Australian Parliamentary evidence and audit reports to have been essential in hindsight [36], both as part of Defence market testing and acceptance into initial service. 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 these tasks to the contractor in the first place [5] [29] [33].

If the French Naval Group undertake significant portions of Australia's submarine systems virtual, constructive and live simulation testing in France, significant Knowledge Transfer issues will make the flow of test results much

harder. Similarly, if Lockheed Martin undertake the simulation testing of their submarine systems in the U.S., there are risks to test results making it unfettered to the stakeholders, especially if they were to use proprietary simulation models that have not been accredited by the U.S. and/or Australian DoD(s). Constraints on travel budgets hampered representation of operators and technical experts on Australia's Landing Helicopter Dock ship during safety and usability assessments and that program only involved travel within Australia [33] [36], much less than would be the case for Cherbourg, France and Rhode Island, U.S. Cybersecurity assessments for cooperative vulnerability and penetration testing further challenge outsourcing of such work without close cooperation between the DoD and contractors [30] [37]. Work by Fowler *et al*. [38] 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 [17] 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.

For Australia's Submarine Program, 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, enable knowledge sovereignty and provide for timely and informed decision making and taking [39]. Such test sites should significantly de-risk any such submarine program by helping to maintain public support, and enabling fully representative technical and operational participation throughout the rolling complex software-intensive systems development especially for safety, usability [40], 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, mostly as a reactive process, rather than for 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, thus making risk trade-offs throughout project's acquisition lifecycles, minimizing the number of systems vulnerabilities, and reducing time for land-based tests. Moreover, early investment in representative land-based sites can be 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 [28], 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. Sovereign-controlled land-based test sites will have additional workforce and National Security benefits. Land-based test infrastructure should provide fertile ground to grow and enhance local cybersecurity workforce. From

a National Security perspective, this infrastructure would enable countries to adopt agile, iterative and incremental acquisition and testing approaches that ultimately enhance their sovereign ability to keep pace with adversaries in cyberspace.

Despite these lessons learned, land-based test sites like those in Australia are likely to face enormous pressure to be scaled back, as they did on the Collins Class Submarine 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 any submarine program, on the actual submarines to resolve operational and technical issues in-build and in-the-water rather than beforehand, and to become truly sovereign capabilities.

In developing land-based test sites to enable live, virtual and constructive distributed simulations [17], it is crucial that the simulations are accredited for intended use, as is required in the U.S. DoD [41]. 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 that into life as detailed by Hecht [42], Normann [43], and Cofer [44].

3. 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 [45]. 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 [15] [20]. A 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 [12], 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, creating an instability in the synthetic ecology which interferes with the human psyche; creating further instability and uncertainty [23]. Sovereign Testing of the entire quantum attack surface is therefore fundamental to Knowledge Transfer and cybersecurity, without which countries like Australia would not have Knowledge Sovereignty over their future submarine.

Cyber-power is relatively cheap, available and largely anonymous, such that it is as attractive for peacetime as it is for war [46], especially for deterrence by smaller powers in the Asia-Pacific region [45]. These attributes also make cyber-power attractive to non-state actors [14] [47] such as cyber criminals, ter-

rorists, hackers, and proxy actors engaged or supported by numerous foreign governments ([45], p. 126), ([48], p. 5). Heinl [45] forecasts that within a few years most states in the Asia-Pacific will develop some form of offensive cyber program, most of whom are also pursuing submarine capabilities for deterrence [49]. Few Indo-Pacific countries pursuing these two Defence capabilities are likely to have examined the risk of cyber warfare to their new submarine capabilities because it is a delicate and futuristic balance of defensive and offensive new technologies [49].

