UNSW CANBERRA

ACCS Discussion Paper #2

Integrating Cyber-Survivability into ADF Platform Development

Keith F. Joiner

January 2016

Integrating Cyber-Survivability into ADF Platform Development

Keith F. Joiner

ACCS DISCUSSION PAPER NO. 2

January 2016

Author Note

Group Captain (ret.) Dr. Keith Joiner CSC joined the Air Force in 1985 and became an aeronautical engineer, project manager and teacher before joining the University of New South Wales Canberra 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. Dr Joiner has an MSc in Aerospace Systems Engineering with Loughborough University in the United Kingdom, a PhD in Calculus Education with Curtin University, and a Masters of Management from University of Canberra. In previous roles he was a design engineer for aircraft and missiles, a project engineering manager, a chief engineer for several aircraft types, and an air base commander. In 2009 he did wartime service in Baghdad for the Multi-National Force Iraq, where he was awarded a U.S. Meritorious Service Medal for his work developing drawdown plans. He is a Certified Practising Engineer and a Certified Practising Project Director.

ACCS Discussion Paper Series

The ACCS Discussion Paper Series is a vehicle to subject the research of scholars affiliated with the Centre to further review and debate prior to the finalisation of research findings in more formal scholarly outlets, such as journals or books. The goals of ACCS are outlined on the back cover of this publication.

More information on ACCS is available at our website:
https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/.

ABSTRACT

The cyber challenge faced by the Australian Defence Force (ADF) is not simply one of preventing information compromise (classic cyber security) in peacetime, but includes preventing its systems and platforms from being crippled or subverted by the offensive cyber operations of an enemy in combat. In principle, all new ADF weapons platforms should have specifications and capabilities that can address both needs. Since 2009, the U.S. armed forces have had clear policies to ensure that the threat posed by cyber warfare is integrated into the development, acquisition, and fielding of all of its platforms that use information or software systems. As a result, U.S. forces attach a high piroity to designing cyber-resilient systems. Unlike its U.S. counterpart, the ADF has not formally required its new defence systems to be tested against cyber-threats as a standard practice in its operational testing and evaluation (T&E) that takes place in the acceptance phase for new major platforms. Consequently, the ADF would appear to be missing a vital step in addressing the potential vulnerabilities of its major platforms to cyber-attack. This paper argues that Australian test agencies urgently need an updated T&E policy and additional funding to enable the ADF to conduct cyber-survivability trials, and that we look for economies in this through enhanced cooperation with the U.S. armed forces.

Contents

The Rising Threat of Cyber Warfare

Cyber warfare has been a growing threat for well over a decade (Christensen 2013). A staggering amount of mobile malware is estimated to be in circulation: more than five million lines of code, growing by around two million lines per year (Borror, 2015). According to the U.S. Department of Defense (DoD):

> The cyber threat has become as real a threat to U.S. military forces as the missile, artillery, aviation and electronic warfare … Any data exchange, however brief, provides an opportunity for a determined and skilled cyber threat to monitor, interrupt, or damage information and combat systems. Real-world cyber adversaries regularly demonstrate their ability to compromise systems and inflict damage. (U.S. DoD 2014a)

For example in 2014 the U.S. Directorate of Operational Testing and Evaluation conducted sixteen major cyber-security evaluations and found "significant vulnerabilities on nearly every acquisition program." Recent risks have also occurred in industrial hacking and citizen hacking, making cyber-security important also to industry and to information technology providers (Troester and Christensen 2015).

Cyber-security is defined in a seminal U.S. Presidential Directive as:

> The prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication. This includes information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (U.S. DoD 2014b)

Testing and evaluating systems for their cyber-security is a new field. Christensen (2013) defines this as examining security measures to reduce the number of points of entry into a system (the "cyber-attack surface") and to reduce an attacker's ability to monitor, interrupt, damage, or shut down a system's operations (the "kill chain effects"). In short, cyber-security testing and evaluation (T&E) examines a system's resilience to cyber-attacks. A 2015 international cyber-security T&E workshop noted that current cyber warfare and cyber-security T&E focuses on defensive perimeters. According to Rice and Russell (2015), "firewalls, email filters, and intrusion detection/prevention systems are all designed to defend a perimeter." However, they conclude that this approach is insufficient: "Whether defending a host's or a network's perimeter, [this approach is] clinging to [the idea of a] Maginot line as cyber strategy", which is to say that it is defending against outdated threats rather than preparing for future attacks. They note that defence planners realise that adversaries will exploit cyber-attack surfaces to penetrate and operate within a system. Such penetrations need to be identified, in addition to denying access to less capable threats. For this reason, Rice and Russell advocate complementing a perimeters approach with a signatures approach in which "anti-virus and blacklists search for known signatures and block known malicious IP addresses and URLs." However, they argue that even this is not enough because the "modern threat [is] more akin to [an] insurgency than [a] regular army. How do you stop an enemy whose TTPs (e.g. tool signatures) constantly change, or one that blends in with the civilian population (e.g. using legit[imate] credentials)?"

