# Ratcatchers, Regulators, and Zealots – A Hitchhiker's Guide to Cyber T&E


Simon Reay Atkinson

Centre for International Security Studies,
Sydney Cyber Security Network
University of Sydney
HTR Synthetic Systems Engineer

simon.reayatkinson@sydney.edu.au

Stuart Fowler

Senior Systems Engineer

stuart.j.fowler@gmail.com

Jean Bogais

Information Warfare, Violence & Terrorism
Research | Applied Ethics | Specialist: SE Asia
RSIS NTU Singapore CPG, Thammasat University, Bangkok
University of Sydney Business School
University of Sydney School of Social & Political Sciences

jean.bogais@sydney.edu.au

Keith F Joiner

Senior Lecturer Test & Evaluation
UNSW University College
Australian Defence Academy
Canberra, ACT

k.joiner@adfa.edu.au



**ABSTRACT**

*This paper considers the current emphasis on Assurance and Accreditation (A&A) representing a significant philosophical change from standards-driven outcomes, to outcomes reflecting the values and trusts contained within regulatory frameworks. It uses this to examine the different characteristics Cyber T&E operators are likely to be defined by, and sometimes termed. The term "ratcatcher" was first coined by Walter Cowan (who commanded HMS Princess Royal at Jutland) when referring to his senior, Admiral of the Fleet David Beatty, Commander of the 1st Battlecruiser Squadron. Cowan considered Beatty to have a 'ratcatching instinct for war' – a rat-like cunning and intuition more typical of an autocrat (Gordon, 2003). In some respects, this allusion also connects with the 1903 French doctrine, "offensive à outrance", stipulating a combination of "élan" and "sureté" (provided by elements of firepower, discipline, logistics and tactics), to protect the "offensive à outrance" (Foch, 1903) but which became 'élan sans sûreté' – 'offence at the expense of defence'. Norman Dixon (1977) used the allusion to 'differentiate between ratcatchers and regulators, autocrat and authoritarian'. More recently, "authoritarians" have tended to differentiate themselves by describing "ratcatchers" and "regulators" as "zealots" – generally as a way of marginalising, discrediting, and so ignoring cyber testers. Emphasis on "autocratic élan", rather than "authoritarian sûreté" almost cost France the war in 1914, and while preventing Jellicoe from losing the war "in an afternoon" at Jutland, "authoritarian regulators" also cost him victory. In the wider translation, "sûreté" refers to 'assurance, security, and safety' – for which there is no English equivalent. Similarly, "élan" means*

*'to perform with energy, verve, style, and enthusiasm' and as "élan vital" (coined by Henri Bergson (1907)), to be 'a vital force emerging from self-organisation and complex morphogenesis'. Zealots meanwhile are "uncompromising fanatics in pursuit of their ideals" – and could be either, or all! We provide an analogy with Bletchley Park and the role of Alan Turing; while also introducing the Hitchhikers Guide to the Galaxy (Adams, 1985) to explain quixotically and imperfectly what modern testers and their institutions/organisations might "be" / become.*

## SECTION I – HEN'S TEETH TESTERS

A running joke amongst those concerned with the employment, hiring, and contracting of Cyber Penetration (Pen) Testers is that they are as rare as hen's teeth, hence 'Hens Teeth Testers', where *Pen Testers* – also known as *ethical hackers* – are variously described as:

> *Specialists involved with the authorised practice of testing, measuring, instrumenting, and assessing a computer system, network, or Web application through simulated (and stimulated) cyber-attack comprising: evaluation of the security of the system; forensic identification of vulnerabilities that an attacker could exploit; and determining whether unauthorised access or other malicious activity is possible, underway, or has previously been enacted.*

Employees generally limit the reach and access of penetration testing so as not to include *full-spectrum testing* (FsT), and *testing to destruction* (TtD). This can be for a number of reasons, including IP, legal, cost, and access to the type of *limited-access* Cyber Range – generally *behind the wire* Government or Security classified Laboratories where such penetration testing may be 'permissible' and undertaken under a *Cyber Cloak*. Where a *Cyber Range* may be considered to be:

> *A virtual, scalable ecology used for scenario development, cyberwarfare exercises, table tops, and cyber-infotechnological development providing: tools, education & training; courseware & materials; accreditation & certification; testing & evaluation; bureau design repositories; and cybersecurity-related facilities / networks / services seeking to assure the stability, security and performance of cyberinfrastructures and IT (including OT and ICT) systems operated (more usually) by government, security, and defence authorities.*

And a *Cyber Cloak*:

> *A **sensitive compartment information** (and data) veil [**facility** or SCIF] behind which sensitive emissions, information, data, and IT (OT and ICT) systems and networks can be securely tested and evaluated by diffusing energy, and virtually / holographically transforming / disguising electromagnetic spectrum emissions to make users and systems invisible and undetectable to outside observers.*

In this regard, *Cyber Cloaks* / *SCIFs* are also related to *Emission Security* (or EMSEC, previously known as TEMPEST), which is considered to:

> *Provide analysis of system vulnerabilities against frequencies emanating from chips, bus pathways, communications lines, networks, unauthorised access, and interference resulting from interstitial and existential electromagnetic spectrum emanations.*

EMSEC is one component of a series of possible security controls that can be used to safeguard protected and classified networks, information and data; including countermeasure reviews for

information, data and communications systems, networks, and cryptographic equipment. Whereas a *Hacker* is generally thought of as:

> *A person expert at programming and solving infotechno-logical problems with a computer and who uses computing, networking, mathematical, or other skills to illegally / maliciously gain unauthorized access / break into computers, systems, ICT, OT, or networks, in order to tamper with information / data, controls and routing in / of a computer system.*

From the above definitions, it will be clear that there are a range of other specialist skills necessary to support the type of *Assurance & Accreditation* (A&A) Teams necessary for *full-spectrum testing*. And that these full-spectrum skill sets extend well beyond those of the *Geeks* and *Nerds* more traditionally (and pejoratively) associated with cyber and computing, frequently (often unkindly) described as:

> *Non-normative, eccentric, non-mainstream, un-fashionable, computer-digital experts and enthusiasts / obsessives of an intellectual bent in a field or technological activity who it is often easy, if not actually permissible within performance management norms, to dislike and discriminate against. (Geek)*
>
> *A person who lacks social skills, is boringly studious, socially awkward, inept and a single-minded expert in a particular technical field such as cyber and computing. (Nerd)*

From Norman Dixon's view of 'ratcatchers and regulators; autocrats and authoritarians' it is unlikely that *Geeks* or *Nerds* would ever be invited to work from front-of-shop, or to any of their parties – populated (more often than not) by beautiful people like them. Yet this is clearly part of the problem, since *authoritarians* and *autocrats* wishing to divide and rule can easily label *Geeks* and *Nerds* as *Zealots* – "uncompromising fanatics in pursuit of their own ideals" – and so permissibly discriminate against them. This, at the same time, may be exacerbating the flight of such *hen's teeth* expertise to the dark web, which is often only too happy to accommodate (and pay for) their "computing, networking or other skills for illegally / maliciously gaining unauthorized access to computers, systems, ICT, OT, or networks".

