Submission to the Defence Trade Controls Review

Air Power Australia

28th May, 2018
The Terms of Reference for the Defence Trade Controls Review 2018 review pose four central questions:

1. whether the Act is fit for purpose;
2. whether there are any gaps in the Act's controls;
3. whether any unintended consequences are resulting from the Act's controls; and
4. any other matters considered relevant.

Air Power Australia (APA) is an independent think tank focussed on research in defence sector policy, strategy and related areas. APA has published hundreds of reports and papers since its inception in 2004, and produced dozens of submissions to the wide range of Defence and Parliamentary Inquiries that have been held over that period.

The Defence Trade Controls Act in its current form has caused widespread difficulties for researchers and publishers in defence and defence related areas – difficulties that are unique to Australia, as they are not present in the US ITAR/CCL and UK systems. When analysed, the DTCA is seen to be designed in a manner closely following that of the recent Russian Federation’s “catch-all” regulatory legislation and associated operating regimes, which puts Australia clearly outside the domain in which Western democracies typically operate. This is demonstrably not in Australia's national interest.

As well as inheriting the problems embedded in the obsolete US ITAR/CCL system, DTCA has added further problems of its own making by expanding the scope of the legislation well beyond that of the US ITAR/CCL and UK systems. The US ITAR and CCL lists were designed primarily for the purpose of regulating the commercial and government export of military and dual use goods. ITAR and CCL were not designed to regulate “fundamental research” in academia or industry. Because DTCA hybridises a much wider scope of intended roles with its Defense Strategic Goods List (DSGL), which itself is a hybrid of the US ITAR/CCL lists, it is doing significant damage to the competitiveness of Australia's research and industry sectors.

In short, whatever good the DTCA might be doing by denying the export or re-export of controlled technologies to unfriendly regimes, this is clearly more than offset by the damage the legislation is doing to Australia’s research and development activities, and to public discourse on military strategy, policy and technology.

Some features of the DTCA are also especially perverse. For example, the exemptions applied to various Commonwealth agencies and personnel create situations where the Commonwealth is free to gain access to anyone’s IP and trade secrets, simply because these are not properly protected from exploitation or improper disclosure by Commonwealth entities, or personnel employed by the Commonwealth. In the US ITAR system, public servants are subject to the same controls and penalties as everybody else. The asymmetry, unique to DTCA, makes it very difficult to convince US entities to outsource work to Australian contractors, consultants or research entities, as any Non Disclosure Agreement (NDA) entered into may not be honoured – the Commonwealth may violate any such NDA with impunity and carry no liability for damages.

Furthermore, the DTCA’s expanded scope to regulate research and publishing activities beyond the scope of ITAR/CCL is especially destructive, as almost anything that is common knowledge in specialist research areas could be construed by the regulator to be in breach of any number of the “catch-all” (D) and (E) clauses in the DSGL. Thus, an APA submission to a US Congressional body surveying foreign technology developments would have to be twice the length it would be without the DTCA, and take twice as long to research and write. Every element drawn from the public domain would have to be shown by citation to be already public knowledge, lest it be misconstrued by the regulator to be original thought, and thus in criminal breach of the DTCA.

Ultimately, the hybridisation of the US ITAR/CCL with the broader objectives of the DTCA makes the determination of what is criminal an unchallengeable and arbitrary exercise by the DTCA regulator's administrative personnel. Submitting any and all open source publications dealing with military technology to the DTCA regulator for censorship is also the regulatory regime employed by the Russian Federation, and is fundamentally different to the US or UK models.

APA articulated this problem in its 2016 submission to the Senate Standing Committee on Foreign Affairs, Defence and Trade (refer Annex D), thus:

“Publishing or disclosing to the public any of the type of forensic analytical research that APA has performed, using public open source materials, could be arbitrarily and unilaterally deemed by defence officials to be a criminal offence under 14A (1) and (2).”
The requirement, under the 14A (3), for Ministerial Approval to disseminate any such material makes any effort to continue such research and publishing non-viable.

The monetary/time costs of defending against an allegation by a defence official that the Act has been breached, even if the publication only disclosed that what was previously published overseas, are too prohibitive for a non-profit volunteer organisation like APA to carry.

Given the current Defence culture, the expectation that some if any senior defence official could act as impartial and objective censors under 14A (3) is at best optimistic.

The track record of senior defence officials since 2003 displays a consistent pattern of muddling public discourse on Defence Matters with vendor propaganda, ideologically motivated beliefs, errors of fact, misleading distractions, and simple nonsense, the intent of which invariably appears to be distraction of Parliament, media and public, to draw attention away from prior mistakes or erroneous advice to governments by senior defence officials.

The observed track record in public statements by senior defence officials reflects the policy within the ADO of misconduct being defined as that what “brings the reputation of an individual, a group or organisation [in the ADO] into disrepute”. Therefore hiding any adverse realities that might bring the ADO into disrepute is considered “Appropriate Conduct”, no matter that doing so might be unethical, dishonest or unlawful.

Put bluntly, Defence are confronted with implicit conflicts of interest if they are to act under the DTCA as a censor of all public discourse in DSGL matters, as defined by 14A (3) of the DTCA. Defence personnel tasked with censoring third party publications that might by their analytical content expose shortcomings in Australian capabilities will be compelled to censor out or disallow such content, or be subject to internal allegations of misconduct.

This problem is further compounded by the obvious deskilling within the Canberra based agencies of Defence; especially in performing critical, independent forensic technical assessments of military technologies, foreign and domestic, then determining its importance.

On the ToR question of “whether the Act is fit for purpose”, the answer is, for these reasons alone, a resounding NO. Moreover, the legislation produces a wide range of other problems that were explained in earlier submissions by other parties, as well as APA and a number of its contributors, the latter included here as Annexes A, B, and C.

On the second ToR question of “whether there are any gaps in the Act’s controls”, the exemptions to the DTCA that apply to Commonwealth personnel are a gap of immense proportions that itself creates widespread problems. If Australia is determined to emulate the Russian Federation's propensity for “catch-all” legislation, in which criminality can be determined a posteriori by arbitrary interpretation of regulatory clauses, then the DTCA should apply to everybody, including the APS, and especially to Defence, its personnel, and its in-house contract personnel.

On the third ToR question of “whether any unintended consequences are resulting from the Act’s controls”, other parties, and APA elaborated on this subject in multiple previous submissions to the Senate Standing Committee on Foreign Affairs, Defence and Trade. Every single one of the “unintended” consequences APA identified has now materialised with varying severity.

To date no amendments have been made to the Act to address these “unintended” consequences.

The material impacts of the “unintended” consequences are also abundantly clear to APA in the severe restrictions that now apply to the organisation's research and publishing effort, knowledge of two export orientated defence sector consultancies that have closed down operations, and knowledge of a third where the proprietor has migrated permanently to another country and has no intention of returning.

Australian talent is now either idle, applied to those limited areas outside the coverage of the DTCA, or has relocated permanently overseas.

On the final ToR question of “any other matters considered relevant”, the restrictions the DTCA imposes on publishing have seen a significant collapse of publishing effort in areas subject to the DTCA, markedly reducing the quality of public discourse on defence topics in Australia.

The public debate on defence related matters in Australia, especially in technology and technological
strategy, is now at the same level of dysfunction as that now observed in the Russian Federation. This should not come as a surprise, given that the DTCA appears to be modelled on various well publicised items of legislation employed to regulate public discourse in the Russian Federation. If Australia chooses to apply the same philosophy to the design of its legislation as that employed by the Russian Federation, then Australia should expect the same outcomes.

To place this in the broader context of the defence and security domain, arbitrary “catch-all” regulatory measures such as the DTCA create unbounded potential for improper use to suppress or inhibit public discourse that is critical of the performance of government agencies. The old adage about the misuse of the classification system, where classification is misused to hide mistakes, applies: “Confidential = Embarrassing, Secret = Very Embarrassing, and Top Secret = Very, Very Embarrassing”.

RECOMMENDATIONS

As APA stated to the Senate Standing Committee on Foreign Affairs, Defence and Trade five years ago, “neither ignore the message nor shoot the messengers”.

“Embrace the opportunity this legislation and the resulting critical debate have created to derive and determine a better way of achieving the fundamental aims of the DTCA 2012 without the unintended consequences or potential for misuse and abuse.”

“Engage those subject matter experts who have demonstrated that they are focused upon leaving Australia in a better condition than they found it to assist in achieving this aim.”

In a period of intense global and regional strategic competition, where national technological capabilities, and public discourse on related strategic matters are of critical importance, the DTCA in its current form is not serving the national interest and must be amended to address its shortcomings.

Annexes:

A. Submission 7, SFADT, February 2013;
B. APA Discussion Paper 2013-0801, August 2013;
C. Submission 39, SFADT, March, 2015;
THE UNINTENDED CONSEQUENCES
OF
THE DEFENCE TRADE CONTROLS ACT 2012
by
Air Commodore Edward Bushell RAAF (Rtd) and Mr Peter Goon, USNTPS (FTE)

EXECUTIVE SUMMARY

In his final speech as the 34th POTUS, Eisenhower talked about the need for balance:

“Good judgement seeks balance and progress; lack of it eventually finds imbalance and frustration.”

34th POTUS, Dwight D Eisenhower, 1961

The POTUS Executive Order 13526 on Classified National Security Information for protecting American sovereignty contains means for achieving balance while it sets prohibitions and limitations for avoiding and countermanding unintended consequences or the misuse and abuse of the system.

No such balance let alone bulwark against unintended consequences or even against the potential for misuse and abuse of the system exist in the ITAR statutes and regulations, or in its inflated Australian sibling, the Defence Trade Controls Act of 2012.

Dissembling confabulation would be a polite, if not understated way to describe the way such well intended but flawed legislation risks being hijacked and manipulated by those whose only perspectives are profit and personal agendas, devoid of any national interest.

The unintended consequences, and those arising from misuse and abuse of the current Act, are outlined in this submission. The overarching view is summarised by these words.

“We cannot mortgage the material assets of our grandchildren without risking the loss also of their political and spiritual heritage. We want democracy to survive for all generations to come, not to become the insolvent phantom of tomorrow.”

34th POTUS, Dwight D Eisenhower, 1961

“I believe... each generation of Australians is obliged to leave our country in better shape than they found it.”

Prime Minister John Howard, July 2004

Sec. 1.7. Classification Prohibitions and Limitations.

(a) In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:
(1) conceal violations of law, inefficiency, or administrative error;
(2) prevent embarrassment to a person, organization, or agency;
(3) restrain competition; or
(4) prevent or delay the release of information that does not require protection in the interest of the national security.
(b) Basic scientific research information not clearly related to the national security shall not be classified.

POTUS Executive Order EO 13526 dated 05 January 2010
INTRODUCTION

In reviewing the Bill that has is now law, the Senate Committee exercised its Oversight Level of Governance responsibility well when it criticised Defence for its lack of proper consultation and transparency, leading to an inadequate identification of the Bill’s impacts.

However, the unintended, if not unforeseen, adverse impacts of the Act are so wide and pervasive that it will be difficult, if not impossible, for a ‘person’ thought by Defence to be subject to the Act to determine if, indeed, they are subject to the Act, and, if so, whether or not their current activities might be in breach of the Act, irrespective of whatever Defence’s interpretation of the Act might be on any particular day and in any particular circumstance.

This submission explores the wide range of problems, some that are very well known and some that are not so well known, about the function and operation of the United States ITAR legislation within the United States, upon which the Act is based. More specifically, it examines the far more extensive problems that are implicit in the Defence Trade Controls Act 2012, which will generate, quite unnecessarily, a wide range of adverse impacts on the Australian community if this legislation is implemented over the coming year.

The development of this Act also raises questions about the current effectiveness of our system of governance, as the passing of this clearly defective piece of legislation reveals a failure at all three levels of governance, due in large part, to a lack of vital competencies, principally, at the Executive and Directing Governance levels – that is, within the executive of the Department and the directing level of the Defence Portfolio, itself.

THE TECHNOLOGY PROLIFERATION PROBLEM

Proliferation of advanced weapons systems together with the technology sectors needed to develop, produce and maintain them, are major aspects of the current strategic landscape. This has become most evident in the global export of Russian, and more recently, Chinese technology that now spans the whole gamut of modern weapon systems, including stealth, radar, electro-optical sensors, data links, guided weapons, including cruise missiles, sensor fusion software, sonar, space technology, satellite navigation technology, unmanned vehicles and associated robotic technology, electro-magnetic weapons, lasers and a plethora of other technologies, advanced as well as fundamental.