For this reason, the term "cyber-security" may be substituted sometimes with a term

such as "cyber-survivability," particularly when evaluating developed systems where the cyber-resilience of the design is for some period unlikely to change and the purpose of the evaluation work is to determine operational risk. This focus on mission-assurance and cyber-survivability as an important aspect of cyber warfare is consistent with several RAND Corporation recommendations to the U.S. Air Force (Snyder et al. 2015).

Information about the vulnerability and survivability of defence systems to cyber-attack is usually classified and so not widely appreciated, even within senior military circles. However, a useful constructivist approach used by Christensen (2013 and 2015a) to highlight the threat is to exhibit the vulnerability of a contemporary, non-military system, such as a motor vehicle. The most cited such example comes from researchers at the Universities of Washington and California, San Diego. They analysed and tested the cyber-resilience of a modern automobile (Koscher et al. 2010). They found that because modern automobiles "are pervasively monitored and controlled by dozens of digital computers coordinated via internal vehicular networks [an] attacker who is able to infiltrate virtually any electronic control unit (ECU) can leverage this ability to completely circumvent a broad array of safety-critical systems." Researchers demonstrated that they were able to "completely ignore driver input—including disabling the brakes, selectively braking individual wheels on demand, stopping the engine, and so on." They were able to do this by bypassing "rudimentary network security protections within the car, such as maliciously bridging the car's two internal subnets." Their research included "an attack that embeds malicious code in a car's telematics unit … that will completely erase any evidence of its presence after a crash."

This research has provided an open-source example of the vulnerability of older software systems that were designed with neither in-built security nor a regard for cyber warfare, such as might be found on the databus of military aircraft, vehicles, or ships in operation today. Such systems assume that all other systems on the databus are necessary and intended (i.e. legitimate) users of the system: as a result, they provide highly accommodating access with little or no monitoring of activities or usage. If electromagnetic probing (i.e. electronic warfare) is combined with a cyber-attack, older "legacy" military systems can be interrogated and manipulated until a cyber-kill process such as an information demand overload is devised. The attack method can then be stored for later use without necessarily being disclosed or leaving a residual signature.

The Australian Defence Force (ADF) needs to give the same attention to testing and evaluating the vulnerability to cyber-attacks of its legacy systems as it affords to testing and evaluating vulnerabilities to conventional threats such as electronic warfare, and to asymmetric threats such as improvised explosive devices. In addition, cyber-security T&E has an important role to play in officers' understanding of the operational deficiencies of their systems against cyber-attacks, and therefore in how they would employ these systems against which adversaries, how they can improve current systems, and in how they establish cyber-resilience requirements for new systems. Military officers best understand, report, and adapt to any threat when it is part of a structured operational T&E or military exercise. As such, cyber-survivability T&E needs to be part of everyday operational T&E.

Research is also needed into the current level of knowledge of ADF officers and officials and their ability to deal with cyber warfare. It is especially important to know whether officers believe fallacies about cyber warfare, such as:

- Cyber warfare only occurs when computers or information systems network
- Stand-alone systems with signal processing are not vulnerable to cyber-attack
- The most likely motive of cyber-attack is to steal information for public embarrassment of the military.

U.S. Defense Forces' Response

The process of responding to cyber-threats in the U.S. defence forces has broadly occurred in three phases, where current practice is moving from the second to the third phase:

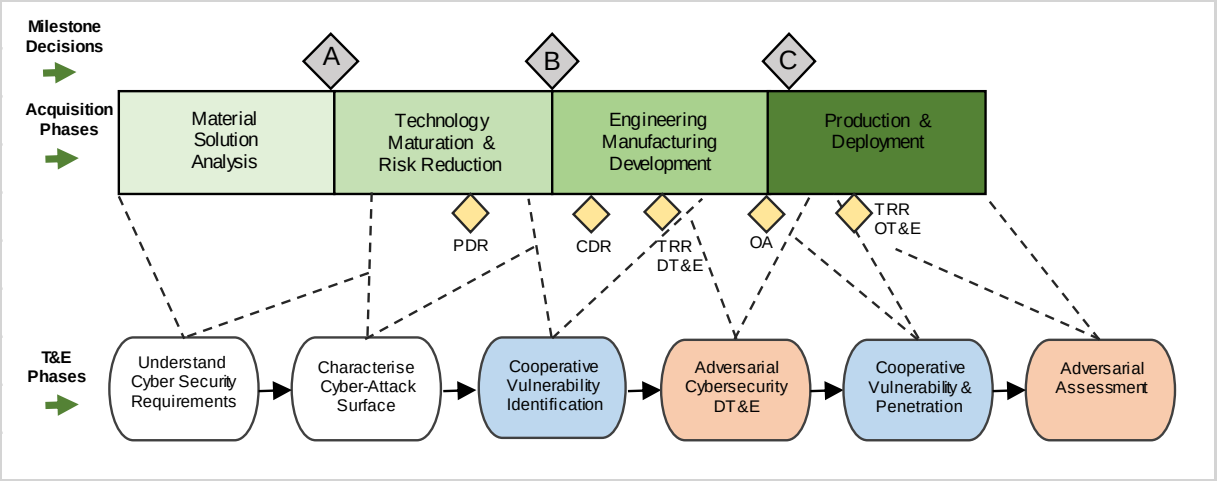
Initial Operational Testing and Evaluation Characterisation of Risks: Following the exposure of several significant cyber threats to U.S. defence forces (U.S. DoD 2014b), the United States developed the necessary infrastructure and funding to conduct extensive cyber-security T&E to assess the cyber warfare vulnerability of newly fielded or updated systems during all operational T&E. This phase did much to raise awareness of the risks to such systems across all environmental domains (i.e. land, maritime etc.) and capabilities (i.e. submarines, artillery, etc.) without obligating any acquisition programme to implement changes. This phase highlighted the obvious difficulties in improving cyber-resilience after a system had been designed, and required independent funding and schedule relief because the programmes had not been scoped for the additional cyber-threat.

Shift-Left Programme for Earlier Resilience: U.S. defence acquisition leaders developed a programme to include cyber-resilience in system design earlier in the process. This "shift-left" asks acquisition programmes to assess vulnerabilities early enough to influence system designs. The shift-left initiative sought to raise the cyber-resiliency requirements and testing in legacy programmes wherever possible (Brown et al. 2015).

Comprehensive Coverage Through the Life Cycle in an Updated Acquisition Manual: The most recent update to the *U.S. Defense Acquisition Manual* has embedded cyber-security requirements, design, and testing throughout the capability life cycle, similar to other comparable threats and associated disciplines. While there are still awareness issues, all environmental domains now have technical advisers in their test agencies and cyber-security T&E is no longer considered special or unachievable (U.S. DoD 2015a; U.S. DoD 2014a; U.S. DoD 2014c).

U.S. Defense developed a thorough six-step programme (Figure 1) for implementing cyber-security T&E as part of their systems acquisition process (Christensen, 2015b). This has recently been characterised at a policy level as broad developmental and then operational T&E phases (U.S. DoD 2014a) that align with U.S. laws on T&E. Nevertheless, the six steps remain clear within the latest cyber-security T&E guidance (Brown et al. 2015; Christensen 2015b). The steps have been colour-coded: white for the predominately early information assurance work, blue for cooperative vulnerability evaluations, and red for adversarial evaluations, as explained in Table 1. Note, however, that experts in all three of these areas usually work across all steps; the colour coding only characterises the dominant team in each step. Also, white, blue, and red testing always occurs in that order as systems are first tested for compliance, and then for vulnerability, before being exposed to a representative threat (i.e. attacked). Note that Steps 3 and 4 are developmental T&E activities and Steps 5 and 6 are operational T&E activities. Ideally Step 5 occurs before the operational assessment that informs the U.S. approval to contract for production (Milestone C) (U.S. DoD 2015b).

FIGURE 1: CYBER-SECURITY T&E STEPS AND PHASES IN U.S. DEFENCE FORCES



Key:

DT&E: Developmental testing and evaluation
OT&E: Operational testing and evaluation
PDR: Preliminary design review
CDR: Critical design review
OA: Operational assessment
TRR: Test readiness review.
U.S. defence milestones shown are approximately:
(A) Approval-to-solicit
(B) Approval to contract for engineering and manufacture development (EMD)
(C) Approval to contract for production and often in-service support.
Source: Adapted from Christensen, 2015b; Brown et al. 2015.