While Australia often relies on deterrence by alliances, kinetic military power like that referred to by Hashim [50] can be unusable in cyber warfare because attribution is slow and difficult [51] [52] [53], cyber-effects are hard to contain, and the adversaries may be globally dispersed [54]. For Australia's major military platforms like the future submarine, which are intended to operate throughout the Asia-Pacific region, they are likely to be a cyber-warfare target starting from the first supply of software-intensive componentry for the test sites. The quantum attack surface for such submarine programs are likely to be defined throughout their 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 [19]. The increased use of commercial hardware and software to perform essential functions for mission-critical systems is likely to have increased the vulnerability of countries like Australia 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 [17] [55] [56], vulnerabilities are even more-likely to be discovered at some stage. Weapons Systems which use commercial hardware and software are extensively interconnected with other platforms [18], 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 identifiable from the U.S. DoD:

- improved security systems engineering and cybersecurity test and evaluation, so as to design and build in cyber-resiliency [15] [16] [28] [30];
- trusted cyber supply chains, as covered in the next section of this paper [18] [20]; and
- trusted cyber-security modules or other resident cyber-threat adaptive sub-systems [20] [38].

Trusted cyber-threat adaptive modules have been the subject of recent review by the U.S. DoD's Defense Science Board [20], 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 ar-

chitecture. 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*".

4. Cybersecurity Acquisition and Test Planning for Submarines

The U.S. DoD's revised acquisition policy with cybersecurity integrated was issued in January 2015 and is comprehensive [30] [31]. The policy is underpinned by a clear and helpful Cybersecurity T&E Guide [57] that is readily available on-line. According to Joiner and Tutty [17], 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 [30] [57]. The types of tasks necessary to recover cybersecurity planning for the Australian submarine program were illustrated at [1] and they are necessary precursors to cybersecurity verification planning and to all land-based test sites and design costings. Any disaggregation of LBTS will compromise the cybersecurity testing of full attack surfaces, especially for simulation of mixed-maturity architectures using modern live, virtual and constructive simulation (LVC) [17]. For example, **Figure 2** illustrates the disaggregation risk of LBTS for the Australian submarine program across countries, arriving at different times, and to differing supply chain standards [1]. 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 Australian submarine warrants the same protections it would in the U.S. DoD.

The U.S. DoD has been implementing this approach for cybersecurity test and evaluation for some time. There are many lessons learned based upon cybersecurity testing accomplished at the National Cyber Range (NCR) [28]. The NCR provisions representative cybersecurity test infrastructure, similar to what

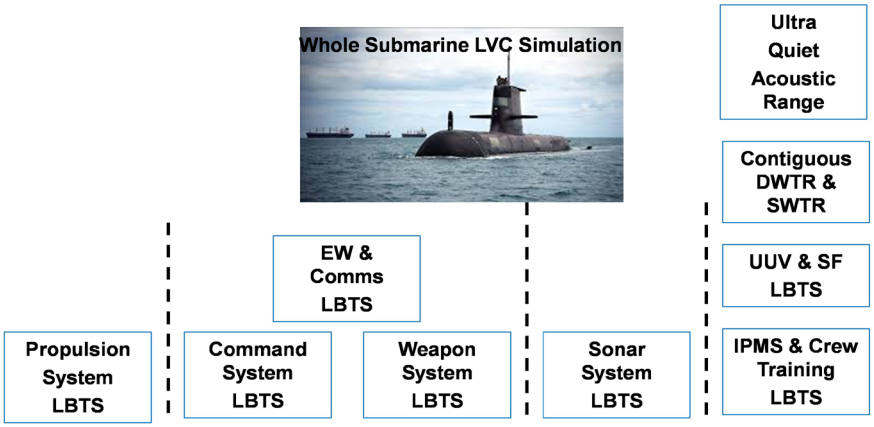

Figure 2. Illustration of risk of disaggregating test sites in time (left to right) and location (*i.e.* U.S., Australia & France) as applied to Australian program (adapted from [1])[2].

should be needed by Australia, to deliver testing as a "*service*" to meet customer requirements. Each test event provides actionable recommendations for hardening information technology and weapon systems and improving operational tactics, techniques, and procedures. Key lessons learned from NCR testing include [28]:

- Start small and grow.
- Cybersecurity testing is an important engineering and design tool.
- The "*cyber tabletop exercise*" is an effective tool to understand mission risks and prioritize testing.
- Focus cybersecurity testing on the mission.
- Cybersecurity testing must be executed with key information technology staff, incident responders, network defenders, and cyber-protection teams.