Tragically, criminal gangs are also known to target hi-functioning autistic teenagers and to pay their parents / provide the safe digital-labs where they can exercise their hobbies to their heart's content. And hard-pressed, socially ostracised parents (often at their wits ends due also to their child's non-normative behaviour) – are only too happy to 'sign up'.

Alan Turing – named on 5 February 2019 by a BBC UK poll as the 'most iconic person of the 20th century' – may have exhibited some of these non-mainstream characteristics. And what was Bletchley Park – where Turing broke the Enigma Code and built his Colossus 'bomb' – but a *Cyber Range* behind a *Cyber Cloak* that maintained its secrecy and security well into the early 1990s. On 11 Sep 2009, British Prime Minister Gordon Brown issued an apology for Alan Turing's untimely death, stating *inter alia*:

> *Turing was a quite brilliant mathematician, most famous for his work on breaking the German Enigma codes. It is no exaggeration to say that, without his outstanding contribution, the history of World War Two could well have been very different. He truly was one of those individuals we can point to whose unique contribution helped to turn the tide of war.*
>
> *The debt of gratitude he is owed makes it all the more horrifying, therefore, that he was treated so inhumanely. In 1952, he was convicted of 'gross indecency' – in effect, tried for*

*being gay. His sentence – and he was faced with the miserable choice of this or prison – was chemical castration by a series of injections of female hormones. He took his own life just two years later.*

*So on behalf of the British government, and all those who live freely thanks to Alan's work I am very proud to say: we're sorry, you deserved so much better.*

## SECTION II – THE PHILOSOPHER'S STONE

In 2002, Sir Winston Churchill was voted by a BBC UK Poll as 'The Greatest Briton Ever'. It must have been somewhat galling to the professional political elites at the BBC that 'The Greatest Britain Ever' (2002) and the 'Most Iconic Person of the 20th century' (2019) were both white males – one now known to have been homosexual; the other a presumed Conservative (Liberal cross-over) heterosexual. Ostracised and detested by the Conservative Party during his *Wilderness Years*, both Churchill and Turing in their lifetimes were considered "as non-normative, eccentric, non-mainstream, un-fashionable, dislikeable obsessives – lacking in social skills". Yet it may now be argued that one may not have existed (Turing) or survived (Churchill) without the other. And together, as *Geek* and *Zealot* – they arguably shared both traits – they created the remarkable "virtual, scalable ecology" that became Bletchley Park. An ecology that could not have existed without one or other of them.

In an unpublished (MoD) study of Bletchley Park undertaken by the First Author, he concluded that 'Bletchley Park would not have worked but for the protection, leadership, and succour provided by Churchill'. That alone, he argued, 'would not have been enough'. Bletchley Park was run as a Naval Station (and Code and Cypher School), under a Naval Command – crewed by a brilliant social-network provided by Officers and Ratings of the Women's Royal Naval Service (The WRNS, 1917-1993). The Royal Navy (and its sister Commonwealth Navies like the RAN, RCN, RIN, and RNZN) has always been a broad church. It had to be, with sailors working together in floating bombs / fuel tanks / Faraday cages (SCIFs), never more than a metre apart. The WRNS provided an essential, linking, social component of naval knowledge – connecting sailors and scientists to shore and humanity – in which Turing could fit and work.

In 1942, with the entry of the U.S. to World War 2 access was also granted to Bletchley Park, building upon the 1941 Atlantic Charter and what was to become the 1943 'British-U.S. Communication Intelligence Agreement' to facilitate co-operation between the U.S. War Department and the British Government Code and Cypher School (GC&CS). Itself replaced on 5 March 1946 by the secret treaty formalized as the 'UKUSA Agreement'. The "agreement" forms the basis for all signal intelligence cooperation between the U.S. NSA and Britain's GCHQ to this day. In 1955, the formal status of "the agreement" was officially expanded to include Canada, Australia, and New Zealand as "UKUSA-collaborating Commonwealth countries" – subsequently known as "Five Eyes".

The Five Eyes Agreement is something of an aberration. On the one hand, many bureaucrats in the U.S. regard it as a mistake that will never be made (or granted by Congress) again – something of a 'multilateral-Bilateral'. On the other hand, for the four "Commonwealth countries" it is their gold standard; representing more to them, than to the U.S. There is therefore a power and perception imbalance. This extends beyond the "agreement" to create rivalries amongst other Allies – who can never be allowed in, and yet who need and often contribute far more (such as NATO, France, and Germany) than the four Commonwealth Countries combined. At the core of Five Eyes to this day lies

Bletchley Park both as "the light of the world at its darkest hour", and an example, ultimately, of failure.

The introduction of the U.S. into Bletchley Park, the First Author concluded (see also Reay Atkinson et al., 2014), caused a 'clash of culture and philosophies' – arguably one and the same thing. On the one hand, there was the more Germanic / U.S. evidential approach of 'positive-logic *proof theories*' (after Wittgenstein (1922)) – objectively verified through interrogation, evidence and experiment. On the other, a more causal, common (as in Common Law), subjective (after Kuhn (1996)) Commonwealth (and indeed French) approach of 'modelling theories' validated and falsified (after Popper (1959)) through experience and existence.