TABLE 1: CHARACTERISTICS OF WHITE, BLUE AND RED TEAM CYBER-SECURITY T&E

Security Controls Assessor (White Team)	**Vulnerability Assessments (Blue Team)**	**Adversarial Cyber-security T&E (Red Team)**
• Assess compliance to Information Assurance controls • Execute Security Assessment Plan (SAP) • Enables certification and accreditation of system • Based on Security Technical Implementation Guides • Can be hands-on testing, interviewing key personal, or examination of artefacts	• Comprehensive • Identifies any known vulnerabilities present in systems using generic threat actors like injection attacks, spear phishing, and web attacks • Reveals systemic weaknesses in security program • Focuses on adequacy and implementation of technical security controls and attributes like port scans, denial of service attacks, and cracking passwords	• Graduation exercise • Usually employing NSA-certified teams • Informed by intelligence but also employs worst-case scenarios • Exploits one or more known or suspected weaknesses • Focuses attention on specific problems or attack vectors • Represents both internal and external threats • Develops an understanding of the inherent weaknesses of a technology

• Includes a review of operational and management security controls • Conducted with full knowledge and assistance of systems administrators, owner, and developer • No harm to systems.	• Full knowledge and cooperation of systems administrators • Hands-on testing, interviewing key personal, and examination of relevant artefacts • No harm to systems • Feedback to developers and system administrators for system remediation and mitigation.	• Models actions of a defined internal or external hostile entity • Conducted covertly with minimal staff knowledge • Requires representative defence teams to conduct intended monitoring and recovery actions where applicable • May harm systems and components and require clean up.

Source: Adapted from Christensen 2013 and 2015a; Brown et al. 2015.

Limits in Australian Defence Progress

Cyber-security is largely not mentioned in Australia's recently updated defence policies for capability development and T&E (DoD 2015). This absence reflects the larger gaps in Australian defence policy which have been documented in international cyber-maturity comparisons, albeit with a note of optimism and an overall assessment of 7 out of 10:

> Australia's score remains unchanged from 2014. Australia also still lacks a publicly available strategy or policy document that guides the department's and the ADF's approach to cyber threats. The Defence Minister has indicated publicly that the upcoming Defence White Paper will look to address Defence's future cyber capability and the role it has to play in contributing to the protection of Australia and its critical systems. (Feakin et al. 2015: 20)

Such optimism in international comparisons probably exists because the ADF is conducting research into cyber-security threats, has deployed developmental T&E in the field, and has created an early coordination office for cyber warfare, all of which means that the ADF has experts who are articulate in the field. However, having a few experts, if they are not supported by policy and systematic implementation, simply risks masking what could be a shallow and not-well-understood threat or response. According to reports like the Senate Inquiry into Defence Procurement (Australian Senate 2012) and Australian National Audit Office reviews (ANAO 2002 and 2011), the ADF's capability-acquisition processes are slow, unwieldy, and largely driven by the policies and requirements envisaged at the time they were first conceived. That is, today's defence acquisitions, some 180 projects, are driven by requirements that were typically drafted a decade earlier, when cyber-security awareness was not prevalent. In the absence of any systematic policy and associated additional funding, the chance that a new capability will undergo cyber-survivability T&E will be left to individuals involved with the projects, who themselves would need to be aware of the new threat, competent to plan appropriate T&E related to the threat, and able to secure funding and the necessary specialist infrastructure to conduct the T&E. In other words, the prospect of making any meaningful progress against the cyber-security threat is very remote, except perhaps in the case of capabilities developed and acquired from the United States. However, even in cases where Australia purchases U.S. military off-the-shelf systems that have been subjected to cyber-survivability T&E, there is a risk that the Australian operating environment will

expose a different cyber-attack surface, and that Australia, due to a lack of policy and additional funding, will not conduct the necessary follow-on cyber-security T&E to ensure that the systems are not compromised.

Furthermore, today's new defence capabilities are undergoing revolutionary changes in their networking, digitisation, and interoperability, all of which means the cyber-attack surfaces of each new system are to some degree dependent on other systems, some of them new and some legacy. Tutty (2015) has characterised military joint forces as a family of systems (FOS)—"family" reflecting the generational mix of equipment, doctrine, training, and competency, as well as the unpredictable nature of warfare and the high degree of human input and decision-making—that are inherently complex and adaptive. For this reason, Tutty proposes developing new, structured T&E frameworks for the FOS to make it more effective and resilient overall. The FOS's cyber-survivability depends to some extent on the resilience of its weakest link and the coordination of its collective defence when under attack. Developing cyber-security T&E for such coordinated multi-systems requires policy and funding. Without these, there is a risk that pursuing increased networking and digitisation simply makes Australia's systems more vulnerable.