The processes in the U.S. DoD Cybersecurity T&E Guidebook [56] 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 [58]. This standard embodies cybersecurity and interleaves it with standard system engineering practices [59]. The recent work by Nejib *et al.* [59] 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 any submarine program [58] [59].

5. Trusted Cyber Supply Chains and Anti-Tamper for Submarines

Cybersecurity craft in the U.S. has found that the most critical of Defense sys-

[2]Figure acronyms: Electronic Warfare (EW), Unmanned Underwater Vehicle (UUV), Integrated Platform Management System (IPMS), Special Forces (SF), Deep-Water Tracking Range (DWTR), Shallow-Water Tracking Range (SWTR), Live Virtual & Constructive (LVC).

tems, 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 [20]. Trust in this regard moves beyond a tick-box, information technology, 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 [60].

In addition the U.S. 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 their Defence Industry, all who should be key for their 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 [61]. Unfortunately, this model provides an increase in the quantum attack surface of Defence materiel, since according to Ferguson [61] "*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*. [18], "*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 information technology networks, however, software-intensive platforms and capabilities that are not information technology networks have no similar controls [62] [63]. All acquisitions need to have cyber planning resources available, such as experts in cyber vulnerability assessments and penetration testing, with the necessary test infrastructure to do threat-representative evaluations through virtual, constructive and then live systems design and simulation. The need for such expertise and test infrastructure is more important for something as developmentally-complex as a future submarine re-design, especially when such submarines will deploy into international waters where they are highly likely to be exposed to cyber threats aimed at cheaply limiting their deterrent value.

Earlier it was noted there was no public evidence yet of the necessary industry engagement in Australia to establish cyber-trusted supply chains, certainly for the imminent submarine test sites. The Australian DoD may need to urgently, assuredly (on the bases of trust development) and systematically scrutinise cybersecurity protections resident in its foreign designers and builders. This would 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. Foreign contractors 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 countries like Australia. They should not therefore be given untested and unfettered technical deference to Knowledge Sovereignty in this key future threat area before trusts are established.

An example of a basic cybersecurity risk management framework [57] to be applied to a submarine development program is shown in **Figure 3**.

6. Recommendations

Based on the case study of the Australian Submarine Program and the U.S. DoD best practice, any submarine program allied to the U.S. should consider:

- Provisioning representative land-based test sites across all submarine systems, that are to be established sovereignly as soon as possible so as to successfully export design work in an enduring way and so as to enable Knowledge Sovereignty and timely and informed decisions on the program.
- Automating land-based test sites to create efficiencies in submarine development, deployment, and redeployment.