A parallel problem that has existed since the 1940s has been the proliferation of Weapons of Mass Destruction (WMD), encompassing nuclear, biological and chemical weapons technologies.

The outstanding performance in this domain over the past decade has been the remarkable technological growth observed in China, which took full advantage of the bankruptcy of post-Soviet Russia, as well as the absence of any technology controls, to buy out significant portions of the Soviet/Russian military technology base, especially in the key areas of aerospace and missile technologies. The Chinese procured not only complete weapons systems, but also basic technology and manufacturing technologies across a wide range of technology sectors. Where technology transfers were constrained by Russia, the Chinese reverse engineered the technologies that it had procured, the most prominent example being the Sukhoi T-10 Flanker series of fighter aircraft, for both land based and aircraft carrier operations.

Chinese advances via the Russian technology base have also been reinforced by the acquisition of Western technologies, often via lawful commercial means, but also notably
through unlawful means. The propensity of Western nations to outsource their productivity to China (and other Asian nations) has been a major contributor to the former while greatly facilitating the latter.

A compounding factor has been the rapidly expanding flexibility of modern digital technologies, and more recently, the development of advanced monolithic microwave technologies, both of which have wide uses across both civil and military applications. Not widely known is that Russian built Agat digital missile seekers (many exported to China) are built around the ubiquitous Texas Instruments signal processing chip, a mainstay in Western radar equipment. It is also not widely known that the advanced Russian Surface to Air Missile systems employ data processing components built around the Silicon Valley developed Sun Microsystems SPARC microprocessor chip architecture.

The import of the technology proliferation problem has been that the long standing monopoly held by Western nations in high technology non-nuclear weapons, and their supporting technology sectors, has been largely eroded, if not lost in many areas, over the past decade. Western nations now maintain a credible lead in only a few areas of solid state radar technology, stealth materials technology, imaging technology and computer and networking technologies. Any such lead is now being eroded, and rapidly.

The long term trend is not encouraging, either, due to the persistent fiscally driven reduction in research and development funding across Western nations in most of these technology areas; be it University research funding in basic and applied technology, or industry and government laboratory funding in applied technologies. At the same time, a significant growth, over the past 30 years, in the Chinese university sector, especially in science and technology education and research, has been observed.

At some point over the next decade, under current trends, the Chinese will close the remaining gaps with the West in their key military technologies.

The import of this is that the strategic military advantage held by Western nations over China, Russia, and their numerous client states, by virtue of having a significant lead in high technology military capabilities, will be lost.

Technological arms races and competitive races in commercial technologies, broadly follow the same pattern seen in attrition warfare, which is described by Lanchester’s Laws of “strategic competition”, originally published in 1916, and used very successfully through the twentieth century against the WWII Axis, and later the Soviet Bloc.

The key dynamic in technological races is the ability to replace obsolete or matched technologies with new technologies, in a manner that parallels the replenishment of attritted forces by replacement forces in attrition warfare. The side which can develop and deploy new technologies sooner than its opponent will eventually prevail, and Lanchester’s differential equations show that the side that gains an advantage will eventual attrit its opponent out of existence, at an ever increasing rate.

This dynamic was central to key twentieth century military technological contests, good examples being during the latter phase of the Second World War, and later throughout the Cold War. The same dynamic has been observed repeatedly in the globalised computer and communications industries, where manufacturers that gained a lead typically displaced their early competitors completely.

In terms of the current global technological race, the only manner in which Western
nations can maintain a lead over Russia, China and other emerging players, such as India, is to develop and deploy new technologies faster.

However, the current preference throughout Western policy circles to opt for highly restrictive regulatory regimes, rather than invest in science and technology research, while supporting science and technology education, cedes the advantage in technological competition decisively to those nations that are not constrained by such regimes, particularly China and Russia.

Combining this preference with the rise in the influence of the Dunning-Kruger Effect within the senior levels of many if not most of the Departments and Ministries of Defence around the Western world with their resulting proclivity for institutionalising groupthink and beliefs in “a total indifference to what is real” will ensure the West’s and, in particular, America’s ceding technological lead and advantages to others.

THE REGULATORY PROBLEM

The imposition of government controls over research areas with military applications has a long and colourful history, with many prominent examples observed during the two twentieth century world wars, and the Cold War that followed. The original CoCom (Coordinating Committee for Multilateral Export Controls) evolved into the current US ITAR (International Traffic in Arms Regulations) system, while the Soviet’s extensive export controls were managed by their Ministry of Defence.

The intent of all such control regimes was to prevent opponents in a technology race from gaining access, thus forcing them to invest resources in developing domestic alternatives. The rationale was that a control regime can or might slow down the rate at which an opponent can match, or overtake, one’s own technology development and deployment.

This “blockade” approach has typically failed over time, as the party or parties under blockade tend to develop indigenous alternatives as substitutes. A good example was the successful South African effort to bypass technology and energy sanctions imposed by the US and European nations.

The CoCom regime proved to be only of limited effectiveness, due to repeated penetration by foreign intelligence agencies, and the capture of intact military equipment which was subsequently reverse engineered by opponents. Notable, mainly Cold War examples, include:

1. Penetration of the Manhattan Project by Soviet intelligence;
2. John Walker compromising US Navy cryptographic equipment to the Soviets;
3. The export by Toshiba and Kongsberg of numerically controlled machine tools to the Soviets between 1974 and 1984;
4. The extensive Soviet Directorate T / Line X technology collection effort in the West;
5. Post-Shah Iran selling US equipment, including the F-14/AWG-9/AIM-54 weapon system to the Soviets;
6. Capture of Soviet Surface Air Missile and radars systems in the Middle East and Africa, and Lt. Victor Belenko's defection to Japan with a MiG-25P Foxbat fighter;
7. Adolf Tolkachev at Phazotron compromising key Soviet radar and missile technology to the West;
Despite an increasing commitment in time, effort and cost, the ITAR regime introduced in 1994 has also had only limited success in slowing down Russian and Chinese technological growth, for a number of reasons, while incurring severe and adverse impacts upon US industry and research organisations.

Failures in “containment” include a multiplicity of widely publicised violations by commercial organisations manufacturing defence equipment or providing services. Successful HUMINT and cyber operations by China, and the increasing attention being paid to the narrowing gap between commercial and military technologies in a wide range of areas, have also contributed to serious breaches and failures of the containment policy.

A good example of this is the scale and scope of the technology containment failures arising from the alleged cyber-penetration of defence contractors in the F-35 program which remains to be fully explained, and may in fact never be explained\textsuperscript{xiii}.

While the absolute effectiveness of the ITAR regime as a legitimate containment mechanism may be open to debate, its adverse impacts on the United States industry and research communities are not, since they are real, present and self evident\textsuperscript{xiv}.

Problems experienced by the US industry include:

1. A significant administrative overhead in tracking products, documentation and associated intellectual property which falls under ITAR;
2. Significant time delays in seeking approvals for ITAR listed products;
3. Significant costs incurred in re-engineering products which may contain components, materials, processes or other intellectual property falling under ITAR\textsuperscript{ xv};
4. Significant security infrastructure costs, and recurring operational costs, ensuring that any material falling under ITAR is treated not unlike classified materials;
5. Constraints on employing engineering talent lacking US citizenship;
6. A competitive disadvantage in bidding against non-US manufacturers offering “ITAR-Free” products, unencumbered by ITAR, especially where the client is seeking technology transfers; and,
7. A dumbing down of Industry, their Customers and those responsible for managing as well as oversight of the associated activities due to significant reductions in diversity, competition, skill levels and critical debate.

There are no current studies that have quantified or qualified the scale of the commercial damage experienced across the entire US industrial base as a result of the cumulative impacts of ITAR. However, some technology sectors have been able to identify a marked causal deterioration in the US technology base.

In evidence to the House Committee on Science and Technology, in February, 2009, Major General Robert Dickman, (USAF, Ret) Executive Director of the American Institute of Aeronautics and Astronautics observed that “We all understand the reasons why our export control policies were put in place. We have enjoyed technical superiority from decades of investment in education and RDT&E, and from producing and attracting generations of the best intellectual talent pool the world has ever seen. To maintain that superiority, these policies were established to insulate our advantages from the rest of the world, and specifically from regimes that maintain a different and adversarial worldview from our own.....we need to make a realistic evaluation of how these policies are being
implemented, and what effects they are having. We need to be willing to act if these policies are falling short, if these policies have become detrimental to our goals. Today, the reality is that these policies are counterproductive to their stated objectives...Without a change of course, we will certainly witness dramatic changes in our competitiveness and level of superiority. We are really talking about generational effects, well beyond five years.\textsuperscript{xvi}

Maj Gen Dickman’s observations on the impact of “ITAR-free” marketing are also important: “ITAR-free” marketing is designed specifically to compete with U.S. systems and components with contracts that have much less regulation, and can be completed in a much shorter timeline. These are policies developed specifically to make the European manufacturers a more attractive alternative to U.S. industry and the marketing has been very successful, even for almost purely commercial products. The effect has been a dwindling U.S. industrial base largely dependent on government contracts to keep production lines open.”

The damage already done to US industry’s advanced system technology sectors, as well as the US education and research sectors, reflects the realities of trying to manage a complex list of technologies in a rapidly evolving environment, where technology is often not exclusively available to the US.

In 2007, Lt Gen Brian Dubie, Chair of the Aerospace States Association, observed that: “The current regulations allow export licenses to be granted when a part is available commercially elsewhere in the world. In fact, the very existence of what Thales calls its “ITAR Free Satellite” suggests most satellite parts no longer belong on the list of prohibited exports. A re-evaluation of the ITAR controlled technologies is critical to ensure U.S. competitiveness and jobs.”\textsuperscript{xvii}

He also stated that: “On a panel at the 58th International Astronautical Congress held this fall in Hyderabad, India, Ray Williamson, a research professor at George Washington University’s Space Policy Institute in Washington, stated, “In the long run ITAR is going to be destructive of U.S. industry.”

These problems will only continue to increase in type and magnitude over time, as European, Russian, Indian and Chinese industry close the gap in a great many technology sectors controlled by ITAR, because many of these competing technology sectors are showing exponential growth. Simply attempting to maintain currency in the ITAR technologies list will require an ever increasing investment in time and effort by highly qualified research grade personnel to survey the global marketplace. Currently, technical surveys of advanced foreign weapons and systems technologies covered by ITAR are not well covered by either government or academic research in the USA, unlike during the Cold War era when considerable and ongoing intellectual effort was invested.

The fundamental paradigm implicit in ITAR is that complete or substantial knowledge of opposing technologies is both available and current, but this is no longer the case.

A good indication of the damage inflicted by ITAR in the “dual-use” category lies in the domain of space technology. The January, 2012, Aerospace Industries Association report titled “Competing for Space:

Satellite Export Policy and U.S. National Security” states: “We surveyed AIA members this year on the topic of export regulations and the message was clear: outdated export controls are hurting U.S. companies. Data supports this view. The U.S. held 73 percent of
the worldwide share of satellite exports in 1995 – this fell to a staggering 25 percent by 2005. Today, U.S. law requires export agencies to still look at a nut, bolt, or screw for a commercial satellite and an anti-tank missile through the same regulatory prism. Clearly, it’s time for a change.”

Direct impacts on the United States’ education sector are less well documented, in part because the US ITAR system provides wide exclusions for “fundamental” research, a.k.a.:

“Fundamental research is defined to mean basic and applied research in science and engineering”.

Nevertheless, the US ITAR system includes strong compliance requirements on those US universities performing US DoD funded research involving controlled facilities, equipment and prior research materials xviii.

An example of a current constraint is that that some US academic organisations are required to divide research conferences into “ITAR-compliant” and “open” streams, applying the same types of controls as generally applied to military technical conferences, which are divided into “classified” and “unclassified” streams, and are further constrained in publishing research in areas which fall under ITAR controls xix.

This, at a minimum, doubles the time and effort required to manage a conference, and places security constraints on venues and facilities.

Another impact of serious concern is that the ITAR system imposes strong constraints on research staffing, and permissible choices of postgraduate students to work on research projects. This restricts the pool of talent that can be used, and inevitably slows down research by creating bottlenecks in recruitment.