Options for Cyber-Survivability Testing and Evaluation

The ADF's current T&E process is shown in relation to its capability development life cycles in Figure 2 (Australian DoD 2015). This capability process, like that in the United States, seeks at every phase of the life cycle to remove operational deficiencies; however, unlike in the United States, Australia has not insisted that testing of representative cyber-threats be included in its operational T&E as a standard practice. Therefore, the ADF may be blind to the operational vulnerabilities of its major systems and platforms to a cyber-attack. Consider also that Australian defence systems are at various phases in the life cycle illustrated in Figure 2. Some capabilities are in-service with relatively fixed designs, others are about to be fielded, and others are in the early concept, planning, tendering, and development stages. As such, these systems have different cyber-characteristics and cyber-vulnerabilities, as well as different evolutionary potential to improve their cyber-resilience.

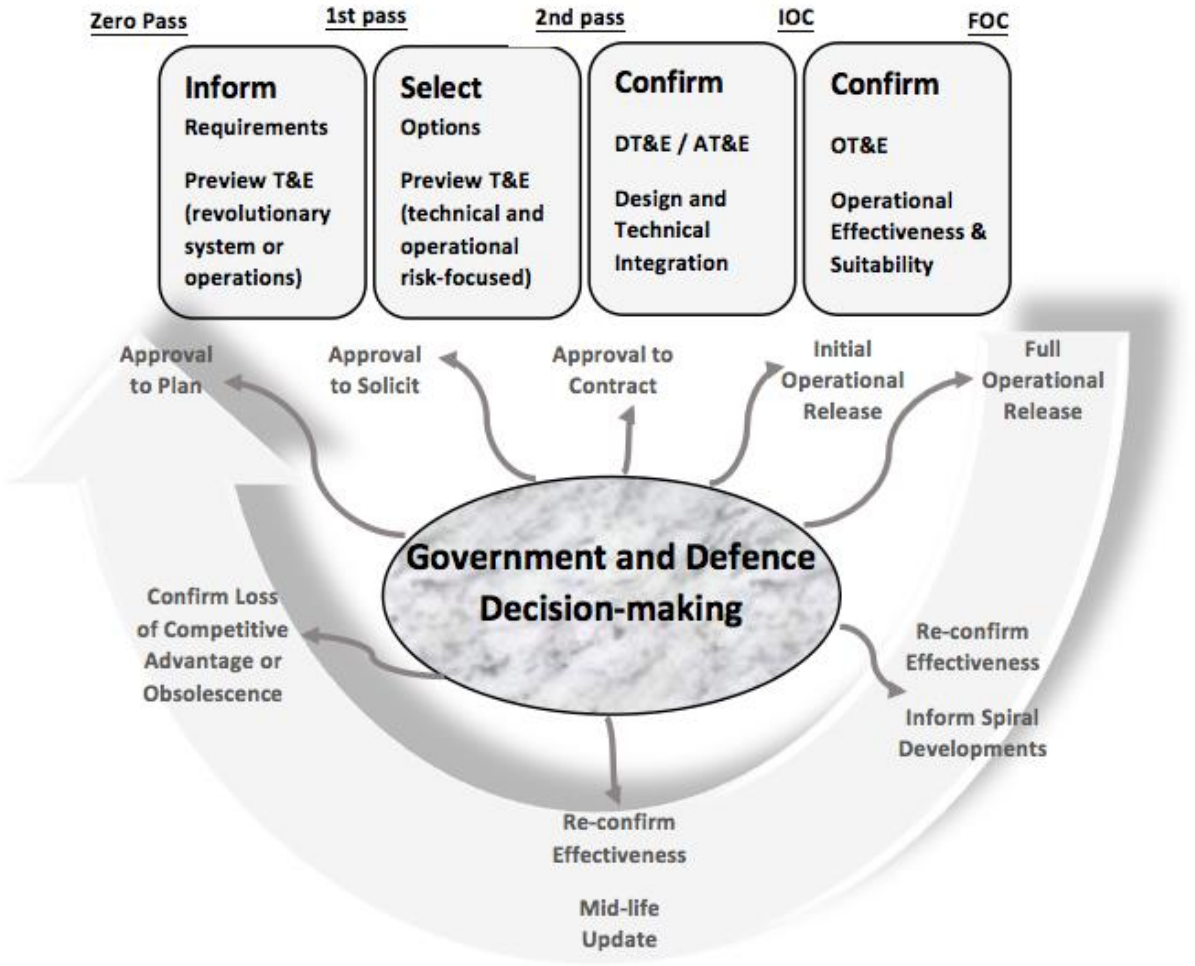
To address this lack of T&E, there are, broadly speaking, three approaches available: test only new systems (the "implementation date" approach); test all systems ("one-off cost now"); or test only new systems, but include any legacy systems that connect with the new system in the tests ("hybrid").