Cyber in this regard may be seen to occupy both worlds – the *control* world of probabilistic, positive-logic (after Wittgenstein), and ergodic automation; and (after Popper) the world of possibilities, dealing more with negative-logic, non-ergodic *influence*, visualisation and explanation. Similarly, *Knowledge Transfer* (KT) may be considered as a quantum phenomenon; connecting past, present and future with the indivisible 'knowledge that is both socio (human) and infotechnological' (see Bunge (2010) and Reay Atkinson & Bogais (2018a)). In this regard, programmes (see Joiner, Atkinson, Christensen & Sitnikova, 2018) need to consider the impact of Cyber as *synthesising* and combining both the socio infotechnological (SIT)[1] and infotechnological-socio (ITS)[2] systems, and the impact of these systems upon knowledge transfer (see Harmaakorpi et al. (2003), and Reay Atkinson et al., (2012a; 2012b)). From this, it may be suggested that Cyber may be:

> *A technologically bounded, largely immeasurable, strongly scientific, stochastic (ITS)[3] 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 (SIT).* (Reay Atkinson, 2009)

Whereas the *Aristotelian* interpretation of *techné* is subjective and about change, *epistemé* more epresents Wittgenstein's 'evidential knowledge of verification and positive-logic'. In Aristotelian logic, sense is provided through *phronesis* – reflective wisdom – deemed necessary to falsify / make sense of the existential and the experiential. It is reflective wisdom that makes adaptation and new creation / designs possible. The British TSR 2 fighter-bomber aircraft programme is a case in point. It created a socio-infotechnological ecology that was 'both a proposal for a machine [and] a theory about how the political, bureaucratic, and strategic world could be made to look five or ten years later' (Law & Callon, 1988). In other words, it combined an inclusive learning model and knowledge network comprising the *epistemé*; the *techné* and *phronesis*.

## SECTION III – BUILDING THE TEAM

The clash of a more *puritanical* (see Hopper & Hopper (2007)), *strong-signal* U.S. Logic-Positive approach, imposed upon the *weak-signal*, "subjective approach of modelling theories validated and

---

[1] Socio-Info-Techno systems stress the reciprocal interrelationship between humans and computers to foster improved shared awareness for agilely shaping the social programmes of work, in such a way that humanity and ICT [control] programs do not contradict each other.
[2] ITS systems seek to program the relationship between technical processes and humans by digitising performance fidelity and coding for repeatable risk free procedures in computer-control-spaces so that data and communication do not [temporally] contradict each other.

[3] More recently consideration has been given to Information Technology (IT) and Operational Technology (OT).

falsified through experience and existence" caused a shock to Bletchley Park. While it continued to function, its great days were over. Fortunately the model had been successfully *replicated* in other "stations" that continued to function effectively well into the 1970s. The tragic legacy of this "clash of philosophies" lay ultimately in the death of Alan Turing. The ban on homosexuals serving in the UK (and Commonwealth) Armed Forces and Security Services was introduced on U.S. insistence after WW2 and was only rescinded fully in the 2000s. The First Author is on record as being one of the very few Royal Navy Officers to stand against the ban – writing against it in his 1995 article in the UK *Naval Review* (Reay Atkinson, 1995) Issue 4, pp. 303-304 (*The Homosexual Enquiry I*).

Andrew Gordon's (2003) allusion of "ratcatchers and regulators" may also be extended to include the *weak-signal*, logic-negativism and falsification of autocrats, and the more authoritarian, *strong-signal* control world of logic-positivism. In isolation or treated separately, one may negate or blind the other. While, since each side can accuse the other of being "zealots", also removing the essential variety of thinking – and establishment-misfits such as Turing and Churchill – necessary to solve complex problems. Moreover, *synthesising* both philosophies (*objective* verification and *subjective* falsification) may contribute to the "complex map of human knowledge". Crucially, the two spaces described by Cyber are complex; highly entangled and connected, so even though they may be distanced in time and space, the Quantum-behaviour of one can be affected instantly by that of the other (see Wendt, 2015). Yet, although both spaces make up the empirical body – taken as pairs, *experimental-evidential* or *experiential-existential* – it is possible that they may become antithetical to each other. Particularly when one emphasises strong-signal ergodic verification through *rule-based* probability and the other seeks to falsify non-ergodic causality based upon common *values-based* truisms and trusts.

As worryingly, today the social sciences seemingly based more on managed-diversity; rather than variety of thinking (Reay Atkinson et al., 2012c)); and an unwitting rejection of Popper's (1959) argument for "subjective-falsifiability"; and the adoption of Wittgenstein's (1922) "objective-verification" model, has largely rejected the empiricism of "existence and experiment" in favour of "experience and evidence-based-research (why bother!?)", see also Tooby & Cosmides, 1992. In the course displacing the very realms of *subjectively* falsifiable 'interpersonal, behavioural and personal traits' one would expect the social sciences, arts and humanities to champion.

All this suggests that, in building a Cyber security Test Team, organisations will need a range of skill-sets and character traits. Inevitably, this means that teams are probably not going to be supported by senior management (for the fear of the unknown and losing control) or HR departments, for which these types of organisations operate on the edge, if not beyond performance-management norms. In simple terms, organisations are being asked to set up Cyber security teams that will necessarily push the organisation to test; while at the same time operating at more of a war-time than peace-time setting – requiring thinking leadership and management; rather than management-by-rules alone.

Cyber Security functions also need to be able to support activities across system and capability Life Cycles; including System Integration and Whole of Capability, such as Support Systems. In addition to testing and evaluation responsibilities, functional Cyber security work-stream activities are likely to require skills, such as:

> **Governance** – providing consultancy services necessary to provide for Cyber Assurance, including the implementation, and development of policy in liaison with outside organisations; in addition to specialist skill set development for Red Teaming, Vulnerability Testing, Scenario Development, and education / training.

**Integration** – incorporating preparation / integration of multiple functions for assuring and enabling Accreditation (IATT, IATO, ATO) of operating and support Systems; including education and development.

**Licensing** – providing for Cyber-Security accreditation and certification (and approvals / recommendations for IATT and IATO) incorporating the requirement to certify, accredit and for penetration (and vulnerability) testing to gain IATT, IATO, and ATO recommendations.

**Cyber Security Operations** (including elements of OPSEC) – providing for the advisory / liaison / and physical ICT security requirements necessary to support / clear / approve certification and accreditation teams and infrastructure requirements.

**Capability Science & Technology** (CS&T) – providing dedicated R&D cyber tools / instruments, independent V&V, in addition to horizon scanning, and supporting Cyber assurance, accreditation, education and development delivery and professional / skills development.

## SECTION IV – ASSURANCE & ACCREDITATION

There are four high level products provided by Assurance and Accreditation:

**Facilitation**: Facilitate, prepare and integrate cyber systems and networks through an approved Accreditation and Certification framework for being granted *Authority to Operate* at the appropriate levels of classification; **Note**. In some cases this will require taking on an integration role to accredit and certify contractor supplied systems for being granted authority to operate.