Problems within the ITAR system are not confined to direct damage effects. A problem that has emerged, and will likely increase over time, is that of difficulties in prosecutions due to an inability of investigators to identify specific references in the mountain of technology and research data that is already in the public domain, and thus already exempt from ITAR controls xx.

In summary, there is sufficient evidence to observe, at this time, that the US ITAR regime has become limited in its effectiveness in containing technology transfers, while inflicting significant damage on the US national technology base, and increasingly on the US university technology and research sectors. This is a direct result of the basic paradigm employed, which was inherited from the CoCom system, which was designed around a “bipolar” technology race between the monolithic Soviet Bloc and the West. In a multi-polar world this model has become impossible to manage in a timely and robust manner, because it becomes increasingly expensive and over-demanding in specialist technological effort, increasingly damaging to research, industry and academia, and, as a result, will become increasingly ineffective.

Every dollar expended on ITAR controls is a dollar not spent on advancing US national security and industry via Research and Development investment, and similar impacts must be expected by all other nations following ITAR as it stands. In a globalised multi-polar competitive technology race, this is ultimately suicidal.
The DTC Bill 2011 passed through the House of Representatives in Australia on the 30th October, 2012, and has since been legislated as the Defence Trade Controls Act 2012.

This regulatory regime is significantly more restrictive than the US ITAR regime, or the Cold War era CoCom regime, and best compares to what is known of the Soviet regulatory regime.

The legislation currently does not provide the same blanket exemptions for “fundamental” research, as defined by ITAR, which are a key feature of the US ITAR systemxx.

The exemption in the legislation for public domain “technology” is also unclear and problematic, as the Act puts the onus of proof on the defendant, rather than the regulator. If the agencies administering the Act lack the competencies to recognise that the “technology” is in the public domain, it may initiate unsuccessful and indeed superfluous investigations and actions at considerable cost to all parties. For parties publishing public domain “technology” within the scope of the legislation, there is a significant time overhead involved in proving that the “technology” is already in the public domain.

Citexxi:

12 14A Publishing etc. DSGL technology
13 (1) A person commits an offence if:
14  (a) either:
15   (i) the person publishes DSGL technology to the public, or
16    to a section of the public, by electronic or other means;
17   or
18   (ii) the person otherwise disseminates DSGL technology to
19    the public, or to a section of the public, by electronic or
20    other means; and
21  (b) the person does not hold an approval under this section
22    authorising the publication or dissemination of the DSGL
23    technology.
24  Penalty: Imprisonment for 10 years or 2,500 penalty units, or
25    both.
26  Exception
27 (2) Subsection (1) does not apply if the DSGL technology has already
28    been lawfully made available to the public or to the section of the
29    public.

Note: A defendant bears an evidential burden in relation to the matter in
subsection (2): see subsection 13.3(3) of the Criminal Code.

Where the DSGL is the Defence Strategic Goods List, the list contents being defined as:

DSGL technology.

technology relating to goods means:

(a) information relating to the design, development, production,
 manufacture, assembly, operation, repair, testing,
 maintenance or modification of the goods (including
 information in the form of blueprints, drawings, photographs,
 plans, instructions, specifications, algorithms or
 documentation); or

(b) software relating to the goods;

As the Australian legislation is modelled in part on the US ITAR regime, it inherits all of the
identified and well established problems and impacts inherent in the ITAR regime. However, it also contains the additional problems arising from the processes that will have to be developed for dealing with the Intangible Transfer of Technology (ITT) that arise via electronic means, such as email, Internet or digital storage devices.

The regulatory regime in the legislation will thus be more complex, extensive and expensive to administer than the ITAR regime due to its wider “blanket coverage”, and significantly narrower, and less defined exemptions.

Another problem fundamental to the establishment of the regulatory system is the endemic
and pervasive shortage of skilled personnel within the Defence organisation capable of
correctly assessing the intellectual content of documents which fall under the scope of the
legislation. An objective review of a research paper, or indeed any technical publication, to
establish whether it breaches the control regime is not an easy task in most instances, but
especially so where it involves leading edge technology, and public domain “technology”
collected from a wide range of sources.

In essence, the legislation is imposing a mandatory “peer review” process upon any and all
information transfers of “technology” within the scope of the DSGL, which encompasses
“information relating to the design, development, production, manufacture, assembly,
operation, repair, testing, maintenance or modification of the goods (including information
in the form of blueprints, drawings, photographs, plans, instructions, specifications,
algorithms or documentation)”, in effect anything which identifies or describes any aspect
of the item in question.

However, the peer review process within the academic system is hampered already in
many areas of science and technology by a global shortage of qualified reviewers, so the
notion that the Defence organisation can maintain its own pool of qualified reviewers, let
alone keep them current with the technologies, within Australia, whether these are
Defence personnel or external delegates, qualifies as a very courageous idea.

The resulting problems will be reflected in a much higher proportion of inappropriately
rejected applications by industry and academia, and in many instances considerable
delays will be incurred, whatever the outcome of the application might be.

Within the Defence organisation there has been a long standing and unstated policy reflected in the well known internal anecdote, which states “*When in doubt, classify it!*”.

Whereas, the overarching policy of the United States of America on National Security Classification (Presidential Executive Order No 13526 dated 05 January 2010) states:

“If there is significant doubt about the need to classify information, it shall not be classified”,

....and....,

“If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.”

The poleaxing contrast between what is the real policy versus the long standing, unstated policy that has contributed, *inter alia*, and significantly to the rampant deskilling and institutionalisation of the Dunning-Kruger Effect (a.k.a. dumbing down) observed in the Defence senior leadership group over the past decade or so, is deserving of its own Issues Paper. However, though closely related, any such detailed treatise is considered outside the scope this submission to the Senate for the simple reason that the Hansard records of both the Senate and House are already replete with example after example of this behaviour thus putting this phenomena into the category of being self evident.

What is also abundantly clear is that any cutting edge industry or academic research and development, which falls under the footprint of this legislation, or which sits on the boundaries of the legislation, will be unlikely to receive approval unless the authors can prove that the “technology” within the work has already been published overseas. The consequence of this is that both industry and academia are guaranteed to become “followers” in research and technology in these mundane areas. Innovation, so frequently trumpeted by both Defence and Education Departments, will become increasingly impossible.

A fundamental weakness within the legislation is that it fails to articulate the scientific criteria against which assessments should be made. In the US, reviewers performing assessments on what leading edge research and development “technology” can be disclosed are typically expected to ask the question: “Do potential or actual opponents already know this?” If the answer is “yes”, then there is no point in either classifying or regulating or otherwise controlling that information or “technology”.

Shortcomings in this specific area lie at the root of a great many of the problems seen in the US ITAR system.

The Australian Defence Organisation has a long and sad history of providing public statements and advice to Parliament and Government which demonstrate its lack of organic skills and expertise in this very area. Though the endemic deskilling that has occurred within the organisation is often used by senior officials as a reason to justify everything from budgetary blowouts and massive schedule delays in projects through to the need for more funds, little if any substantive fixing of the problem has been done. Technical and scientific intelligence analysis of foreign nations’ military technology is a capability which is almost non-existent within the entire Australian Defence Organisation.

In contrast, for example, Air Power Australia has well over a decade of experience in performing forensic scientific analysis of foreign military technology, especially Russian
and Chinese technology, with such analyses often including the reverse engineering of key performance parameters in such systems. Around 66% of this organisation's publications deal specifically with this problem, and such publications are widely used in the United States defense community as reference material for education, training and foreign capability assessments, because the material is open source and thus suitable for public release documents. This effort was invested specifically to plug the gap in unclassified reference literature detailing foreign military capabilities that resulted from the large scale, post Cold War reduction in US government research in this area, and the total absence of this capability within the Australian Defence organisation.

From its experience, Air Power Australia understands well that answering the pivotal question of "Do potential or actual opponents already know this?" requires significant scientific and engineering expertise and effort, and considerable experience as well.

The failure of the legislation to address properly the foreign capability problem reflects an almost complete absence of understanding within the Australian Defence organisation of this problem area. The belief within the Defence Organisation that this problem can be managed through administrative process rather than using a scientific/technology/strategy and engineering risk based approach reinforces this observation.

Defence's reliance upon administrative process to manage its force analysis and structure challenges, and its capability acquisition and sustainment functions, was reviewed recently by the Senate Foreign Affairs, Defence and Trade References Committee (ref), which found that the organisation had a flawed management structure, was overly dependent upon process, lacked the ability to manage risk, had confused or blurred lines of responsibility, ineffective accountability and a lack of the necessary skills and competencies, especially in strategic analysis, project management and engineeringxxii.

In fact, the lack of these skills and competencies were characteristic of all elements of the Department – the Department itself, DSTO, the Defence Materiel Organisation, the Services and throughout local Defence Industry. Such an organisation can hardly be considered competent to manage DTCA 2012.

**UNIVERSITY SECTOR CONCERNS**

Representations by the Australian university sector to the Senate inquiry on the draft legislation were heeded only in part, and so the legislation failed to properly address the manifold and legitimate concerns raised in multiple submissions to the Senate Committee on Foreign Affairs, Defence and Tradexxiii.

Amendments to the draft bill proposed by the Senate were not introduced. The only concession made was to permit a two year duration "no penalty" trial period to assess the impact of the legislation on the university sector, given that no significant effort was made to assess the impact of the legislation prior to its enactmentxxiv.

The considerably more restrictive nature of the legislation, compared to the ITAR system, and the differences between the Australian and US university sectors, will produce a significantly greater impact than observed in the US.

This reflects two realities. The first is that the US university system has, since the 1940s, received significant funding for basic and applied research in DSGL "technologies", and has well established mechanisms for segregating "open" and "ITAR controlled" research
activities. These mechanisms have not always operated well in the US, and there have been repeated failures in process resulting in prosecutions and convictions\textsuperscript{xxv}.

Another key difference between the US and the Australian university systems is size, and as a result, there is a considerably greater dependency in Australia on overseas research collaborations, and the use of foreign nationals in research activities. With China having now overtaken the US as our top ‘knowledge partner’, and with Australia’s wholehearted embracing of the ‘Asian Century’, the Bill will cause widespread mayhem throughout what is left of Australia’s teaching and research capabilities within academia.

What is abundantly clear is that without heavy tailoring and amendments, the new legislation will produce a significant and detrimental impact on University research in any areas which overlap the listed DSGL “technologies”, or are thought to overlap them. In some instances, the result will be cessation of all research in those areas.

The flow-on effect of this will be pervasive, as the university sector will have great difficulty in pursuing further research collaborations, will lose a great many researchers working in these areas, and will be unable to recruit researchers to work in those areas.

For example, the language used in the Bill, now the DTCA 2012, amounts, prima-facie, to censorship controls on all publishing on all topics covered by the DTCA, embracing:

- All open-sourced research on any topic related to DSGL technologies.
- All open-sourced research on any topic impinging upon military operations.
- All open-sourced research impinging upon military technological strategy, as this cannot be conducted in the absence of capability analysis.
- All applied research in areas of DSGL and related technologies.
- All submissions to parliamentary inquiries covering any matters involving defence operations, strategy or technologies.

Furthermore, the Bill as enacted lacks any definition of ‘person’, so the Act may (and will almost certainly) be construed as applying not only to ‘everything’, but also ‘every person’. A definition of ‘Intangible Technology’ also does not appear, nor is there a reference as to where such a definition might be found, leaving it open to legal interpretation.

The issues pertaining to open-sourced research and, more particularly, given its importance, today, open source intelligence analysis and the effect the now enacted Bill will have on these vital functions, is worthy of closer scrutiny.

**THE OPEN SOURCE INTELLIGENCE ANALYSIS PROBLEM**

In October this year the influential *Intelligence and National Security Alliance* (INSA) think tank in the United States published a seminal white paper entitled “Expectations of Intelligence in the Information Age”. The non-profit, non-partisan, public-private INSA is described as the “premier intelligence and national security organization that brings together the public, private and academic sectors to collaborate on the most challenging policy issues and solutions.” \textsuperscript{xxvi}
The paper performs a broad and deep study of the implicit problems and opportunities arising in an era where a globalised Internet and digital social media provide nearly instantaneous distribution of vast amounts of open source material covering almost any conceivable category.