Implementation Date: Mandate that all systems put into the field after a certain date must meet new cyber-security requirements and be subjected to cyber-survivability T&E. This puts at risk all systems that were fielded before that specified date, and therefore puts at risk the overall collective defence of families-of-systems to cyber-threats.

One-off Cost Now: Require all systems to be assessed for cyber-survivability, irrespective of where they are in the life cycle, and provide whatever resources are necessary to mitigate their vulnerabilities. This puts at risk the cost, schedule, and capability benefits of all projects currently in development while new baselines are set. This approach could also be prohibitively expensive.

Hybrid: Set a future date for new systems to incorporate cyber-resilience in their design; in the interim, conduct cyber-survivability T&E only on newly fielded systems as part of their operational T&E, including their interfaces with legacy systems. This option leverages planned operational T&E by including T&E of the new threat. Sharing the results will help increase commanders' understanding of their systems' operational vulnerabilities to cyber-attack, which will in turn highlight the need to increase the cyber-resilience of new systems.

Figure 2: Illustration of Use of T&E in Defence Life Cycle



Key:
AT&E: Acceptance testing and evaluation
DT&E: Developmental testing and evaluation
OT&E: Operational testing and evaluation
IOC: Initial operational capability
FOC: Final operational capability

Source: Adapted from Australia DoD (2015)

The hybrid option is similar to the first "Initial Operational Testing and Evaluation Characterisation of Risks" phase approach taken by U.S. defence forces outlined above. It ensures that the operational vulnerabilities of new systems are understood. It is also fundamental in identifying the requirements and highlighting the urgency of future improvements without imposing the prohibitively expensive retrofits or unacceptable production delays that are inherent in the other options. Overall, the hybrid option is

essentially the only option available to Australia because Australia does not yet have the expertise or the infrastructure to undertake wholesale cyber-security T&E. This expertise and infrastructure has to be grown.

Several agreements between Australia and the United States regarding assistance in T&E could be leveraged to kick-start Australia's operational cyber-survivability T&E (Australian DoD 2015: part 3, ch. 8; Duma 2013). It is difficult to subject large, complex defence platforms such as warships, fighter aircraft, and the like to representative operational cyber-threats because some systems and some threats can only be safely evaluated in controlled cyber ranges and other threat-effects can only be safely emulated in large, complex platforms (Borror 2015; Christensen 2015a; Ross 2015; Troester and Christensen 2015; Arwine 2015). The skill necessary to perform multi-system[1] cyber-survivability testing has been refined by U.S. operational test agencies and this expertise is potentially available to Australia if Australia pays for it under the provisions of the agreement concerning reciprocal use of test facilities. Such U.S. support would kick-start the development of equivalent Australian T&E organisations to eventually match in rigour, if not in scale, U.S. cyber-survivability T&E.

Implementing the hybrid option would be relatively simple if Australia were to adopt the U.S. cyber-security T&E policy (U.S. DoD 2014a) as an interim policy that includes any necessary Australian exclusions and clarifications. Under such an arrangement, Australia would require U.S. assistance to design and develop cyber-survivability trials as part of its operational T&E of newly fielded systems because Australian defence T&E agencies are unlikely to have the expertise necessary even to plan such events. Under the agreements with the United States, to begin Australia need only recognise that it needs assistance, ask for that help, and be prepared to fund the U.S. defence experts to plan the early trials so that they can be budgeted. Such trials would need to occur in all environmental domains (land, maritime, aerospace, etc.) because there are independent sponsors, acquisition divisions, and T&E organisations for each domain, each of which needs to build awareness and competence comparable to their U.S. defense equivalents.

Australia's Hobart-class air warfare destroyers (AWD) provide one example of a defence capability that should undergo cooperative cyber-survivability testing as part of its impending operational T&E. The AWDs incorporate U.S.-designed systems in a Spanish ship design that was built based on Australian requirements established in 2004. These ships are likely to undergo combat ship qualification trials on a U.S. maritime range around 2018–19. These trials will be similar to those used to test the U.S. Arleigh Burke class of ships. The T&E requirements for the AWDs are likely to include kinetic effects such as supersonic missiles, and non-kinetic effects for electronic warfare, but are unlikely to include cyber warfare. The cyber warfare threat could be included in a cooperative trial between Australia and the United States in such a way that it would fundamentally improve the ability of the Royal Australian Navy's T&E agency to conduct such cyber-survivability T&E on other classes like the future submarine and frigate. However, this is unlikely to happen because the AWD project is already late and heavily over-budget. To include contemporary cyber warfare threats in the project's operational T&E would require additional funding.