**Certification**: Develop and lead an approved / licensed cooperative Certification programme.

**Assurance**: A cyber-security *Assurance* programme capability, involving all security stakeholders, leading to the granting of ATO status. This is a broad undertaking which may include developing skill sets, S&T horizon-scanning, cyber-tools, cyber education & development, consultancy, and awareness programmes, as well as table top simulation exercises and workshops.

**Accreditation**: Develop and lead an approved / licensed cooperative Accreditation programme.

In Cyber security, *Certification* deals with confirming that specified 'norms, rules or standards' are conformed with; whereas Accreditation is more about the process by which a *trusted* body 'grants formal recognition, approval and acceptance of the associated residual security risk within the operation of a system': [4] *Certification* is about ensuring ethical norms, rules or standards for right conduct or practice are adhered to; and *Accreditation* about moral values for *assuring*, granting and upholding higher values for proper conduct, over time. *Certification* is also largely about static controls – shutting the stable door before the horse can bolt. While *Accreditation* is about the dynamic; *assuring* controls are in place and that the horse does not need or want to bolt in the first place.

[4] Source ISM (Dec 2018).

***Table 1. Assurance & Accreditation Stages***

| Assurance & Accreditation Stage | Description |
|---|---|
| **Certification (Static – rules-based)** | Certification by an accredited organisation, or equivalent certification body, in relation to cyber. The end result of a process which provides the formal acknowledgement that a capability conforms to a specialised standard at different threat levels and may be given: Interim Authority to Test (IATT); Authority to Connect (ATC); and Interim Approval to Operate (IATO) |
| **Accreditation & Certification (Moving towards the Dynamic)** | Formal recognition by an Authorised body that an organisation has demonstrated competence to carry out certain duties and tasks and that a system can be authorised to operate in a defined configuration recognising, approving and accepting the associated residual security risk with its operation in a specified role and a particular cyber threat environment, for example a capability or system may be granted IATT, ATC, or IATO. |
| **Assurance & Accreditation (Dynamic)** | Assurance looks to provide confidence that the specialised standards applied during certification were both appropriate to the target system and accurately assessed. Cyber Test & Evaluation provides the Accrediting Authority with assurance that platforms, systems, and networks are capable of operating securely at different cyber security threat levels.<br>Accreditation means that an Authoritative Body has given formal recognition, approval and acceptance of the associated residual security risk with the operation of a system in its intended cyberspace environment, meaning:<br>Accrediting bodies granting ATO and FOC caveated upon meeting specified standards giving Approval to Connect and to Operate Securely at different cyber threat levels. |

The certification approach of applying static-rules fails to address the individuality of complex systems, particularly when applied to cyber-physical systems and critical OT networks. This variability is typically addressed using a risk management approach where variations to the static certification rules are granted by the individual certifier or auditor. This risk is inevitably subjective, and the resultant residual risk presented to accreditation authorities are driven by the personalities involved in the certification process. Zealots will likely assess a risk as more severe than Ratcatchers.

Of course, each participant in the certification process is neither entirely a Zealot nor entirely a Ratcatcher. Personal experience with one or more threat, or with the implementation of one or more security controls, results in certifiers taking a Zealot-like approach to some risks and a Ratcatcher-like approach to other risks. Additionally, the manifestation of these traits within the system designers and integrators can further influence the residual risk attached to a certification report.

The Australian National Audit Office's report into the cyber resilience of government departments (AS-ANAO, 2018) demonstrated this inconsistency. Even when auditors were only dealing with a certification against four security controls, the self-assessment of the National Archives deviated from the audit findings of the ANAO. The report concludes that:

*Entities must rely on professional judgement – from internal and/or external ICT security advisors – to assess security controls' effectiveness. Different approaches and interpretations of the assessment criteria will continue in the absence of a common control assessment methodology.*

This inconsistency in approach and interpretation is only amplified when certification is performed against a broader set of security controls, such as those common in government certification standards. While a common control assessment methodology may help to mitigate these issues in enterprise IT networks, it can be argued that a strict assessment methodology would only worsen the incompatibility between these certification standards and cyber-physical systems.

The result when certification standards are applied to complex cyber-physical systems is an accreditation authority that is expecting an objective assessment receiving a subjective recommendation that is influenced by the Zealots and Ratcatchers designing and assessing the system, with no apparent way to sensibly normalise these risks. This conclusion is not meant to minimise the importance of comprehensive cyber security certification standards, but rather to highlight that they are insufficient in isolation, particularly when considering complex cyber-physical systems.

The dynamic Assurance & Accreditation approach, as articulated in MITRE's work of Cyber Resilience (Bodeau et al., 2012) and the RAN's concept of Cyberworthiness (Fowler et al., 2017), provides an avenue for addressing the shortcomings of static rules-based certification. These concepts build upon existing Certification and Accreditation frameworks through an understanding that complex critical systems require an ability to operate within a hostile cyber environment. Rules-based certification and accreditation approaches that employ a methodology based on static risk assessments struggle to quantify this ability to perform when under sustained cyber-attack.

The solution to a consistent implementation of these dynamic assurance and accreditation frameworks to cyber-physical systems is an area of ongoing research. One proposed approach would be to develop a comprehensive threat model specific to the system and the varying contexts within which the system operates, with controls allocated to mitigate those threats using the So Far As Reasonably Practicable (SFARP) methodologies common in system safety analysis. In order to minimise the influence of Zealots and Ratcatchers, variables within the threat model are to be modelled endogenously where possible, with exogenous variables strongly interrogated for their validity.

Cyber security test and evaluation remains the primary method for validating the results of any desktop risk assessment, including those underpinned by comprehensive threat modelling. This test and evaluation must be focused and tailored to the system based on the threat modelling in order to efficiently allocate the resources which were highlighted for their rarity in Section I (Joiner, Ghildyal, Devine, Laing, Coull & Sitnikova, 2018). When built atop the foundation of a rules-based certification assessment, comprehensive cyber security test and evaluation can provide the assurance that the system is worthy of accreditation.