This information includes a large amount of open source material which falls under the scope of the DSGL and ACTA. Good examples include millions of high resolution photographs of military equipment collected and disseminated by enthusiasts and professionals globally. Open source materials now available globally via the Internet include technical, operational and tactical manuals for Soviet weapons and missiles, flight manuals for combat aircraft, and other technical literature and materials covering the whole scope of the DSGL. Intentionally or otherwise “leaked” photographs from China provide and rich tapestry of the vast military technological advancement seen in that nation since the end of the Cold War. Google Earth and other providers now offer free access to high resolution satellite imagery of most developed nations, typically of better quality than many older military satellites, and easily exploitable for military use. Free services such as Google Translate permit rapid translation of publications in foreign languages, as a result of which foreign DSGL “technology” publications globally can be rapidly analysed and findings disseminated.

Globally the analysis of open source intelligence (OSINT), whether commercial, economic or military, has become a large scale activity by commercial and academic organisations, which now have capabilities in this area which typically surpass those of governments.

A notable example of OSINT which presented a major “capability surprise” in recent years was the analysis of China's vast network of thousands of kilometres of underground tunnels constructed as hides for ballistic missile launchers. This work was produced by Georgetown University students under the supervision of Professor Phillip Karber. The effort involved the analysis of many thousands of photographs published or leaked onto the Chinese Internet, Chinese media reports, and satellite imagery. A similar and earlier study by Air Power Australia, that informed the Georgetown study, and was performed collaboratively with OSINT researchers in US academia, found more than 40 Chinese “superhardened” airbases, equipped with underground hangars capable of protecting a large part of China's air force.

Other OSINT studies by Air Power Australia include the detailed radar signature analysis of Russian and Chinese stealth fighters, forensic technical analysis of advanced Russian and Chinese radar and missile technology, performed mostly in collaboration with academic researchers in the United States.

In Canada, researchers at the University of Toronto identified the large scale Ghostnet hacking network, involving penetrations of government facilities on a global scale, and continue to produce valuable research detailing cyber-operations globally.

The results of such OSINT research projects have been of enormous value, since they identify often strategically important developments, frequently not studied by government managed intelligence organisations.

These results may also be unpalatable to government organisations since they identify gaps, shortfalls or failings in their intelligence work.

The INSA white paper makes a critically important observation: “Given what is already an increased reliance on these new sources of knowledge and the likelihood that their use will
expand dramatically in the years ahead, the government (and Intelligence Community specifically) must be ever mindful that the rights of individuals are the very foundation of U.S. national security. While technology has transformed the world of knowledge, it has also introduced new challenges and threats to the security of the United States. **Going forward, it is imperative that U.S. laws and practices keep pace with this information revolution in a manner that respects privacy and civil liberties. This core value must be woven into the fabric of what one might call “open sourcing” of intelligence.**

Another important observation in the INSA paper is the changing character of intelligence collection and analysis in the “Knowledge Era”. The INSA points out that increasingly, the role of government intelligence organisations will be the validation of collected OSINT, rather than the Cold War era deployment of systems and operations to collect technical, strategic and operational intelligence in foreign nations, and then the analysis of this data.

Cite: “The light blue circles are meant to represent the “center of gravity” for intelligence collection, analysis, and distribution. Situated in the upper left hand quadrant, and fairly filling it, the light blue circle implies that historically, information—irrespective of source, method or sensitivity—was viewed and treated within the IC (Intelligence Community) and accepted by policy makers as secret. The light blue circle in the lower right quadrant acknowledges that historically neither the IC nor policy makers ignored information gathered from open sources—recall the Foreign Broadcast Information Service—but that such information was rarely delivered in an unclassified format to policy makers. Hence, that smaller circle resides closer to the crossover point between classified and unclassified information.”

**Source: ISNA**
The INSA is entirely correct in its assessment, in that OSINT is becoming a critical “centre-of-gravity” in the current practice of intelligence collection and analysis.

In Australia, the DTCA by intent or otherwise, closes down all OSINT technical intelligence collection, analysis and dissemination, as most such effort involves “technologies” covered by the DSGL, and collaboration with overseas foreign nationals. An OSINT analyst is exposed to prosecution, unless foreign sources are disclosed, for violations of the prohibition on “Intangible Technology Transfers”, in an environment where these foreign sources could be exposed. No differently, an OSINT analyst is exposed to prosecution, when publishing results of collection and analysis, should these be seen to overlap or agree with classified or controlled data held by the Defence Organisation. Should the OSINT analyst submit work to the Defence Organisation for approval, it may be simply disallowed if the findings of the work yield any discomfort or embarrassment to the Defence Organisation, on the basis of “national interest” or “foreign relations”.

This confines all future OSINT effort in the DSGL domain to citing foreign publications, and avoiding all and any critical analysis or discussion, which could be misconstrued to represent or be indicative of an offence under the Act. The result of this is that Australia loses the increasingly valuable results of public domain OSINT collection and analysis. These problems simply do not arise with the US and UK legislation, due to their fundamentally different approach to what information is and is not controlled.

REVIEW OF THE BILL PRIOR TO BECOMING LAW.

The obvious deficiencies embedded in the Bill proposed by Defence became the subject of a Senate Committee Inquiry which, after several unsuccessful attempts to have Defence consult meaningfully with Industry and Academia on perceived adverse impacts of the Bill, the Committee concluded:

“The committee is disappointed with the consultation undertaken by Defence in regards to this bill. Evidence provided to the committee demonstrates that the consultation conducted by Defence was started too late in the process; lacked transparency; and was not conducted in a way which encouraged consensus in solving the policy problems at hand. The committee draws Defence’s attention to the issues outlined in this (the committee’s preliminary) report.”

Independent analysis of the Bill supports the Senate Committee’s reservations, and some of the more important observations from that analysis follow.

The Explanatory Memorandum

The key document presented to Parliament in support of the Bill is the Explanatory Memorandum, circulated under the authority of the Minister for Defence. Within that document, the key section is that providing a form of Regulation Impact Statement (RIS) “examining proposals to implement a strengthening of the existing defence export controls”, including “a high level impact analysis of the Treaty for the benefit of readers who have an interest in the Treaty implementation. The Department of Defence will conduct a detailed analysis during the required Treaty Post-Implementation Review.”

Analysis of the Memorandum gives rise to the view that it does not present a full and true statement of the adverse impacts of the Bill in its current form, and fails to identify the
widespread risk to Australia’s long-term national security that will stem from those impacts.

In short, Parliament has approved a Bill that, if not amended promptly, will only contribute to the continued loss of Western competitiveness militarily, industrially and academically, and so will weaken rather than enhance Australia’s national security.

**Matters of Concern**

**Financial Impacts.**

Financial provisions for Defence to implement and administer the Bill have been made but are not given, nor is there any estimate of the costs that will fall to Defence activities such as capability planning and research, capability acquisition and sustainment, DSTO activities, Services’ activities, or Industry (defence and non-defence) or Academia costs. Industry has been waived aside with the statement that “The impact could be small depending on whether businesses have sound business processes.” In regard to Academia, Defence has no statistical data available on research programs or foreign researchers or students, but concludes that there should be minimal impact on university courses or research partnerships. Finally, Defence was unable to provide any net benefit to the Australian Community from the Treaty.

In short, Defence, knowing the impacts of ITAR in the US, and the manner in which the UK dealt with their ITAR problems in academia, should have been able to do a much better job of identifying and scaling the impacts of the Bill. As it stands, the Parliament, on behalf of the people of Australia, have signed a blank cheque for this new Act.

**Principles Behind the New Controls.**

These have been identified as:

- International Obligations.
- Human Rights.
- National Security.
- Foreign Policy.

Surely, the Bill should focus upon Australia’s national security, in the first instance, with all other factors forming part of our national security planning.

**Central Role of the DECO.**

The question already raised above is where Defence (DECO) will get the range and depth of technological skills and competencies needed to judge complicated questions about the military end use of both tangible and intangible materiel (e.g. equipment and information). Defence has been unable to manage its current responsibilities through a lack of required skills and competencies, so the likelihood that ITAR matters will be managed efficiently, effectively and economically is just not plausible, let alone feasible.

Furthermore, the plan to refer reviews of ministerial decisions to the Australian Administrative Tribunal, where the lack of technological competencies will be even greater, is baffling.

**Legislation Consultation with Industry.**
Much is made of the consultation conducted with Industry, but the net result was that only two comments were received by email, and four bland ‘main themes’ arose from the consultative workshops. This matter has been dealt with by the Senate Committee, but the reason for the total absence of meaningful feedback has not been forthcoming. Perhaps it was as a result of pressures from Defence for Industry to conform or face consequences, in keeping with the now entrenched attitude in the DMO and Defence at large so starkly demonstrated, recently, before the Australian Parliament.

Mr Dunstall: . . . . Normally in Commonwealth negotiations it is the Commonwealth against the little guys.

Senator MARK BISHOP: The Commonwealth against???

Mr Dunstall: The little guys. There is the big Commonwealth and 'if you want to do deals with the Commonwealth you basically accept our terms and conditions or you do not do business'.

Coupled with the impacts of the savage cuts to the Defence Budget on Industry, the DTCA will only hasten the closing down of European and other non-US nations’ defence contracting activities in Australia, driving Australia to rely overwhelmingly upon US defence contractors.

Legislation Consultation with Academia.

This subject was also covered by the Senate Inquiry, and has been discussed above. While Defence makes the claim that Academia will suffer minimal impacts, the Memorandum tries to make the case that the UK has encountered no significant adverse impacts. However, it is also noted that the Memorandum fails to advise that the UK amended their equivalent Export Control Act to include Sections 8 and 18, expressly to preserve and protect its University Sector.

No intention to consult widely and meaningfully with either Industry or Academia can be identified.

THE PROBLEMS WITH GOVERNANCE

Background

To date, discussion surrounding the Bill has centred mainly upon:

- Identifying the widespread problems that will materialise as a result of known problems with the US ITAR legislation that formed the basis of the Bill, now enacted legislation as the DTCA 2012.

- The additional, and even more widespread, impacts that will materialise from the blanket, ‘catch-all’ regulatory requirements that have been added to the Bill, particularly those relating to the transfer of both tangible and intangible technology.

- The failure by Defence to conduct meaningful consultation with those most affected, especially Industry and Academia.
• The inadequacy of the Regulation Impact Statement in providing important financial and other impacts, and the lack of any assessment of the net benefit of the Treaty to the Australian Community.

However, notwithstanding the procrastination in Defence’s protracted inability to resolve these problems, and the Senate’s proposal to delay the Bill until the problems had been resolved, Government saw fit to enact the Bill, thus ensuring that all the known as well as highly probable and even low probability risks, will materialise. Sorting these out post-implementation will be a long, complex, confusing, expensive and quite unnecessary workload – a task well beyond Defence to manage.

In short, this was a Bill that should not have been passed into law, and those following the Bill’s journey may now well ask, “How could this have come about?”

The Problems with Governance.

Analysis of the manner in which the Bill has been processed suggests that the primary cause of the problems identified lies in a chain of failures linking all three levels of Australia’s system of governance – the Executive, the Directive and the Oversight.

The First Failure of Governance.

The first failure occurred at the Executive Level of Governance – within the Department of Defence Executive, which comes under the responsibility of the Secretary and CDF. It was here that it may reasonably be assumed that the need for the Bill, its scope, and its application, its impacts and its implementation were determined. It was thus here that:

• Problems identified with the US ITAR legislation, which forms the basis of the Bill, were ignored.

• Provisions made by the UK in its equivalent legislation for the protection of Academic and Research sectors were ignored.

• Only a sham consultation process was conducted with Industry and Academia, with important academical reservations ignored and Industry briefed on policy, but not the implementation process where the adverse impacts were hidden.

• Most importantly, a decision was taken to broaden the scope of the Bill (as reflected in the DSGL) to go well beyond the US ITAR system, which will be found to be excessive, destructive and quite unnecessary.

• The decision was taken to include a very limited RIS in the Minister’s Explanatory Memorandum, one lacking in information that could give confidence that the Bill was sound or, in keeping with need for due diligence, show the opposite to be the case.

The draft Bill was then referred to the Minister for his acceptance and presentation to Parliament.

The Second Failure of Governance.

The second failure occurred at the Directive Level of Governance, for which the Minister has responsibility, being solely accountable to the Parliament for the proper management of his Department, and thus the quality of the Bill being proposed. It is not known whether
the Minister saw fit to amend the Bill or not. While the Minister has subsequently assured parliament that wide and lengthy consultation had been undertaken, the fact remains that his Memorandum and the Act stand starkly deficient in requirement, impacts, risks and costs, and reads more like the result of an omnibus (consensus)–driven administrative/sales-marketing process during which any ‘good (sounding) idea’ was included and ‘everything covered, just in case’.