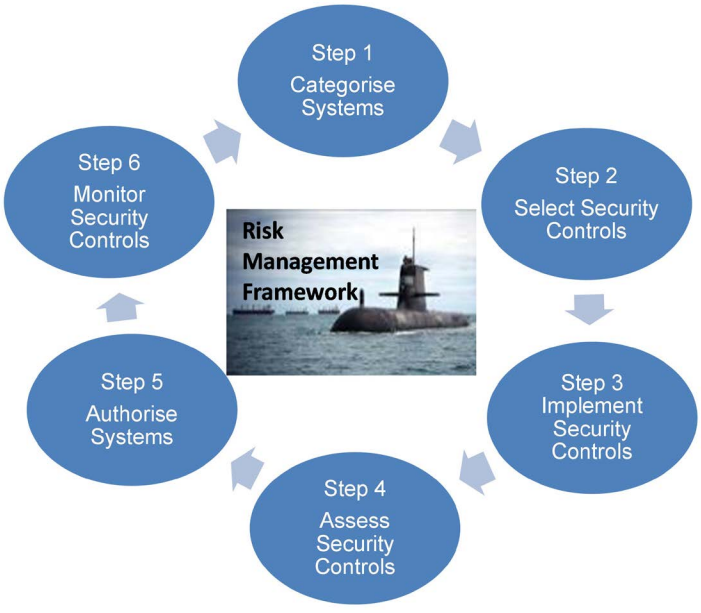

Figure 3. Example cybersecurity risk management framework from [57].

- Using test sites to significantly de-risk the submarine program by helping to build trust, 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.
- Using test sites to also improve overall cost schedule and performance and position the ally for long term sustainment.
- Applying the U.S. acquisition guidebooks for cybersecurity, as these protections are apropos to any U.S. DoD systems being used and they represent best practice.
- Including targeted sovereign information technology industry in the cybersecurity acquisition strategy.
- Exploiting cybersecurity testing as a continuous engineering design tool to improve and retain cyber resilience.
- Executing "*cybertable top exercises*" as a tool to understand mission risks and prioritize testing.
- Using the recently developed industry cybersecurity matrix framework and the NIST 800-160 standard for all the supply chain options as a fundamental requirement of integrating cybersecurity into the systems engineering.
- Linking new land-based test facilities and laboratories, wherever they are, to the U.S. test and evaluation networks or their equivalents, 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 cybersecurity threat levels.
- Using linked and distributed test facilities to enable agile development and test, so the ally can reduce development, test, operations and sustainment costs and stay ahead of cyber adversaries.
- Undertake *Quantum Network Mapping* (the subject of ongoing research by Author's one and two) of each submarine's unique cyber-attack surface.
- Obtaining independent review by cybersecurity and test professionals of all test concept strategies and plans.

7. Conclusions

Australia's Future Submarine Project illustrates the modern challenge of advancing a significant new complex deterrent while being resilient to new cyber warfare threats, and doing so without risking fundamental design rework and associated capability limitations. Key to any submarine development are the necessary land-based test sites and using them to attain and maintain cyber-resilience of the critical systems. A serious concern with any delays in such test capability is that the foreign designer and builder can hold technical sway over Knowledge Transfer and project direction. It may suit commercial purposes for such test sites to be deferred, so foreign sites pick up the slack. Such an out-

come would seriously impair Knowledge Sovereignty, Knowledge Transfer and independent test capability in the difficulties of foreign release.

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 not even submarines, however unconnected or firewalled they may be, are immune to probing of, and interference with, their systems. Future submarines 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. To do so, submarine systems have to respond dynamically to a quantum attack surface for 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.

Some countries like Australia have precious few chip, processor, board and software manufacturers for Defence Industry, all of whom should be key for sovereign resilience of a submarine program, including its test sites. The high-level requirements of submarines need to have cyber-resilience as a key feature and then flow these through to the key cybersecurity plans like those usual in a U.S. project (*i.e.* Project Protection Plan). There needs to be sovereign industry engagement to establish cyber-trusted supply chains in time for the test sites and sovereign oversight of the cybersecurity of any foreign designers and builders, or otherwise these prime contractors will not 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 to establish a robust, perennial and independent cybersecurity test framework. Foreign contractors should not be given untested and unfettered technical deference in this key future threat area or ultimately expensive new deterrent submarines risk being vulnerable to relative low-cost cyber warfare threats.

Acknowledgements

The examination of the cybersecurity challenges and processes for the Australian Submarine Program was presented initially to the Australian Submarine Institute's annual conferences in 2017 [1] and the Institute has kindly agreed for these aspects to be used herein for broader implications. This research was greatly 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.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Joiner, K.F., Atkinson, S.R. and Sitnikova, E. (2017) Cybersecurity Challenges and Processes for Australia's Future Submarine. *Proceedings of the* 4*th Submarine Science, Technology and Engineering Conference*, Adelaide, 13-16 November 2017, 166-174.