## SECTION V – ON ETHICS

Recent US and Australian DoD directives relating also to Cyber transition organisations from a rules-based to a values or trusts-based organisation. This represents a significant philosophical change from standards-driven outcomes, to outcomes reflecting more the values and trusts contained within

regulatory frameworks – explicit to effective Risk Mitigation. This also has ethical and moral implications for the Cyber-security Regulatory Framework, for whereas:

> ***Ethics*** *deal with morals and the principles of morality pertaining to right and wrong conduct and being in accordance with the norms, rules or standards for right conduct or practice, such as the standards of a profession;*
>
> ***Morals*** *are concerned with the principle of first doing no harm; then of right and wrong behaviour with regard to holding or manifesting higher values for proper conduct.* (Reay Atkinson & Bogais, 2018b)

Ethics is about the philosophy of the social and values. This is not about good versus harm; or right versus good; this becomes the essence of the indivisibility between the infotechnology and the socio that is ethics, hence considerations of the socio-infotechnological (SIT): "*Knowledge today is the Social and the Infotechnological, or Socio-IT*". This needs to be understood in any understanding of Data, Information, Communications and Knowledge and their interactions and biases. This is the socio-ethical. (Reay Atkinson & Bogais, 2018a) ((Reay Atkinson, 2018a)

The tension between morals and ethics is implicit within an understanding of Command and Control; Leadership and Management; their application and the maintaining of trusts and values throughout an organisation life cycle. *Assurances* are vested in higher values. (Reay Atkinson & Bogais, 2018b) (Reay Atkinson, 2018b) Paraphrasing Reay Atkinson & Goodman (2008), 'rule-driven strategies (for example certification, alone) give the enemy the opportunity to harness and so fix one's own tactics to their advantage. They confuse strategy and tactics, with strategic objectives and lead one to define one's enemies in terms of their tactics and capabilities rather than their strategy'.

There are also questions to do with cyber and its application, not simply in Defence, specifically in the region of new and emerging sciences and technologies that offer the potential of 'completely removing humanity from the loop'. (Reay Atkinson & Bogais, 2018a) The separation of the human from the artefactual, the arte[5] from the fact (through, for example, AI – see Klemas & Chan, 2018), marks a fundamental critical juncture of this new age with all other scientific ages and human generations that have come before. There will inevitably come a time when the Knowledge that was previously sovereign to humanity may also be non-human and non-natural (as in nanotechnology); vested in some form of AI:

> *The resultant loss of human sovereignty may create a colonial existence for all humanity in which humans are ruled, governed, controlled, or under the sway of a new interstisence – 'a perfect heteronomy'. (Rousseau, 2010 (1754-1762)) Clearly this has significant ethical and moral implications, hence the need to differentiate between ethics[6] and morality[7]. There may be shades of morality but ethics is a binary: one is ethical, or not. For example, one may be moral, immoral, or indeed amoral and still be found ethical in terms of certifiable norms,*

---

[5] Arte may be considered as a form of social knowledge that is a product of the abstract, the conceptual and the arts, and to be a form of nonverbal communication depending on internal form and visualisation rather than pictorial representation.

[6] Dealing with morals and the principles of morality pertaining to right and wrong conduct and being in accordance with the norms, rules or standards for right conduct or practice, such as the standards of a profession.

[7] Concerned with the principle of first doing no harm; then of right and wrong behaviour with regard to holding or manifesting higher values for proper conduct.

*rules and standards of behaviour; whereas once in breach of the norms, rules and standards (in other words struck-off as being unethical) one may never be declared ethical even though one may be acting morally in assuring higher values, for example by refusing to obey an unlawful order no matter how ethical – the Nuremberg / Srebrenica question.* (Reay Atkinson & Bogais, 2018a)

## SECTION VI – NO PLACE FOR THE FAINT HEARTED

For engineers and scientists of older Gen X and younger Gen Y (b. 1960-1974; and 1975-1989), Douglas Adams *Hitchhikers Guide to the Galaxy* (Adams, 1985)[8] – with later cult-following amongst the *Millennials*, b. 1990-2004 – represented an epiphany. 'Hitchhikers' follows the adventures of a hapless Englishman, *Arthur Dent*, who is the last surviving man (later joined by the last surviving woman, *Trillian*), who happens to be rescued (by Ford Prefect) just before the destruction of the Earth by the *Vogons* (a race of zealous, deeply unpleasant, bureaucratic aliens) to make way for an intergalactic bypass. The main characters of *Hitchhikers*, as developed by the radio/TV series, and in films, would appear to fit the *deployable* five-crew Assurance and Accreditation Team profiles

**Blue Team Lead** (responsible for Assuring and bringing together the Accreditation, Certification and Testing teams): *Arthur Dent's* insistence on his way of life and determination is exhibited when he interrupts his morning shave to fight with the people trying to bulldoze his house down. A paradoxical, *every-human* character, he is nevertheless a model citizen who supports his community, and is generally liked (and loved) by those who meet him – probably for his optimism (despite everything); his remarkable 'stiff upper lip" and sangfroid even when the earth has been destroyed and he has been abducted by aliens. Humble, with an omega-autocratic (as opposed to alpha-regulatory) style of leadership, through *falsification* he looks to find the humour in any situation. Resilient, he keeps on bouncing back, overcoming adversity, and fighting on as hard as he can. [9]

**Green Team Lead** (responsible for Certification): *Zaphod Beeblebrox* a hedonistic, multi-headed (brained), eternal gap-year thrill-seeker, clever, imaginative, control-order narcissist – almost to the point of zealousness and obsessive solipsism.[10] Irreverent (to those he dis-trusts or dislikes), he is extremely insensitive to the feelings of those around him, particularly those without recognisable order and [certifiable] function. A *positivist*, enthusiastic about everything, with no table-manners and oft to throw temper tantrums, he does some things without reason, such as pressing the Improbability Drive button "just because it was large and shiny". He is nevertheless quite charismatic and has a 'nervous sort of hyper-energetic way of trying to appear relaxed'(Gaiman, 1993); while ordering other parts of his brain in order to pursue his grand strategy, which he can never achieve largely because of over-compartmentalisation and control of his mind at the unit/tactical level.

**Red Team Lead** (responsible for scenario and Table Top development): *Trillian* a strategic analyst, mathematician and astrophysicist developed the 'Guide Books for the AI (synthetic)

---

[8] The book was published by Pan Books because the BBC in its infinite bureaucratic wisdom – led, no doubt, by "zealous advertising accountancy consultants/ executives and film makers", turned down the opportunity!

[9] See Ean Adams on Arthur Dent: https://prezi.com/nrim3upqj3si/arthur-dent-character-analysis-ean-adams/, accessed Feb 2019.