The key fact is that the Bill forwarded to Parliament contained all of the problems identified above, and the Minister must carry primary governance responsibility for them from wherever they came.

The Third Failure of Governance.

The third failure occurred at the Oversight Level of Governance which is exercised by Parliament on behalf of the Australian people. Here, the Bill was examined by a Senate Committee and was, in effect, not recommended for enacting in its present form. However, rather than allowing the Senate to exercise its Parliamentary oversight governance function, Government enacted the Bill arbitrarily with all its known and suspected problems.

Why Government acted in this way has not been explained, but it might be assumed that it saw its primary obligation to the US rather than Australia’s national security.

The Root Cause behind the Failures in Governance.

At the Executive Level of Governance, the adverse impacts embedded in the Bill may have been conscious, which may in part be so, but they were more likely to have arisen from a lack of relevant skills and competencies within the Defence Executive. This probability is enhanced by the evidence given before, and the findings of, the Senate Foreign Affairs, Defence and Trade References Committee Inquiry into Procurement Procedures for Defence Capital Projects. This inquiry highlighted a wholly inadequate level of required competencies, especially in strategic analysis, project management, risk management, and engineering (technology) across all elements of the Defence Organisation, including DSTO and DMO.

As a result, decisions were being taken in Defence by both civilian and military staff lacking the requisite competencies. This situation may be traced to the purge of competent staff during 1999 to 2002, when skilled civilians and military people were replaced by unskilled civilians and military people who were required to adopt a culture of institutionalised conformance and compliance with the wishes of the Minister, as interpreted by senior management in the Department. The resulting behaviours seen throughout the Defence organisation are entirely consistent with the Dunning-Kruger Effect, typically over confident and consensus based, rather than providing well-informed and reasoned decisions, and exhibiting an overt hostility to countervailing or differing perspectives on problems and their solutionsxxvii.

These characteristics are also reflected clearly in the content of the Bill and the behaviours exhibited by Defence during the ‘consultation’ process, as well as before the Hearings of the Senate Inquiry.

The challenge is thus not limited to sorting out the problems embedded in DTCA 2012, but also reinforcing the chain of governance by ensuring that the Executive Level in Defence is staffed by people having the required skills and competencies.
Unfortunately, the Dunning – Kruger Effect is not limited to the Department of Defence. It may be seen in every government department, as evidenced by the chronic problems being encountered with policy decisions being taken by government, but implementation just not thought through, and so consigned to failure from the start. The root cause for these continual failures is simply a lack of required competencies within departments, coupled with an inappropriate emphasis upon ‘social inclusion’ and ‘cultural’ approaches, framed in a way akin to the classic marketing/sales culture devoid of technical literacy and Scientific/Engineering integrity.

AUSTRALIAN SME INDUSTRY CONCERNS

Deskilling is one of the biggest challenges before our Nation, today.

One of the more insidious characteristics of the levels of deskilling in Defence, increasingly over the past decade and currently today, is the tasking and empowerment of individuals in the DMO and Canberra based elements of the Defence organisation who don’t know what they don’t know and have little understanding of the matters for which they have been made responsible.

In other words, the system is tasking people to undertake duties and activities for which they have neither the background, knowledge, training, experience nor expertise to perform, let alone perform effectively. The Dunning-Kruger Effect is now institutionalised within the DMO and rampant in other Canberra based elements of the Defence Portfolio.

Though personal professional integrity should and must be paramount in any endeavour, this is not, in the first instance, the fault of the individual so appointed and tasked, but of the Defence management system which, since the Great Purge in Defence of 1999-2002, has actively pursued and promoted mediocrity as the norm through a sales/marketing culture based approach devoid of technical literacy or the integrity that comes from the rigorous application of ethos and methods of Science and Engineering.

One of the larger effects of the application of this sales/marketing culture approach that has been followed for over a decade, now, is evident in the dwindling membership of the group known as the Australian Defence Industry SMEs.

There can be little doubt that the Australian owned and operated sections of the Defence Industry, principally small to medium size enterprises (SMEs), are now at the top of the endangered species list.

This situation has been coming for over a decade; since the formation of the DMO and the adoption of “the Primes’ Policy” wherein the DMO chooses to focus on prime contractors and expects SMEs to be subordinate and responsive to the Primes with little if any consideration that anyone who has a fish aquarium knows instinctively; namely, you don’t put the little fish in with the big fish!

This policy has both written and un- written elements, the latter being empowered by attitudes generated by the former which result in behaviours that typify those associated with the misuse and abuse of power, authority and trust.

In failing to ensure Defence and the DMO fully adopted the Strategic Policy of Defence and Industry of 1998 and its ethos of partnering with the Australian Defence Industry and
providing this Industry with ‘a fair go’, successive Ministers, Governments and Parliaments since around 2000 have assured this outcome.

The DTCA of 2012 is yet another tool handed to overseas interests and their ideological supporters in the DMO, as well as Defence, to perpetrate and then perpetuate abuses on Australian Industry, this time using draconian legislated powers able to be wielded by individuals in low, middle management positions who will almost certainly not have the background, knowledge, training, experience nor the technical expertise to know what they don’t know, let alone to competently fulfil the roles for which they are authorised and empowered under the Act.

**POTENTIAL FOR MANIPULATION AND ABUSE OF THE LEGISLATION**

A longitudinal analysis of US legislation which was originally intended to improve processes and the resulting outcomes for the benefit of the Military (here read ‘the warfighter’ as opposed to the Generals and senior bureaucrats in the Pentagon); the defence and security of America; and, thus, the citizenry of the USA provides a fascinating insight into the way these have been hijacked and manipulated by the Military-Industrial-Congressional-Complex (MICC).

In his final speech as the 34th President of the United States (POTUS), Dwight D Eisenhower warned his fellow Americans about the risks associated with the growing, inappropriate and potentially destructive influences of the MICC.

The longitudinal analysis shows that these risks have now materialised on a huge scale.

The analysis shows that the good intentions of legislation such as the False Claims (Qui Tam) Act, Truth in Negotiations Act (TINA), Nunn-McCurdy Act, Weapon System Acquisition Reform Act of 2009 (WSARA), and even the DoD 5001 Acquisition Regulations have not only been thwarted by the MICC but hijacked, principally by large corporations, to enhance, inter alia, their ability to generate increasingly greater revenues from tax payer funded ventures.

The mechanisms employed by these large corporations mirror what the Wall Street corporations did and didn’t do (for omission is one of the great sins) with respect to similarly well intended legislation such as the Sarbanes-Oxley Act of 2002 (SOX). The hijacking as well as misuse and abuse of this legislation by corporations and regulators, alike, contributed if not led to the Global Financial Crisis, the effects under which the Western world is still reeling.

In the same speech, the 34th POTUS also warned his fellow Americans about the risks associated with “The prospect of domination of the Nation’s scholars” and “…the free university, historically the fountainhead of free ideas and scientific discovery” by the MICC and, more broadly, the government bureaucracies with which the MICC players are now so closely coupled.

Eisenhower exhorted his fellow citizens to be wary of inappropriate influences and controls on “the technological revolution” in which “research has become central”. Similarly on the American education and research communities, themselves, where “a government contract becomes virtually a substitute for intellectual curiosity” and “Federal employment, project allocations, and the power of money is ever present”, strongly declaring that any such situation “is gravely to be regarded”.


Having these observations as background and noting the draconian powers the Act creates and puts into the hands of an organisation well known for its proclivity and dexterity in the abuse of power, authority and trust, the potential for manipulation, misuse, and abuse of this legislation becomes self-evident and, in the broad sense, includes:

- Vexatious claims and actions
- Intimidation for political or ideological reasons
- Loss of academic freedom and independence
- Limitations on free speech
- Legislated ‘Blacklisting’ of those with countervailing views to Defence groupthink
- Damage to the public defence debate and defence governance and policy debate

CONCLUSIONS

Global proliferation of advanced military and dual use technologies is an acknowledged problem which is vexing and not easily solved, because any basic technology can be adapted in one or another way for military use.

China and Russia have made use of a wide range of commodity commercial technologies as well as acquired military technologies to enhance their military technology base since 1991. The United States lead in advanced military technology has been largely eroded over the last decade, in a large part due to underinvestment in research and development.

The US ITAR system has not been particularly effective in stemming the flow of advanced technology from Western nations, and has been very costly to administer and maintain, as its basic structure is based on ideas from the Cold War period, when the Soviets were the sole strategic competitor.

The US ITAR system has produced serious systemic damage to many high technology industries as a result in their limited ability to compete in both the national and global marketplaces. This has been a particular problem for the US aerospace industry.

Australia’s DTCA 2012 imposes much wider and more stringent controls on the Australian community than ITAR does on the US community, as many exclusions in the US ITAR are absent or much narrower than exclusions in ITAR. It will be significantly more difficult to manage and much more expensive to operate than the US ITAR controls.

There is no evidence to support the notion that the Defence Organisation has the skills and competencies to properly administer a system identical to ITAR, let alone a system which is that much broader in scope and stringency, such as the DTCA 2012.

The controls over the University system imposed by the DTCA 2012 are well in excess of controls imposed over University research in the US by ITAR, and will produce large scale impacts upon Australian University research in many areas of science and technology as well as defence and strategic studies. Researchers without access to sensitive ITAR
technology will suffer similar constraints on publishing as researchers in the US, working with privileged access to sensitive materials. The independence of Australian universities is thus lost, as is basic academic freedom in many areas of study.

Open source research in foreign military technologies, military operations, and strategy has been identified in the United States as a valuable resource for Governments to exploit in strategic planning and intelligence analysis, as well as governance, but the DTCA effectively closes down such research and publishing activities.

The passage of the DTCB 2011 through the Parliament was characterised by a series of multiple governance failures, nearly all of which can be attributed to how the Defence Organisation failed to perform proper due diligence in its role. The legitimate concerns of the Senate and proposed amendments were not addressed. This was a Bill that should never have been passed into law in its present form.

Deskilling is one of the biggest challenges before our Nation, today. The Dunning-Kruger Effect is now institutionalised in the DMO and running rampant in other Canberra based elements of the Defence Portfolio.

Australian owned and operated sections of the Defence Industry, principally small to medium size enterprises (SMEs), are now at the top of the endangered species list. The current form of the DTCA 2012 legislation makes any recovery from this situation highly improbable if not impossible.

In its current form, the potential for manipulation, misuse, and abuse of the DTCA 2012 legislation is real, present and self evident.

RECOMMENDATIONS

Neither ignore the message nor shoot the messengers.

Embrace the opportunity this legislation and the resulting critical debate have created to derive and determine a better way of achieving the fundamental aims of the DTCA 2012 without the unintended consequences or potential for misuse and abuse.

Engage those subject matter experts who have demonstrated that they are focused upon leaving Australia in a better condition than they found it to assist in achieving this aim.

Researched, Authored, Approved and Submitted by:
Air Commodore Edward “Ted” Bushell, RAAF (Rtd)
Mr Peter Goon, USNTPS (FTE)

References and Bibliography


xi Gus W. Weiss, *The Farewell Dossier; Duping the Soviets*, Studies in Intelligence; Central Intelligence Agency;


xviii SUBCHAPTER M - INTERNATIONAL TRAFFIC IN ARMS REGULATIONS, PART 120 - PURPOSE AND DEFINITIONS, § 120.11 Public domain, "(8) Through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community. as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if:

(i) The University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity or:

(ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable."
Exploring the Impacts of the Defence Trade Controls Act 2012

DISCUSSION PAPER
APA-DP-2013-0801

29th August, 2013

Carlo Kopp, BE(Hons), MSc, PhD, PEng

Editor, Air Power Australia Essays on Military Ethics and Culture, ISSN 2201-9502 and Air Power Australia Analyses, ISSN 1832-2433

© 2013, Carlo Kopp
Executive Summary

Proclaimed in November, 2012, the DTCA 2012 departs from extant regulatory schemes such as ITAR due to its pervasive scope, and the provisions on “intangible technology transfers”, not yet proclaimed, which essentially force a priori approval from the regulators for nearly all activities involving any disclosures. The lack of proper exemptions for open source materials, and severe criminal penalties for even inadvertent disclosures, with the onus of proof reversed, remove the historically accepted hard boundaries between classified/controlled information, and open source information.