---

[1] In systems engineering, the term "multi-systems" is often referred to with far greater precision as "systems of systems" and even "families of systems" (Tutty 2015).

Conclusion

The cyber-threat faced by the ADF concerns not only information security, but includes the cyber kill chain tactic of denying systems and platforms. Techniques to probe legacy systems for vulnerabilities and record a system kill can be used without detection, as most software-intensive systems that are not ordinarily networked are not monitored and are vulnerable to combining electromagnetic probing with cyber techniques. Successful penetration of unmonitored legacy systems need not be revealed or implemented immediately; instead, it can be stored for later use. Since 2009, the U.S. response to the cyber-threat has been to inculcate this threat into its mainstream development, acquisition, and fielding of all platforms and systems that use information or software systems, especially into its operational T&E. Such T&E involves adversarial attacks that try to penetrate and effect a cyber kill procedure. As a result, U.S. defence forces have reached an earlier understanding of the operational risk posed by cyber warfare to current systems, and therefore of the necessity of designing more cyber-resilient systems. The Australian defence capability-acquisition process, like that in the United States, seeks at every phase of the life cycle to remove operational deficiencies; however, unlike the United States, Australia has not required the testing of cyber-threats as a standard practice in its current T&E, at least not publically. Consequently, the ADF is likely to be blind to the operational vulnerabilities of their major complex systems and platforms to cyber-attack, and are also unlikely to be sufficiently informed to set capability research and development priorities in this field. Several agreements related to T&E assistance exist between Australia and the United States that could be leveraged to kick-start Australia's T&E in cyber-survivability. Particularly important for Australia is the critical knowledge of how to conduct cyber-survivability T&E on major platforms. In this field, Australia is probably about six years behind the United States. Australian test agencies critically need an updated T&E policy and extra funding to enable selected cyber-survivability trials to occur cooperatively with the United States.

References

Arnwine, M. 2015. “Distributed Testing for Cyber Security.” Presentation to International Test and Evaluation Association (ITEA) Cybersecurity Workshop: Test and Evaluation to Meet the Advanced Persistent Threat, Belcamp MD, 24–26 February 2015.

Australia. Department of Defence (DoD). 2015. *Defence Capability Development Manual*, Part 3, Test and Evaluation, and Part 2, Chapter 7, “T&E Planning in Capability Development.” Accessed http://www.defence.gov.au/... 23 March 2015.

Australia. Australian National Audit Office. 2002. “Report No. 30 2001-02: Test and Evaluation of Major Defence Equipment Acquisitions.” Canberra: ANAO.

Australia. Australian National Audit Office. 2011. “Report No. 57 2010-11: Acceptance into Service of Navy Capability.” Canberra: ANAO.

Australia. The Senate. 2012. Senate Inquiry into Defence Procurement. Canberra: Australian Parliament House.

Australian Institute of Project Management. 2015. “Certification of PMOs.” Accessed http://www.aipm.com.au/certification/pmo-award on 27 October 2015.

Borror, S. 2015. “Cyber-Vulnerability Flight Test.” Presentation to ITEA Cybersecurity Workshop: Test and Evaluation to Meet the Advanced Persistent Threat, Belcamp MD, 24–26 February 2015.

Brown, C., P. Christensen, J. McNeil, and L. Messerschmidt. 2015. “Using the Developmental Evaluation Framework to Right Size Cyber T&E Test Data and Infrastructure Requirements.” *The ITEA Journal* 36 (1): 26–34.

Christensen, P. 2013. “Proposed Cybersecurity T&E Process.” Track 3 presentation to the ITEA International Conference, Washington DC, November 2013.

Christensen, P. 2015a. “Introduction to Cyberspace T&E.” Tutorial presentation at ITEA International Conference, Washington DC, August 2015.

Christensen, P. 2015b. “There is Life Inside the Beltway and Progress on Cyber Security Test and Evaluation.” *The ITEA Journal* 36 (3): 184–189.Duma, D. 2013. “Guest Editorial: Multinational Test and Evaluation of the Future.” *The ITEA Journal* 34 (4): 312–314.

Feakin, T., J. Woodall, and L. Nevill. 2015. *Cyber Maturity In The Asia–Pacific Region 2015*. Canberra: Australian Strategic Policy Institute. Accessed www.aspi.org.au on 28 October 2015.