[10] The philosophy of the mind that takes only one part of Descartes's maxim ("I think, therefore I am") to ascertain one's own existence; holding that external knowledge (beyond the mind) is uncertain and un-verifiable – other minds cannot be known and may not exist outside the mind.

universe' and saves the Krikketers[11]. She is seemingly in an eternal love triangle between Arthur Dent and Zaphod Beeblebrox – one she loves for his simplicity, depth of character, and caring nature; the other (Zaphod) for his spontaneity, charisma, and complicated order-disordered (every Parent's dreaded Gap-year boyfriend/girlfriend). Arthur considers his feeling for Trillian to be "the only thing that he ever had questions about where the answer made him happy". Through maculate, imperfect conception (largely it would appear because she and Zaphod were different species), she and Arthur have a child, *Random Dent*. Later she becomes a Sub-Etha scholar-practitioner – a specialist in interstellar faster-than-light, superluminal, hyper-subliminal, networked telecommunications systems, used by hitchhikers to flag down passing spaceships – under the handle[12], *Trillian* [*ad*] *Astra*.[13]

**Assessors** (for example individuals licensed under the Information Security Registered Assessors Program (IRAP)): *Ford Prefect*, an existentialist who takes an independent, broad, sometimes nihilistic view of the universe. Eccentric, in a Heideggerian way endlessly seeking to experiment and test the bounds in order to surprise (see Derrida, 1989), he is said to possess a quixotic and very dark sense of humour. His smile, when delivering an assessment, is said to "send hitherto sane men scampering into the trees". In *Hitchhikers*, he acts as a guide to the universe for the often bewildered every-human Arthur Dent – pulling the loose and disparate parts of the picture together. He introduces *Arthur* to *Zaphod*, *Trillian* and *Marvin* – and to fantastical mind-boggling concepts, from "teasers", an explanation of UFO sightings on Earth; to the extraordinary usefulness of towels – he also uses as veils (Cyber?). He is not specifically interested in such "causes" as *Assurance* & *Accreditation*, and is a dilettante when it comes to the search for the question to the ultimate answer of "life, the universe and everything", which he leaves to *Arthur*, *Zaphod*, *Trillian*, and *Marvin*.

**Testers** (including Ethical Hackers/Penetration Testers): *Marvin* [the Paranoid Android] a depressive stoic[14] consumed more by doubt, than paranoia and a need to think, test, analyse – with a perfectly rational feeling that all his companions want him to do is "open the door". Adams considered Marvin as an "Eeyore" type character – and it is *Zaphod* (in his zealousness?) who calls him "the *Paranoid Android*", probably to hide his own paranoia? *Marvin* remains eternally pessimistic, exacerbated by accompanying Zaphod on his endless missions of self-discovery. Waiting 40 million years to be re-found – "the first ten million years were the worst, and the second ten million years, they were the worst too. The third ten million I didn't enjoy at all. After that I went into a bit of a decline" – the best conversation he had was with a coffee machine. *Marvin* applies Descartes full maxim 'I doubt; therefore I think; therefore I am' to form an extreme negative logic based on the existential struggle between "I", "Android" and "Being". This existential-interstitial question logically afflicts Marvin with depression, despair, and ennui. Not helped by the fact that he has a "brain the size

[11] The planet Krikkit (with seemingly many names / rules similar to the game of Cricket) is located in a dust cloud composed chiefly of the disintegrated remains of the enormous spaceborne computer Hactar. Due to the dust cloud, the sky above Krikkit is completely black, and thus Krikkiters lead insular lives and never realised the existence of the Universe.
[12] A tradition given to pilots and astronauts and bestowed on them by their colleagues; by which, henceforth, they are known – including in official signals. For example "Ice" in the film *Top Gun*.
[13] Adams potentially makes reference in Trillian's name to the RAAF / RAF motto: *Per Ardua ad Astra*; 'Through Adversity to the Stars'.
[14] Stoics, from the Greek school of Stoicism, are those who can endure depression, pain or hardship without showing their feelings or complaining.

of a planet" which he is seldom, if ever, given the chance to use. Except for "opening doors", for which he reserves a particular contempt, "despising their blissful satisfaction with existence".

The paradox appears two fold. The first is in recruiting, identifying, educating and developing the skill sets required for effective Assurance & Accreditation Teams (described in our Hitchhikers analogy by two Aliens; an Android; a man and a woman!); secondly, in *fitting* these teams into normative managerialist structures, controlled and scripted by various Performance Management regimes – such as Lean / 6 Sigma, project management, systems engineering etc. – into which these Teams simply may not *fit*, be accepted or be subordinate to the extant tensions between them (i.e., Bradley et al., 2019: submitted & Gray et al., 2017). In fact, it is probably worse than that: Professionalization (for all its goods) has inevitably led to *normification* – which, in turn, has created closed-shops, restricting entry to all but increasingly narrow, qualified-elites. At the same time, "HR" has applied mandated-diversity-to-normification; scripting teams based more upon "looks" – ethnic, gender, and sexual balance, *per se* – than common values and variety of thinking.[15] Variety, in terms of thinking and behaving differently to prescribed norms, has potentially become *proscribable* – today it may be perfectly permissible to proscribe against those who think differently, and who disrupt the norms. This is very dangerous. In a final, rather sad analogy in *Hitchhikers*, the "Golgafrincham Ark Fleet, Ship B" is populated by 'hairdressers, accounting [consultancy] executives[16], film makers, security guards, telephone sanitisers, and the like…' as a ruse for ridding Golgafrincham of such middle-aliens and retaining leaders in the fictional "Ark Fleet, Ship A" and workers in "Ark Fleet, Ship C".