As the DTCA 2012 is now active in the defence industry, and producing initial impacts, careful consideration of these is warranted, as similar impacts will arise once the legislation becomes fully active across the higher education sector, and other areas of the Australian community working with technology deemed to fall under the dual use category.

Major risks which an SME or consultant must consider include the arbitrary denial of licences; the arbitrary suspension or withdrawal of licences; the arbitrary censorship of disclosures to a client; weak regulatory agency protection for IP produced for a client; weak protection for client background IP being used; weak mechanisms for resolving disputes or differences with the regulator; and the possibility of vexatious investigations or prosecutions being initiated over matters outside the scope of the licence.

Air Power Australia performed a confidential survey of the views of a number of SMEs and consultants, in relation to the impact of the DTCA 2012. Most parties disclosed the intent to cease operations in the defence sector, due to the combination of compliance costs, but especially due to risks arising from regulator behaviours, based on past experience dealing with the ADO.

The proposed amendments to the DTCA 2012 intended to provide the same protections for the university sector in Australia, as exist in the US and UK, address only the potential damage to the university sector. They do not address damage to the defence industry, other industry sectors, and governance functions, where dual use technology is employed, developed, studied or produced, and will impair the ability to commercialise the outcomes of scientific research in Australia.

The experience with the US ITAR system shows that this type of regulatory regime is obsolete, and no longer suitable for a multipolar world.

All parts of the DTCA 2012 other than those dealing with the protection of ITAR data, and previous regulation of military and WMD exports, should be repealed immediately, and the design of a more suitable regulatory regime initiated, in which the regulator is required to be not only fully accountable, but demonstrate a very robust evidentiary basis for all actions and decisions.

There will be a need for original thinking to solve this problem, and this will require a multi-disciplinary approach, in which key stakeholders such as the academic community must play a role.
Introduction

Proclaimed in mid November, 2012, the *Defence Trade Controls Act 2012* (DTCA 2012) legislation is designed to impose the most restrictive regulatory controls on science and technology ever seen in a Western democracy, and most closely resembles the regulatory regime employed in Soviet Bloc nations during the Cold War. Once fully active, this legislation provides Australian Defence Organisation (ADO) regulators with absolute power over almost all public discourse and activity involving all areas of “dual use” and military science and technology, in Australia. What can be discussed publicly, or privately with parties in other nations, what can be bought, sold, taught, developed and researched in most areas of advanced science and technology, will be regulated with severe criminal penalties applied for breaches of the Act, where the onus of proof is upon the accused.

The legislation was marketed to the parliament and public as being similar to the United States ITAR regulatory regime, and necessary to finalise the *Australia-United States Defense Trade Cooperation Treaty* [1]. These claims are not correct, as the DTCA 2012 legislation imposes controls over “intangible technology transfers” which are absent in ITAR, and applies controls to all activities, with much narrower and ill defined exemptions, providing regulators with powers to arbitrarily control and censor any activities involving any science or technology in the *Defence Strategic Goods List (DSGL)*, a document with more than 350 pages, and subject to arbitrary changes by the regulatory agency at any time [2]¹.

The ADO performed no meaningful impact assessments before the legislation was provided to the parliament, and despite numerous well founded concerns by the Senate committee reviewing the draft bill, it was pushed through the parliament in October, 2012 by the incumbent Government, and became law on the 13th November, 2012. There was little public debate, and limited parliamentary debate on the strategic justifications for such a restrictive regulatory regime, the direct and indirect costs to administer such a pervasive regulatory system, or the direct and indirect impacts to the economy, the industrial base, the higher education system, and public governance functions in the areas of science, technology and national defence. Moreover, no governance responsibility was exercised at either the Executive (Secretary) Level, or the Directing (Ministerial) Level before the Act was submitted to Parliament. As a result, the DTCA lacks proper protections in many key areas [2].

In many respects, the DTCA 2012 follows the model of “principles based legislation”, where the agency implementing the legislation is also delegated most if not all oversight and

---

¹ In discussions with *Air Power Australia*, following the proclamation of the DTCA 2012, when asked why ADO management considered such draconian legislation to be necessary, a senior ADO executive and former Division Head in the *Defence Materiel Organisation* stated that they needed to get researchers and academics in the Universities “under control and held accountable” for the information and technologies they were passing to other nations in the region, such as China and India, through what was seen as the universities’ quite open higher education policy, especially involving foreign postgraduates, and collaborative research programs. The same was required of members of Australian Industry at large, though members of the Australian Defence Industry were deemed less of a problem due to their familiarity with working under ITAR constraints.
Exploring the Impacts of the Defence Trade Controls

governance functions, and ongoing assessments of effectiveness and impact in implementation [3]. The DTCA 2012 lacks proper protections against malfeasance, and misconduct, in the regulatory organization, and is designed to minimize and legislative oversight once the regulatory regime is fully active. For all intents and purposes, the DTCA 2012 provides ADO regulators with the proverbial “carte blanche” in how science and technology are regulated across industry, academia, media and the defence sector. The DTCA will thus impact adversely a number of important Commonwealth policy areas, particularly higher education, manufacturing, and engagement with Asia.

The US ITAR regime, designed around the Cold War CoCom “bipolar” model, has been subject to-intensive criticism by US industry, as it has severely damaged the competitiveness of many industry sectors, while often proving ineffective in its intended objective of denying access to nations which are in strategic competition with the United States. DTCA 2012 magnifies all of the known problems in ITAR, as its scope is greater, its regulatory footprint is larger, its regime is more restrictive, its protections and governance weaker, and its regulatory agency much less equipped to perform objective assessments of what should or should not be disclosed [2].

Australia is not a major player in the global military and “dual use” technology export markets for products and services. Australia has made very few if any important contributions to research, development and design in these areas in recent years, reflecting chronically limited Commonwealth funding across these sectors, and ADO procurement practices over the last decade which strongly favour imports of MOTS (Military Off The Shelf) products and services, over domestic products. Australia’s indigenous defence industry is weak, by global standards, and its most productive SME (Small Medium Enterprise) sector is now in danger of vanishing altogether.

Australia does not and cannot present a major risk in terms of unwanted transfers of locally developed advanced military and dual use technology into nations outside the Western Alliance, compared to nations with strong defence and dual use technology sectors, such as Israel, Japan or France. The rapid growth and sophistication in these sectors seen in China and India make Australia’s national capabilities look trivial, and if anything, indicate that Australia should be investing significantly more, rather than regulating to severely limit all national activity across these sectors. The strategic case for highly restrictive regulation of locally developed military and dual use technologies is simply unsustainable by any robust evidence [2].

If the primary purpose of DTCA 2012 is to improve efficiencies in bureaucratic approval processes for importing ITAR controlled MOTS products from the US for ADO use, the cost incurred across the nation by adopting a regulatory regime far in excess of ITAR begs the more basic question of whether the defence trade treaty is even worth having. Arrangements extant prior to the DTCA 2012 may have been inconvenient for the ADO and some defence contractors, but did not inflict damage in other sectors.
As the DTCA 2012 is now active in the defence industry, and producing initial impacts, careful consideration of these is warranted, as similar impacts will arise once the legislation becomes fully active across the higher education sector, and other sectors working with technology deemed to fall under the dual use category [4].

**Direct DTCA 2012 Impacts on the Defence SME and Consultancy Sector**

Australia has a small community of SMEs and consultants operating in the defence sector, mostly comprising former ADO and major defence contractor personnel. This sector has historically been most active in providing specialist niche products and services to the ADO, as previous regulation for most military exports, and a highly competitive global market, presented genuine obstacles to export. The sector has been in a steady decline over the last fifteen years as a result of a number of ill-considered policies and practices in defence sector procurement. There have been no robust studies performed to date surveying the health, size and prospects for this sector, as despite its often very high value-added contributions to national defence, it is seen by the current ADO procurement system as unimportant [5].

Like all businesses, SMEs and consultants must consider the impact of regulation very carefully, if they are to realize any profit and remain in business, and not become embroiled in disputes or expensive litigation with a regulator. These impacts fall into two categories, which are fixed and variable compliance costs in administration, and in the defence sector, also security, and risks associated with the track record, behaviours, agendas and known biases of the regulating agency.

The DTCA 2012 departs from extant regulatory schemes such as ITAR due to its pervasive scope, and the provisions on “intangible technology transfers”, which are yet to be proclaimed, and which essentially force *a priori* approval from the regulators for nearly all activities involving any disclosures. The lack of proper exemptions for open source materials, and severe criminal penalties for even inadvertent disclosures (with the onus of proof reversed), remove the historical hard boundaries between classified/controlled “information”, and open source “information”. Because the DTCA 2012 does not distinguish between disclosures based on classified/controlled source data or public open source data, all “information” must be protected under DTCA 2012, regardless of origin, as if it were classified material [2].

For a contractor or consultant to safely operate under any regime like DTCA 2012, all technical information regardless of source must be secured to the same standard as formally classified information. Compliance with this requirement imposes the need for physically secure facilities, highly secure networks and computers, secure document storage, and all of the other costly compliance overheads required for government classified grade security. The security standards required to protect commercially sensitive IP (Intellectual Property) are simply insufficient, given the criminal penalties associated with
DTCA 2012, applicable to any disclosures, regardless of whether the source material was or was not previously classified or controlled under ITAR.

Of no less concern is the past track record of the regulator, the ADO, in dealing with the defence industry.

Major risks which an SME or consultant must consider include:

1. Arbitrary denial of licences;
2. Arbitrary suspension or withdrawal of licences;
3. Arbitrary censorship of disclosures to a client;
4. Weak protection for IP produced for a client;
5. Weak protection for client background IP being used;
6. Weak mechanisms for resolving disputes or differences with the regulator;
7. The possibility of vexatious investigations or prosecutions being initiated over matters outside the scope of the licence.

An SME or consultant must therefore consider the risks arising from being prevented from initiating a contract, fulfilling a contract either partly or wholly, meeting client deadlines, as well as the risks that IP may not be well protected from improper disclosure by ADO personnel.

Air Power Australia performed a confidential survey of the views of a number of SMEs and consultants, in relation to the impact of the DTCA 2012, after November, 2012. Most parties disclosed the intent to cease operations in the defence sector, due to the combination of compliance costs, but especially due to risks arising from regulator behaviours, based on past experience dealing with the ADO. One SME observed, that “DTCA 2012 is the straw that breaks the camel’s back.”

The effects observed now across the defence industry SME sector reflect the sector’s reaction to the legislation, and to well known and yet to be repaired problems with the culture and internal management of the regulating agency, the ADO [5], [6], [7], [8], [9], [10], [11], [12].

Exploring Known Adverse Impacts of the ITAR Regime

The US ITAR regime, which replaced CoCom in 1994, cannot be described as particularly effective, is very expensive to administer, while it has a well documented history of adverse impacts, often of considerable severity, especially across industry and research organisations. There are numerous known instances of “containment failure”, which include many widely publicised violations by commercial organisations manufacturing defence equipment or providing services, and successful human intelligence and cyber penetrations of US government and defence contractor facilities [2].

The absolute effectiveness of the ITAR regime as a legitimate containment mechanism is clearly open to debate. The adverse impacts of the ITAR regime on the

---

2 The author ceased defence sector consultancy operations in November, 2012, terminating negotiations for a consultancy in the US, and has since turned away two US defence contractors who sought consultancy services involving unclassified open source analysis and performance modeling of Russian and Chinese military technology.
United States industry and research communities are not open to debate, since they are real, present and self evident [2].

Problems experienced by the US industry include [2]:

1. A significant administrative overhead in tracking products, documentation and associated intellectual property which falls under ITAR;
2. Significant time delays in seeking approvals for ITAR listed products;
3. Significant costs incurred in re-engineering products which may contain components, materials, processes or other intellectual property falling under ITAR [13];
4. Significant security infrastructure costs, and recurring operational costs, ensuring that any material falling under ITAR is treated not unlike classified materials;
5. Constraints on employing engineering talent lacking US citizenship;
6. A competitive disadvantage in bidding against non-US manufacturers offering “ITAR-Free” products, unencumbered by ITAR, especially where the client is seeking technology transfers.
7. Deskilling effects across the defence and oversight of the associated activities due to significant reductions in diversity, competition and critical debate.

There are no studies at this time, which have quantified or qualified the scale of the commercial damage experienced across the entire US industrial base as a result of the cumulative impacts of ITAR. However, some technology sectors have been able to identify a marked causal deterioration in the US technology base [2].