[2] ANAO (2016) Performance Audit, Future Submarine—Competitive Evaluation Process. Report No. 48: 2016-17, Australian National Audit Office, Canberra.

[3] Stanford, J. (2017) Australia's Future Submarine Getting This Key Capability Right. In: Stanford, J., Ed., *Public Policy Report to Submarines for Australia*, Public Policy Report, Insight Economics Pty. Ltd., Canberra.

[4] Joiner, K.F. and Atkinson, S.R. (2016) Australia's Future Submarine: Shaping Early Adaptive Designs through Test and Evaluation. *Australian Journal of Multi-Disciplinary Engineering*, **12**, 3-26. https://doi.org/10.1080/14488388.2016.1238025

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

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

[7] Stewart, C. (2016) Our French Submarine Builder in Massive Leak Scandal. *The Australian Newspaper*. http://www.theaustralian.com.au/national-affairs/defence/our-french-submarine-builder-in-massive-leak-scandal/news-story/3fe0d25b7733873c44aaa0a4d42db39e

[8] Keany, F. (2016) French Shipbuilder DCNS Learned of Submarine Breach via the Media: Pyne Accuses Xenophon Staffer of Leak. ABC News. http://www.abc.net.au/news/2016-12-15/submarine-french-company-unaware-of-breach-until-media-reports/8122548

[9] 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. https://www.unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/DISCUSSION%20PAPER%20AUSTRALIA%20REARMED.pdf

[10] Fitsanakis, J. (2013) Chinese Hackers "Stole Blueprints" of Australian Spy Agencies New HQ. IntelNews. https://intelnews.org/2013/05/28/01-1267/

[11] Grubb, B. (2013) Blueprints for New ASIO Headquarters "Stolen". *The Sydney Morning Herald*. http://www.smh.com.au/it-pro/security-it/blueprints-for-new-asio-headquarters-stolen-20130527-2n7kz.html

[12] Pearce, R. (2016) Cyber Deterrant: PM Talks up Australia's Offensive Capabilities. Computerworld. https://www.computerworld.com.au/article/598443

[13] Heinbockel, W.J., Laderman, E.R. and Serrao, G.J. (2017) Supply Chain Attacks and Resiliency Mitigations: Guidance for System Security Engineers. Mitre Technical Report MTR170477. https://www.mitre.org/sites/default/files/publications/pr-18-0854-supply-chain-cyb

er-resiliency-mitigations.pdf

[14] Australian DoD (2016) Defence White Paper 2016. 50, 81-82. http://www.defence.gov.au/

[15] 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*, **26**, 74-84.

[16] Joiner, K., Sitnikova, E. and Tutty, M.G. (2016) Structuring Defence Cyber-Survivability T&E to Research Best Practice in Cyber-Resilient Systems. *Systems Engineering Test and Evaluation Conference*, Melbourne, 50-63.

[17] Joiner, K.F. and Tutty, M.G. (2018) A Tale of Two Allied Defence Departments: New Assurance Initiatives for Managing Increasing System Complexity, Interconnectedness, and Vulnerability. *Australian Journal of Multi-Disciplinary Engineering*.

[18] Alberts, C., Haller, J., Wallen, C. and Woody, C. (2017) Assessing DoD System Acquisition Supply Chain Risk Management. *CrossTalk*, **30**, 4-8.

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

[20] U.S. DoD Defense Science Board (DSB) (2016) Summer Study on Autonomy. 28-30. https://autonomousweapons.org/department-of-defense-science-board-summer-study-on-autonomy/

[21] Reay Atkinson, S. and Bogais, J.J. (2017) Socio-Ethics to Critical Thinking. Royal Australian Navy Fleet Air Arm Tactical Forum 24 Aug., HMAS Albatross, Nowra.