## SECTION VII – END GAME?

The view of the authors runs contrary to the perfection of performance management regimes, or the Golgafrinchams – warned also against by Voltaire: "do not let perfection become the enemy of the good". We believe in the common values, of the common man and woman (in a non-binary sense) – the concept of Laïcité in the French – and that amongst all our populations, Assurance & Accreditation (Cyber) capability skill-sets exist and can be brought forward; educated and developed. Indeed, the bases of our argument – running throughout this paper – is that our institutions need to be "broad churches", open to a variety of different thinking and thinkers if we are to answer the critical questions currently and forever facing humanity. This is not confined to Cyber, but we would be wrong not to acknowledge that we are creating, or on the cusp of creating a new existence within Cyber, and potentially new 'AI beings' to live alongside humans, in these synthetic ecologies. Similarly, we do not believe in an "ultimate answer", let alone an ultimate solution designed to remove humans or

---

[15] **According to the U.S. Department Labor's, Bureau of Labor Statistics, 73.3% of HR managers are women. Writing in 'The HR profession's big diversity question: Where are the men?' (*HR Dive*, Nov 2018), Pamela DeLoatch posits: "Diversity issue works both ways – and having a profession that is so heavily dominated by one gender isn't a good thing, as so much research indicates". Steve Browne, executive director of HR for LaRosa's Inc., is quoted as saying that "perhaps the most important focus for HR is diversity of thought" – by which the authors infer variety. See https://www.hrdive.com/news/the-hr-professions-big-diversity-question-where-are-the-men/542611/ , accessed Feb 2019.**

[16] Belonging to the type of Accountancy Consultancy Companies (ACCs) who introduced Performance Management in the 1980s as the "ultimate answer".

particular types of humans from existence. We argue, instead, that at key moments in our existence humans have created the institutions and organisations to engender and enable such thinking, and thinkers – such as Bletchley Park, which stands as a talismanic beacon of hope in adversity to this very day.

The authors are probably most afraid of certainty – the type of certainty in righteousness and "doing right" (rather than "first no harm") – upon which Zealots (be they certifiers, ratcatchers or regulators) thrive, and depend for their tyrannies. Each of the authors has been subject to such accusation and marginalisation in the past, generally by those seeking to dismiss the truth – exactly because they "cannot handle the truth". [17] It is this handling of the truth that is fundamentally important. The maxim of the Public Service is to 'Tell Truth to Power", impartially and however unpleasant that truth may be. Yet in recent years, those telling truths to power – increasingly the imperfect (for example denialists) and outsiders – have faced dismissal, dis-accreditation, or worse. So much easier to keep *schtum*, and carry on up the professional grease pole to the slippery top – except. Except when, as now, the system no longer works and the very zealous certainty necessary for managing the status quo is creating yet more instability. It is at these times of change when leadership is necessary to break the bandwidth-yolk imposed by conformity, through normification. A new set of maths is needed to deal with "radical uncertainty". (Marsay, 2015) These are times at which new leadership (and management) is required – when we can bring such thinkers (themselves potentially zealous in their own domains) and enable them to thrive and to be. As Turing was able to do in the being of Churchill's Bletchley Park.

The problem is not capability, per se – but capacity. And that means a new "war-time thinking" approach that considers how we take in people from a broad range of the population – Sir Edwin Hardy Amies, the Queen's dressmaker from her accession to the throne 1952 until his retirement in 1989, was also a member of Churchill's WW2 Special Operations Executive – and educate and develop them to 'be' those thinking people humanity needs. It was no accident that GCHQ and Bletchley Park both began also as Code and Cypher Schools – and we need such Cyber Schools again, and the mentality that enables and thrives on the imperfection of the good and the many (the *populus vulgaris*) – and Robert Watson-Watts' (1935) "Cult of the Imperfect".

Finally, while we do not necessarily suggest that humanity should not be involved in calculating the "Answer to the Ultimate Question of Life, the Universe, and Everything" – which may be 42, or 54, or possibly both – we do believe that the liberal democracies provide the best models to enable humanity to answer these questions, and to "live long and prosper'.

May you live in interesting times. [18]

## REFERENCES

Adams D. (1985) *The Hitchhiker's Guide to the Galaxy, Original Hitchhiker Radio Scripts,* London: Pan Books.

AS-ANAO. (2018) Cyber Resilience. *ANAO Report No. 53.* Canberra: Australian National Audit Office.

[17] Colonel Nathan R. Jessop (Jack Nicholson) to Lt. Daniel Kaffee (Tom Cruise) a naval lawyer in the film A Few Good Men (1992).
[18] Old English curse, although often ascribed to the Chinese – as Descartes might say 'he was blessed by the interesting times of hardship, and cursed by the stability of normal times'. Perhaps it is actually a blessing from the perfidious English?

Baron-Cohen S. (2003) *The Essential Difference - Male and Female Brains and the Truth about Autism,* New York: Basic Books.

Bergson H. (1907 (1911 tr. Arthur Mitchell)) *L'Évolution créatrice (Creative Evolution)* London: Henry Holt and Company.

Bodeau D, Graubart R., Picciotto J., & McQuaid R. (2012) Cyber Resiliency Engineering Framework. Washington: The MITRE Corporation.

Bradley J., K. M. Castelle, M. Efatmaneshnik, & K. F. Joiner. (2019: submitted) 'On parsimony in governance: foundational fusing of complex program management and system engineering', 14th Annual Systems of Systems Conference, IEEE & INCOSE, Anchorage, Alaska, U.S., 19 - 22 May.

Bunge MA. (2000) Ten Modes of Individualism - None of Which Works - And Their Alternatives. *Philosophy of the Social Sciences* 30(3): pp. 384-406.

Derrida J. (1989) Of Spirit, Heidegger and the Question. *Critical Inquiry translated by G. Bennington & R. Bowlby* The University of Chicago Press, Vol. 15, No. 2 (Winter): pp. 457-474.

Dixon N. (1977) *The Psychology of Military Incompetence,* London: Jonathan Cape.

Foch FJM. (1903) *Les Principes de la guerre. Conférences faites à l'Ecole supérieure de guerre (On the Principles of War),* Paris: Berger-Levrault.

Fowler S, Sweetman C, Ravindran S, Joiner K, & Sitnikova E. (2017) Developing cyber-security policies that penetrate Australian defence acquisitions , . *Australian Defence Force Journal* vol 202, July.

Gaiman N. (1993) *Don't Panic: Douglas Adams and the Hitchhiker's Guide to the Galaxy,* London: Titan Books.

Gordon A. (2003) Ratcatchers and Regulators at the Battle of Jutland. In: Sheffield G, et al. (ed) *The Challenges of High Command.* London: Macmillan Publishers Limited.

Gray A., H. Nasser A., J. K. Richardson, & K. Rooke. (2017) 'Foundations for improved integration – Using Systems Engineering in Programme and Project Management,' INCOSE Conference, Adelaide, 15-20 July.

Harmaakorpi V, I., Kauranen, & A., Haikonen. (2003) The Shift in the Techno-socio-economic Paradigm and Regional Competitiveness. *The 43rd Conference of European Regional Sciences Association (ERSA), 27-31 Aug.* Lahti Center, Jyväskylä, Finland: Helsinki University of Technology.