The impacts are best documented in the aerospace industry. In evidence to the House Committee on Science and Technology, in February, 2009, Major General Robert Dickman, (USAF, Ret), Executive Director of the American Institute of Aeronautics and Astronautics observed thus [14]:

“We all understand the reasons why our export control policies were put in place. We have enjoyed technical superiority from decades of investment in education and RDT&E, and from producing and attracting generations of the best intellectual talent pool the world has ever seen. To maintain that superiority, these policies were established to insulate our advantages from the rest of the world, and specifically from regimes that maintain a different and adversarial worldview from our own.....we need to make a realistic evaluation of how these policies are being implemented, and what effects they are having. We need to be willing to act if these policies are falling short, if these policies have become detrimental to our goals. Today, the reality is that these policies are counterproductive to their stated objectives. ...Without a change of course, we will certainly witness dramatic changes in our competitiveness and level of superiority. We are really talking about generational effects, well beyond five years.”

Maj Gen Dickman's observations on the impact of “ITAR-free” marketing are also important:
“ITAR-free’ marketing is designed specifically to compete with U.S. systems and components with contracts that have much less regulation, and can be completed in a much shorter timeline. These are policies developed specifically to make the European manufacturers a more attractive alternative to U.S. industry and the marketing has been very successful, even for almost purely commercial products. The effect has been a dwindling U.S. industrial base largely dependent on government contracts to keep production lines open.”

The damage already done to US industry’s advanced system technology sectors, as well as the US education and research sectors, reflects the realities of trying to manage a complex list of technologies in a rapidly evolving environment, where technology is often not exclusively available to the US [2].

In 2007, Lt Gen Brian Dubie, Chair of the Aerospace States Association, observed that [15]:

“The current regulations allow export licenses to be granted when a part is available commercially elsewhere in the world. In fact, the very existence of what Thales calls its “ITAR Free Satellite” suggests most satellite parts no longer belong on the list of prohibited exports. A re-evaluation of the ITAR controlled technologies is critical to ensure U.S. competitiveness and jobs.”

He also stated that:

“On a panel at the 58th International Astronautical Congress held this fall in Hyderabad, India, Ray Williamson, a research professor at George Washington University’s Space Policy Institute in Washington, stated, “In the long run ITAR is going to be destructive of U.S. industry.””

A US colleague of the author’s, and former president of a major US professional association, noted privately: “Put very simply, ITAR does far more harm to US national security than it helps”.

The problems inherent in the ITAR regime will only continue to increase in type and magnitude over time, as European, Russian, Indian and Chinese industry close the gap in a great many technology sectors controlled by ITAR, because many of these competing technology sectors are showing exponential growth. Simply attempting to maintain currency in the ITAR technologies list will require an ever increasing investment in time and effort by highly qualified research grade personnel to survey the global marketplace. Currently,
Exploring the Impacts of the Defence Trade Controls

technical surveys of advanced foreign weapons and systems technologies covered by ITAR are not well covered by either government or academic research in the USA, unlike during the Cold War era when considerable and ongoing intellectual effort was invested [2].

The fundamental paradigm implicit in ITAR is that complete or substantial knowledge of opposing nations’ technologies is both available and current, but this is no longer the case.


“We surveyed AIA members this year on the topic of export regulations and the message was clear: outdated export controls are hurting U.S. companies. Data supports this view. The U.S. held 73 percent of the worldwide share of satellite exports in 1995 – this fell to a staggering 25 percent by 2005. Today, U.S. law requires export agencies to still look at a nut, bolt, or screw for a commercial satellite and an anti-tank missile through the same regulatory prism. Clearly, it’s time for a change.”

Direct impacts on the United States’ higher education sector are less well documented, in part because the US ITAR system provides wide exclusions for “fundamental” research, where in ITAR “Fundamental research is defined to mean basic and applied research in science and engineering”. The ITAR system includes strong compliance requirements on those US universities performing US DoD funded research involving controlled facilities, equipment and prior research material [16], [17].

An example of a current constraint is that that some US academic organisations are required to divide research conferences into “ITAR-compliant” and “open” streams, applying the same types of controls as generally applied to military technical conferences, which are divided into “classified” and “unclassified” streams, and are further constrained in publishing research in areas which fall under ITAR controls [16], [17].

This, at a minimum, doubles the time and effort required to manage a conference, and places security constraints on venues and facilities.

Another impact of serious concern is that the ITAR system imposes strong constraints on research staffing, and permissible choices of postgraduate students to work on research projects. This restricts the pool of talent that can be used, and inevitably slows down research by creating bottlenecks in recruitment.

Problems within the ITAR system are not confined to direct damage effects. A problem that has emerged, and will likely increase over time, is that of difficulties in prosecutions due to an inability of investigators to identify specific references in the mountain of technology and research data that is already in the public domain, and thus already exempt from ITAR controls.
In summary, there is sufficient evidence to observe, at this time, that the US ITAR regime has become limited in its effectiveness in containing technology transfers, while inflicting significant damage on the US national technology base, and increasingly on the US university technology and research sectors. This is a direct result of the basic paradigm employed, which was inherited from the CoCom system, which was designed around a "bipolar" technology race between the monolithic Soviet Bloc and the West. In a multi-polar world this model has become impossible to manage in a timely and robust manner, because it becomes increasingly expensive and over-demanding in specialist technological effort, increasingly damaging to research, industry and academia, and, as a result, will become increasingly ineffective.

*Every dollar expended on ITAR controls is a dollar not spent on advancing US national security and industry via Research and Development investment, and similar impacts must be expected by all other nations following ITAR as it stands. In a globalised multi-polar competitive technology race, this is ultimately suicidal.*

**Exploring Adverse Impacts of the DTCA 2012**

Because the DTCA 2012 has a much greater footprint than ITAR, and incorporates exceptionally restrictive prohibitions on "intangible technology transfers", it implicitly amplifies every known adverse impact of ITAR, across the whole Australian community, including higher education, all industries, and public administration, governance and media.

This reality is not open to argument. The design of the Act is such that all public discourse, and private discourse with foreign nationals, in all "dual use" and military technologies will be regulated by the ADO.

Many of the adverse impacts of the DTCA 2012 on the higher education system, and research, have been well articulated by numerous Senate submissions by Universities Australia, and other higher education sector entities [2], [4].

The inevitable result of the DTCA 2012 will be a progressive and classical "cascade failure" event across the Australian higher education sector, as the sector, now integrated into a globalized and extremely competitive higher education market, reacts as all market players do³.

Cascade failures are a well studied effect, which can arise in any networked system, where there are functional dependencies between nodes in the system [18], [19], [20], [21].

Current practice in university research is to form collaborative networks, across departments, schools, faculties, institutions, and between researchers and research groups,

---

³ The author observed a partial supply chain cascade failure event in the computer industry, during the early 1990s, arising from changes to subsidy policy in the automotive industry. The latter caused closures in many smaller manufacturers, which also supplied components to the computer industry. The result was the need to source these components from overseas, decreasing Australian content and increasing costs considerably.
Exploring the Impacts of the Defence Trade Controls

globally. Australia is especially dependent on networking in research, due to the small domestic university system, by global standards, and is thus unusually susceptible and vulnerable to disruptions to such networks - having finally overcome the “tyranny of distance”, Australian research is now critically functionally dependent on physical and human networks.

The first impact of the DTCA 2012 will be that foreign talent will depart the country, by necessity, thus seeing an exodus of foreign national science and engineering researchers, experienced academics, and postgraduate and postdoctoral students. This in turn will damage research projects under way, while future research projects, which would have utilized the experience of these personnel, will stall or be terminated at conception.

The reduced capacity and thus competitiveness of impacted research communities will produce a second wave of departures, as Australian nationals start to depart the country, to work at overseas universities, while many older researchers simply opt for early retirement4.

In a globalized education marketplace, the best talent is recruited when and where the opportunity might arise. Historically, some of Australia’s best academic talent has been difficult to retain in the Australian higher education sector, due to scarce research funding, and was frequently recruited by the private sector or foreign universities, especially in the US and EU. Unfortunately, the most sought after talent in the global marketplace is the best talent, so the highest achievers will likely be the first to join the exodus, unless other lifestyle considerations are important enough for them to compromise career advancement.

Inevitably, losses of the highest quality academic staff will increase workloads for remaining staff, reducing incentives to stay in Australia, while compliance overheads and risks will also produce a strong incentive to depart, in turn likely to progressively induce further departures from the higher education sector.

The rate at which this “cascade failure” event unfolds will be determined mostly by the availability of positions across the global higher education and knowledge intensive industry sectors.

It is likely that once this cascade event starts, there will be an active campaign of recruitment across the global marketplace, as opportunities to plunder another nation’s pool of talent are infrequent, and usually the result of major social upheavals. Notable examples include Germany, in 1945, Iran in 1979, and more recently, former Warsaw Pact and Soviet Republics, following the collapse of the Soviet Union in 1992. The US, EU and Israeli

4 The latter will exacerbate existing and well studied problems with the age demographic in the Australian university system.
university sectors and high technology industries were major beneficiaries of the fall of the Soviet system.

Recovery from such a cascade failure is extremely expensive, and could take decades, as many personnel will be reluctant to return, and opportunities to recruit top overseas talent will be hampered by the damaged reputation of Australia as a good environment for a research career.

It is worth observing that the study of how to externally produce cascade failures in an opposing nation’s critical systems has been a topic of much interest and research activity in the military sciences and strategy communities, over the last two decades. From a strategy perspective, an attacker would be hard pressed to devise a better strategy than the DTCA 2012 to cause a cascade failure in Australia’s higher education and knowledge intensive industry sectors, as the legislation specifically targets high value nodes, and impairs the operation of most links, in both of these highly networked systems\(^5\).

Industries, which fall under the footprint of the DTCA 2012, include the aerospace sector, the information technology sector, the biotechnology and bio-informatics sectors, and portions of the resource sector, where remote sensing and sophisticated analysis are performed. In Australia, these sectors are mostly populated by SMEs, with some major overseas multinationals operating some research and development offices in Australia. The DTCA 2012 will “decapitate” these industries, in the manner that ITAR has crippled many sectors in the US, leaving only “low technology” commodity product and service industries intact, but dependent on overseas supply of more advanced technologies and services\(^6\).

The outcome will be a progressive departure, over time, of industry research and development talent to overseas positions, as overseas parent companies simply relocate their research and development groups to nations other than Australia, and SMEs close down. Products and services currently delivered by these organisations will have to be sourced from overseas, giving a competitive advantage to larger overseas suppliers who are able to carry the cost overheads of meeting any import compliance requirements of DTCA 2012\(^7\).

---

\(^5\) The author has a multiplicity of publications across this area, primarily in military strategy, and the systemic effects of electromagnetic weapons and electronic combat on critical infrastructure and warfighting systems.

\(^6\) The author has worked at various times in the IT, resource and aerospace sectors, in roles including engineer, design engineer, chief engineer, software engineer, production engineer, test engineer, analyst, and consultant, over a 32 year period. Many if not most of the “cutting edge” industry development projects the author worked on would not have been possible, had DTCA 2012 been in effect at that time.

\(^7\) An anecdotal scenario describing the effects of the DTCA 2012 was proposed by a colleague: “Bloggs Electronics Pty Ltd can see an enormous business opportunity in replacing the copper links in the Governments NBN ‘Fibre to the Node’ system, and the Board decides to invest a half a billion dollars in a mass-produced Vector AESA WiLiAN modem, that sits on a node and strobes data packets in Line-of-Sight to up to 1024 transceivers over ranges of over ten kilometres. The ‘WiiVEASA’ uses Chinese produced chips and AESA elements. Only operating in the commercial communications sector, the Board
Exploring the Impacts of the Defence Trade Controls

The DTCA 2012 will produce collateral damage effects in other areas. One of these will be public discourse, policy development, and governance in all areas under the footprint of the legislation, especially defence. Bushell and Goon discuss direct impacts in these areas, and their importance, extensively [2].

Given the known impacts of the ITAR regime in the US, and the much more pervasive, restrictive nature of the DTCA 2012 regime, there can be no doubt that this legislation will produce more damaging impacts to Australia’s national science and technology base than any other single regulatory or funding environmental change ever seen before. It would not be unreasonable to apply the emotive term “scorched earth policy” to the DTCA 2012, in terms of its predictable impacts on the higher education and knowledge intensive industry sectors.