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

[23] Reay Atkinson, S. and Bogais, J.J. (2017) Quantum AI—Future Imperfect? Data Centre Dynamics (DCD) Converged, International Convention Centre, Sydney.

[24] Reay Atkinson, S. (2009) Cyber: Envisaging New Frontiers of Possibility. UKDA Advanced Research and Assessment Group, Occasional Series, 03/09.

[25] Barrett, T. (2016) An Expanded Submarine Fleet: Meeting the Challenges. *Presentation to 8th Biennial Conference of the Submarine Institute of Australia*, Canberra, 15 November 2016.

[26] Sammut, G. (2016) The Future Submarine Program. *Presentation to 8th Biennial Conference of the Submarine Institute of Australia*, Canberra, 15 November 2016.

[27] Bradley, J.M., Joiner, K.F., Efatmaneshnik, M. and 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*, Adelaide, 15-20 July 2017, 187-199. https://doi.org/10.1002/j.2334-5837.2017.00353.x

[28] Christensen, P. (2017) Cybersecurity Test and Evaluation: A Look Back, Some Lessons Learned, and a Look Forward! *ITEA Journal*, **38**, 221-228.

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

[30] Brown, C., Christensen, P., McNeil, J. and Messerschmidt, L. (2015) Using the Developmental Evaluation Framework to Right Size Cyber TandE Test Data and Infrastructure Requirements. *ITEA Journal*, **36**, 26-34.

[31] Mead, N.R. and Woody, C.C. (2017) Cyber Security Engineering: A Practitional Approach for Systems and Software Assurance. Pearson Education, London.

[32] Joiner, K.F. (2015) How New Test and Evaluation Policy Is Being Used to De-Risk Project Approvals through Preview TandE. *ITEA Journal*, **36**, 288-297.

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

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

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

[36] Australian Parliament (2016) Joint Parliamentary Committee for Accounts and Audit (JCPAA) Hearing with Defence and the Australian National Audit Office. http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/Reports_Nos_52_3_and_9 http://parlview.aph.gov.au/mediaPlayer.php?videoID=296010andoperation_mode=parlview

[37] Zhu, L., Staples, M. and Nguyen, T. (2014) The Need for Software Architecture Evaluation in the Acquisition of Software-Intensive Systems. Aerospace Division, Defence Science and Technology Organisation, Fishermans Bend.

[38] Fowler, S., Sweetman, C., Ravindran, S., Joiner, K.F. and Sitnikova, E. (2017) Developing Cyber-Security Policies That Penetrate Australian Defence Acquisitions. *Australian Defence Force Journal*, No. 202, 17-26.

[39] Reay Atkinson, S., Levula, A.V., Caldwell, N.H.M., Wigand, R.T. and Hossain, L. (2014) Signalling Decision Making and Taking in a Complex World. *International Conference on Information Technology and Management Science*, Hong Kong, 1-2 May 2014.

[40] Wickens, C.D., Lee, J., Liu, Y. and Becker, S.D. (2014) An Introduction to Human Factors Engineering. 2nd Edition, Pearson Prentice Hall, New York.

[41] Elele, J.N., Hall, D.H., Davis, M.E., Turner, D., Faird, A. and Madry, J. (2016) MandS Requirements and VVandA Requirements: What's the Relationship? *ITEA Journal*, **37**, 333-341.

[42] Hecht, M. (2015) Verification of Software Intensive System Reliability and Availability through Testing and Modeling. *ITEA Journal*, **36**, 304-312.

[43] Normann, B. (2015) Continuous System Monitoring as a Test Tool for Complex Systems of Systems. *ITEA Journal*, **36**, 298-303.

[44] Cofer, D. (2015) Taming the Complexity Beast. *ITEA Journal*, **36**, 313-318.