Koscher, K., A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. 2010. “Experimental Security Analysis of a Modern Automobile.” 2010 Institute of Electrical and Electronics Engineers Symposium on Security and Privacy, Oakland, CA, 16–19 May 2010. Available at http://www.autosec.org/pubs/cars-oakland2010.pdf.

Rice, R. L. and E. R. Russell. 2015. “Cyber Threat Portrayal in Test and Evaluation.” Presentation to ITEA Cybersecurity Workshop: Test and Evaluation to Meet the Advanced Persistent Threat, Belcamp MD, 24–26 February 2015.

Ross, J. 2015. “The Perfect Storm – Cyber RDT&E.” Presentation to ITEA Cybersecurity Workshop: Test and Evaluation to Meet the Advanced Persistent Threat, Belcamp MD, 24–26 February 2015.

Snyder, D., J. D. Powers, E. Bodine-Baron, B. Fox, L. Kendrick, and M. H. Powell. 2015.). *Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles.* RAND Corporation Research Report No. 1007. Santa Monica, California: RAND Corporation. Available at http://www.rand.org/pubs/research_reports/RR1007.html.

Troester, D. and P. Christensen. 2015. "National Cyber Range Overview." Presentation to ITEA Cybersecurity Workshop: Test and Evaluation to Meet the Advanced Persistent Threat, Belcamp MD, 24–26 February 2015.

Tutty, M. 2015. "The Profession of Arms in the Information Age." PhD thesis, University of South Australia.

United States. Department of Defense (DoD). 2014a. "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs." Director of OT&E Memorandum dated 1 August 2014.

_____ 2014b. National Security Presidential Directive-54/Homeland Security Presidential Directive-23 of 8 January 2008 (CLASSIFIED) as cited in U.S. Department of Defense Instruction No. 8500.01 Cybersecurity dated 14 March 2014. Available at http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf.

_____ 2014c. "Effective Integration of Cyber and Traditional Security Efforts." Joint Memorandum of Chief Information Officer and Under Secretary of Defense for Intelligence, dated 31 March 2014. Available at http://www.cdse.edu/documents/toolkits-cybersecurity/usd_strat_cio_cyber_traditional_FE_security.pdf.

_____ 2015a. "Operations of the Defense Acquisition System." U.S. Department of Defense Instruction No. 5000.02 dated 7 January 2015.

_____ 2015b. United States Code, Title 10 Armed Forces, Subtitle A – General Military Law, Part IV – Service, Supply, and Procurement, Chapter 141 – Miscellaneous Procurement Provisions, Section 2399 – Operational Test and Evaluation of Defense Acquisition Programs. Accessed from http://www.gpo.gov/fdsys/pkg/USCODE-2011-title10/html/USCODE-2011-title10-subtitleA-partIV-chap141-sec2399.htm on 28 October 2015.

ABOUT ACCS

The Australian Centre for Cyber Security (ACCS) is a unique, interdisciplinary research and teaching centre. It has its headquarters at UNSW Canberra, bringing together more than 50 researchers across UNSW. It serves as a national hub for policy related research and education across the full spectrum of cyber security (hardware, software, payload, networks, policy, human factors, organizational factors and the information ecosystem).

RESEARCH PRIORITIES

The centre enhances UNSW's existing and emerging research strengths in four broad areas:

- Australian Cyber Strategy, Law and Policy
- Technologies of Cyber Security, Information Assurance and Situational Awareness
- Human and Organisational Factors
- World Politics, Security and International Law in Cyber Space.

ACCS combines expertise from a range of relevant communities; political, cyber industry, defence, academic, individual and organisational users, and the media. The centre depends on close working relationships with both domestic and international industry and government, including UNSW's unique half-century relationship with Defence.

EDUCATION WITH ACCS

ACCS at UNSW Canberra is host to three innovative Masters of Cyber Security streams and other professional education programs. We offer advanced inter-disciplinary study at Master's degree-level in some of the most exciting aspects of security in cyber space: adversary tradecraft, reverse engineering of malware, red teaming, cyber war, cyber crime, cyber terrorism, to name just a small selection of our offerings. Our teaching staff includes scholars with global reputations in their field. Further information can be found on the websites indicated below with hyperlinks:

- technical stream: Cyber Security
- management stream: Cyber Security Operations
- strategy and diplomacy stream: Cyber Security, Strategy and Diplomacy

Download a brochure on these courses here.

Details on high quality professional education courses delivered in intensive mode can be found in this brochure. ACCS professional courses are delivered by full-time and adjunct staff. The adjunct staff have highly relevant direct experience in Australia's intelligence and security agencies. Our state of the art facilities include red and blue team labs and utilise an isolated network with Cyber Range, Ixia traffic generator and other enterprise-grade tools.