Hopper K, & W., Hopper. (2007) *The Puritan Gift,* London: I.B. Taurus and Co. Ltd.

Joiner K. F., S. R. Atkinson, P. H. Christensen, & E. Sitnikova. (2018) 'Cybersecurity for Allied Future Submarines', World Journal of Engineering and Technology, vol. 6, pp. 696 - 712, http://dx.doi.org/10.4236/wjet.2018.64045.

Joiner K. F., A. Ghildyal, N. Devine, A. Laing, A. Coull & E. Sitnikova. (2018) 'Four testing types core to informed ICT governance for cyber-resilient systems', *International Journal of Advances in Security*, vol. 11, pp. 313 - 327, http://www.iariajournals.org/security/sec_v11_n34_2018_paged.pdf

Klemas, T. J. & Chan, S. (2018) 'Harnessing Machine Learning, Data Analytics, and Computer-Aided Testing for CyberSecurity Applications: Achieving Sustained Cyber Resilience for Typical Attack Surface Configurations and Environments,' *CYBER 2018 : The Third International Conference on Cyber-Technologies and Cyber-Systems*, IARIA, Athens Greece, 18-22 November.

Kuhn T. (1996) *The Structure of Scientific Revolutions,* Chicago, IL: University of Chicago Press.

Law J, & M., Callon. (1988) Engineering and Sociology in a Military Aircraft Project: A Network Analysis of Technological Change. *Social Problems. Special Issue: The Sociology of Science and Technology.* Vol. 35, No. 3, June.

Marsay D. (2015) Decision-Making under Radical Uncertainty: An Interpretation of Keynes' Treatise. *Economics - The Open-Access, Open-Assessment E-Journal* Economics Discussion Papers, No 2015-43, Kiel Institute for the World Economy. http://www.economics-ejournal.org/.

Popper K. (1959 (1934)) *The Logic of Scientific Discovery,* (published in German 1934) Berlin: Mohr Siebeck.

Reay Atkinson S. (1995) The Homosexual Enquiry I. *UK Naval Review* Issue 4: pp. 303-304.

Reay Atkinson S. (2009) Cyber-: Envisaging New Frontiers of Possibility. *UKDA Advanced Research & Assessmnent Group* Unpublished, Occasional Series, 03/09.

Reay Atkinson S, & A. Goodman. (2008) Network Strategy and Decision Taking. *ARAG Occasional, UK Defence Academy* 11 / 08.

Reay Atkinson S, & J. J., Bogais. (2018a) A Critical Juncture – DC Dynamics or DC Stasism: to be or not to be? That is the question In: Parfitt N (ed) *Data Center Dynamics (DCD) White Paper.* London DCD - Feb 2018.

Reay Atkinson S, &, J. J., Bogais. (2018b) Research Ethics in Quantum Photonics, AI, Robotics, and Nanotechnology – Thinking New Codes of Ethics. *Prometheus - Critical Studies in Innovation* Submitted - Unpublished.

Reay Atkinson S, A. Goodger, N.H.M Caldwell, L. Hossain. (2012a) How lean the machine: how agile the mind. *The Learning Organization* Vol. 19 Iss: 3: pp. 183 - 206.

Reay Atkinson S, A., Goodger, S. Lesher, N.H.M. Caldwell, J. Steel, & D. Shoupe. (2014) What are the real risk of knowing and not knowing - leading Knowledge in Cyber. In: DoD C-U (ed) *19th ICCRTS: C2 Agility: Lessons Learned from Research and Operations, 16-19 June.* Alexandria, (Washington), Virginia: CCRP (submitted).

Reay Atkinson S, D. Walker, K. Beaulne, & L. Hossain. (2012b) Cyber - Transparencies, Assurance and Deterrence. *Presented at IEEE Cyber Conference, 14-16 Dec.* Dec. Washington: IEEE.

Reay Atkinson S, S., Feczak, A., Goodger, N.H.M., Caldwell & L. Hossain. (2012c) Cyber-internet: a potential eco-system for innovation and adaptation. *European Alliance for Innovation: Internet as Innovation Eco-System Summit and Exhibition 2012, 4-6 Oct.* Riva del Garda: Italy: EAI.

Rousseau JJ. (2010 (1754-1762)) *The Social Contract, A Discourse on the Origin of Inequality, and A Discourse on Political Economy. : ,* New York: Classic Books International.

Tooby J, L. Cosmides. (1992) The Psychological Foundations of Culture. In: Jerome H, L. Cosmides & J. Tooby (ed) *Chapter 2: The Adapted Mind: Evolutionary Psychology and the Generation of Culture.* Oxford: OUP.

Wendt A. (2015) *Quantum Mind and social science,* Cambridge, England: Cambridge University Press.

Wittgenstein L. (1922) Translated by F.P. Ramsey and C.K. Ogden. *Tractatus Logico-Philosophicus.* London: Kegan Paul.

## BIOGRAPHY

**Associate Professor (CAPT (Dr)) Simon Reay Atkinson RANR** is an Associate Professor at the CISS and in Engineering and Information Technologies at the University of Sydney. A first degree in engineering was combined with a second degree (a research-based MPhil) in International Relations; majoring in Law and Economics. This provided the foundation for a PhD that explored, through engineering, security, defence and social science lenses, complex systems and behavioural modelling. The underlying strength of research has been its applicability and re-use; allowing for practical application, specifically in the area of Cyber.

**Dr Keith Joiner, CSC,** 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 conducted numerous joint test and evaluation activities and where he was awarded a Conspicuous Service Cross. He is a Certified Practising Engineer and a Certified Practising Project Director with over 60 major academic presentations and publications.

**Stuart Fowler** holds an undergraduate degree in mechatronic engineering and a post-graduate degree in cybersecurity. He has more than a decade of experience working as a systems engineer in the defence industry during which time he has helped to design and deliver some of Australia's most complex military systems.

**Associate Professor Jean (Jonathan) Bogais** is a Paris-Sorbonne educated sociologist and intercultural psychologist with over 30 years experience working in spaces of violence. His principal interests are Applied Ethics, Information Warfare and deconfliction. Applying complex systems to strategic analysis and decision-making, he has considerable experience in building networks that can identify and manage uncertainty to introduce change over time. He is a recognised specialist in Southeast Asian affairs, for example serving as a UN special advisor in the negotiations of the 1991 Paris Peace Agreement for Cambodia. He was awarded a Master in Social and Intercultural Psychology in 1978 and a PhD in Sociology in 1984.