[45] Heinl, C.H. (2016) The Potential Military Impact of Emerging Technologies in the Asia-Pacific Region: A Focus on Cyber Capabilities. In: Bitzinger, R.A., Ed., *Emerging Critical Technologies and Security in the Asia-Pacific*, Palgrave Macmillan, Hampshire, 123-137. https://doi.org/10.1057/9781137461285_10

[46] Sheldon, J.B. (2012) Toward a Theory of Cyber Power: Strategic Purpose in Peace and War. In: Reveron, D.S., Ed., *Cyberspace and National Security Threats, Opportunities, and Power in a Virtual World*, Georgetown University Press, Washington DC, 212.

[47] Reveron, D.S. (2012) Cyberspace and National Security Threats, Opportunities, and Power in a Virtual World. Georgetown University Press, Washington DC.

[48] RAND Corporation (2015) Perspective on 2015 DoD Cyber Strategy.

http://www.dtic.mil/get-tr-doc/pdf?AD=ADA621794

[49] Bitzinger, R.A. (2016) Emerging Critical Technologies and Security in the Asia Pacific. Pallgrave Macmillan, Hampshire, 37-62 and 91-106.

[50] 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.

[51] Adres, R.B. (2012) The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence. In: Reveron, D.S., Ed., *Cyberspace and National Security Threats*, *Opportunities*, *and Power in a Virtual World*, Georgetown University Press, Washington DC, 92.

[52] Fidler, D.P. (2012) Inter Arma Silent Leges Redux? The Law of Armed Conflict and Cyber Conflict. In: Reveron, D.S., Ed., *Cyberspace and National Security Threats*, *Opportunities*, *and Power in a Virtual World*, Georgetown University Press, Washington DC, 76.

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

[54] Demchak, C. (2012) Cybered Conflict, Cyber Power, and Security Resilience as a Strategy. In: Reveron, D.S., Ed., *Cyberspace and National Security Threats*, *Opportunities*, *and Power in a Virtual World*, Georgetown University Press, Washington DC, 120.

[55] Hardung, B., Kozlow, T. and Kruger, A. (2004) Reuse of Software in Distributed Embedded Automotive Systems. *Proceedings of the* 4*th ACM International Conference on Embedded Software*, Pisa, 27-29 September 2004, 203-210. https://doi.org/10.1145/1017753.1017787

[56] Pretschner, A., Broy, M., Kruger, I.H. and Stauner, T. (2007) Software Engineering for Automotive Systems: A Roadmap. *Future of Software Engineering*, Minneapolis, 23-25 May 2007, 55-71.

[57] U.S. DoD (2015) Cybersecurity TandE Guidebook. Version 1.0.

[58] Ross, R., McEvilley, M. and Oren, J.C. (2016) NIST Special Publication 800-160, Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. U.S. Department of Commerce. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

[59] Nejib, P., Beyer, D. and Yakabovicz, E. (2017) Systems Security Engineering: What Every System Engineer Needs to Know. 27*th Annual INCOSE International Symposium*, Adelaide, 15-20 July 2017, 434-445.

[60] Reay Atkinson, S., Maier, A.M., Caldwell, N.H.M. and Clarkson, P.J. (2011) Collaborative Trust Networks in Engineering Design Adaptation. *International Conference of Engineering Design*, Denmark, 15-19 August 2011, 152-161.

[61] Ferguson, G. (2012) Product Innovation Success in the Australian Defence Industry—An Exploratory Study. The University of Adelaide, Adelaide. https://digital.library.adelaide.edu.au/dspace/bitstream/2440/79198/8/02whole.pdf

[62] Australian DoD (2017) Defence Procurement Policy Manual. http://www.defence.gov.au/casg/DoingBusiness/ProcurementDefence/ContractingWithDefence/PoliciesGuidelinesTemplates/ProcurementPolicy/dppm.aspx

[63] Australian DoD (2017) Defence Information Security Manual. https://acsc.gov.au/infosec/ism/