Conclusions - Repairing the DTCA 2012 Legislation

As currently legislated, the DTCA 2012 regulatory regime applies unreasonably restrictive controls in most areas, out of all proportion to any strategic need, and will produce inevitable adverse impacts across all regulated sectors, as it amplifies all of the well known problems in the US ITAR regime.

The risks associated with the basic design of the DTCA 2012 regulatory regime, and its weak governance and protection mechanisms, will be seriously exacerbated by known and well documented problems within the regulatory entity.

The proposed amendments to the DTCA 2012 intended to provide the same protections for the university sector in Australia, as exist in the US and UK, address only the potential damage to the university sector. They do not address damage to the defence industry, and other industry sectors, where dual use technology is employed, developed, or produced, and will impair the ability to commercialise the outcomes of scientific research in Australia.

of Bloggs Electronics Pty Ltd are blissfully ignorant of the provisions of the DTCA. The WiiVEASA project is conducted with great secrecy to protect what will be enormously valuable intellectual property. After spending more than $300M, and just before a mass rollout, the regulator discovers the project and issues an infringement notice to Bloggs Electroncs, including a 'cease and desist' order. The WiiVEASA system is clearly within the scope of the DTCA 2012 regime, and the Court finds the Bloggs Industries board members guilty of a breach. They are all sentenced to 10 years jail and are fined 10,000 points. Over 1,000 Australians lose their jobs as Bloggs Electronics is bankrupted. The story does not end there. Bloggs Industries Intellectual Property become worthless, because it cannot be exploited by Australian citizens. This 'inconvenience' does not hamper China's industry, which mass produces a clone of the WiiVEASA system and markets it internationally, where it soon becomes the world standard for delivery of high speed digital networks. After five years, the gross sales exceed US$100 Billion.” A worthwhile observation is that many wireless networks today use technology initially developed by Radiata, using CSIRO and Macquarie University technology, sold to Cisco Systems in the US, in November, 2000. Under a regime such as the DTCA 2012, it is unlikely this could have ever happened.

APA-DP-2013-0801
The prospect of a “cascade failure event” arising in the higher education sector, as the best research talent departs from Australia, is very real, and could take decades to recover from. In many industry sectors, a similar exodus is the most likely outcome.

Any effort to estimate the cumulative damage this legislation will inflict across the higher education sector, the defence industry, and other industry sectors, where dual use technology is employed, developed, or produced, is a major undertaking, and one which should have been performed well before the draft bill was put to parliament.

The experience with the US ITAR system shows that this type of regulatory regime is obsolete, and no longer suitable for a multipolar world [2].

All parts of the DTCA 2012 other than those dealing with the protection of ITAR data, and previous regulation of military and WMD exports, should be repealed immediately, and the design of a more suitable regulatory regime initiated, in which the regulator is required to be not only fully accountable, but demonstrate a very robust evidentiary basis for all actions and decisions. There will be a need for original thinking to solve this problem, and this will require a multi-disciplinary approach, in which key stakeholders such as the academic community must play a role.

About the Author
Dr Carlo Kopp has published in excess of 670 publications across all categories, since 1980, dealing with military technology, operations, strategy and dual use technology. Since the 1990s he has consulted to the defence sector, including DSTO. He has authored, co-authored or contributed to more than thirty Federal parliamentary submissions on defence matters, dealing with military strategy, force structure planning, governance, and cultural breakdowns, in the Australian Defence Organization. The author was a Visiting Research Fellow at ADFA in 2004-2005, and an Adjunct Research Fellow at Monash Asia Institute between 2005 and 2010, and is a practicing part time academic at a G08 University, actively researching in the information and game theoretic foundations of deception mechanisms. In 2004, Dr Kopp co-founded the independent Air Power Australia military and strategic think tank, which is best known for forensic studies of advanced Russian and Chinese military technology, defence governance, and its studies in Asia-Pacific strategy. Dr Kopp is a Fellow of the Lean Systems Society, an Associate Fellow of the American Institute of Aeronautics and Astronautics, a Senior Member of the Institution of Electrical and Electronic Engineers, and a Member of the Association of Old Crows.
References and Bibliography


To: Chair and Members of the SFADT Defence Sub-Committee,

CONNECTING THE DOTS…AND THE RISKS

WHY DEFENCE INDUSTRY IS NOW AT THE TOP OF ENDANGERED SPECIES LIST

(...and about to take a head shot, along with Australian Innovation and Academia)

12 March 2015

Dear Senators,

Air Power Australia welcomes the invitation, and provides this submission, to assist you in your deliberations on the implementation of the Defence Trade Controls Act of 2012 (DTCA 2012) and the Amendment Bill before you (DTCB 2015).

This submission draws, principally, on knowledge of what has happened within and to the Canberra based agencies of the ADO over that past 20 years or so, and how these happenings have effected relations between the ADO and what the Strategic Policy of Defence and Industry of 1998 referred to as “the Fourth Arm of Defence”; namely, Australian Industry and Academia.

This knowledge and the accompanying experiences have led to our giving some prominence to the following adages when looking at or into Defence Matters:

“The devil is often in the detail…as is the salvation.”

“The voices of those who know and understand such things are being ignored and drowned out by those who don’t.”

“Some of the big things that are wrong in Defence can be put down to the differences between ‘believing’ and ‘knowing’.”

….however….

“The Root Cause of much that ails and is broken in Defence, today, is the fact that the protection of the reputations and decisions of public officials, past and present, and their individual interests is now considered paramount over everything else.”

We recommend viewing this and other submissions to your Committee, as well as the DTCA 2012 and the process that have led to the DTCB 2015, through the prism of these knowledge and experience-based adages may prove helpful to your inquiry.
Introduction

Australia is on threshold of a significant loss in its capabilities to research, develop, test & evaluate, and innovate as well as produce creative new capabilities and export oriented products for the defence sector. This is a consequence of three ill-considered policy choices actively promoted by the Department of Defence, for reasons the Department has never been willing or able to properly explain.

The most recent of these policies is implemented in the Defence Trade Controls Act 2012 and its proposed revision, the Defence Trade Controls Bill 2015, on which this submission is focused.

The other two policies are introduced for completeness.

The second of these policies has been the wilful departure from the well-designed 1998 Strategic Policy for Defence and Industry (and supporting cultural guidance and standards), with its explicit focus on bolstering Australian Industry and relevant parts of Academia as the fourth arm of Defence.

The third of these policies is the maintenance of an entirely inappropriate culture and ethical imperative within the ADO, articulated in the Department's 2011 Personal Conduct Review document.

Finally, a detailed Risk Assessment has been done into DTCA 2012 and the consequences that will almost certainly result from its implementation. Some examples of the results of this Risk Assessment are enclosed. We look forward to providing more details at the Committee’s earliest convenience.

Impacts of the Defence Trade Controls Act 2012 (DTCB 2015)

The DTCA2012/DTCB2015 legislation is unique in Western democracies, as it criminalises a wide range of public and open source military and dual use research, development, test and evaluation, collaboration, manufacturing and distribution activities that are legal and indeed actively fostered in most Western democracies.

The study of other models determines the legislation most closely resembles that in force in Putin's Russia, which has its origins in the Soviet regulatory regime for science, technology and military matters, where almost everything was subject to censorship and criminal penalties, with all powers vested in an unaccountable central bureaucracy. Case studies of how this type of legislation works include Russia's jailing of former Russian open source academic defence analyst Dr Igor Sutyagin for ten years, and the recent charging of Russian physicist Dr Vladimir Golubev, under the same legislation.

Once this legislation is active, which is intended for May, 2015, Australia will depart the community of Western democracies, and join the community of dysfunctional regimes where public intellectual discourse in military and advanced Science and Engineering comes under defence bureaucratic control, censored and actively suppressed by criminal penalties.
The legislation is constructed around a series of fundamentally unsupportable assumptions about how and why intellectual discourse operates; about how professional discourse and R&D as well as T&E in the open source, Academic and Industry environments actually works. Key problems for Industry include:

1. Inappropriate and excessive restrictions on public disclosures, private correspondence, collaboration and publishing, notwithstanding proposed DTCB 2015 amendments;
2. The absence of any credible protection of Intellectual Property and trade secrets from the Commonwealth, including a contractor's client IP that may be used;
3. The lack of credible appeal mechanisms, protections and dispute resolution mechanisms, where disagreements arise with the regulator;
4. The risk of arbitrary denial of licences;
5. The risk of arbitrary suspension or withdrawal of licences;
6. The risk of arbitrary censorship of disclosures to a client;
7. The possibility of vexatious investigations or prosecutions being initiated over matters outside the scope of the licence;
8. Compliance and security costs that will be too high for SMEs, consultancies, and research organisations to fund;
9. Placing the onus of proof on to the accused, thus absolving the Commonwealth of responsibility for mistakes;
10. The lack of breadth and depth in Science and Engineering skills in the regulating agency to cover the scope of the legislation; and,
11. The risk of the Defence Strategic Goods List (DSGL) continuing to grow in the topsy turvy fashion it has so far, unabated.

The DTCB 2015 has done little, if anything, to address the problems and concerns formerly provided and petitioned to the Chair of the Strengthened Export Controls (SEC) Steering Group by those in Academia and Industry, alike, effected by this legislation.

In the contrary, claims of broad consultation are based, at best, on “a total indifference to what is real”.

Nor does the initial Act nor the work of the SEC Steering Group address the biggest risk this piece of legislation perpetrates on the Australian Tax Payer, the ultimate clients of Industry and Academia; namely, like its American sibling, the DTCA 2012 as amended, will almost certainly result in catastrophic and vastly increased costs and delays, not only in the provision of defence materiel but across most if not all endeavours of Australian Academia and Industry. This arising from the DTCA 2012, as amended, is assessed at the Extreme Level of Risk.

For those who have any doubts about the veracity of this assessment, they only have to look at the data and facts from defence acquisition programs over the past 15 years, and test the evidence that provides the proof. For example, the costs and time taken in administering the US ITAR requirements, as interpreted within the sub (-optimal)
contracts of some of the overseas primes and principal contractors, have often exceeded the costs and times required to produce the actual parts, deemed by the prime/principal contractors to come under the purview of the US ITAR regime.

The complete structural, strategic, philosophical and implementation model of this legislation is fundamentally broken, and incoherent with Australian values and past practices. The claims by the Department that it is needed for strategic and national security reasons have no basis in fact - many other nations have been able to maintain control over critical national defence technologies with regulatory regimes far more permissive than the US ITAR regime, itself far more permissive than the draconian and, as observed, soviet like DTCA regime.

The US ITAR and now Australian DTCA regimes are not limited to even what is too often loosely termed “Classified Information” but are attempts by those who use this term to broaden the protection of their interests, flawed decisions and reputations, along with those of others.

All parts of the DTCA 2012 other than those dealing with the protection of ITAR data, and previous regulation of military and WMD exports, should be repealed immediately, and the design of a more suitable regulatory regime initiated, in which the regulator is required to be not only fully accountable, but demonstrate a very robust evidentiary basis for all actions and decisions.


“Defence has a public face by there are private disclosures…”

The public face of Defence is fully supportive of the DTCA 2012 – after all, senior Defence officials and their views of the world are the inspirations behind the DTCA 2012.

However, at the working levels within Defence and the DMO, as in Industry, things are quite different, principally because people are better informed from working with the US ITAR regime and understanding that “DTCA 2012 will be like having the ITAR regime on steroids, EPO and other blood doping”.

If the Strategic Policy for Defence and Industry had been implemented, and properly, rather than shut down by senior Defence officials and those who saw it as significant risk to their interests, we would likely not be making this submission and your Committee would not be holding this inquiry.

APA looks forward to expanding on the above, in detail, at the Committee’s earliest convenience.

Repairing the Self-Interest Driven Culture in the ADO

The 2011 Departmental report by then Brig. Craig Orme, entitled "Beyond compliance : professionalism, trust and capability in the profession of arms : report of the Australian Defence Force Personal Conduct Review" articulates the current "ethical" and thus cultural imperative in the ADO to be effectively "protecting the reputation of an individual, an Agency or the ADO", placing this imperative clearly above national interest, and
traditional military ethical virtues such as integrity, honesty and self-sacrifice. Root Cause Analysis shows that every major instance of problems in the ADO, whether in individual conduct, management of procurements, planning etc. can be backtracked to this basic and pervasive shift in the ADO's basic imperative - put differently, this imperative puts the self-interest of the ADO and its leadership, and individual personnel, above the national interest.

*The purpose of the ADO when formed was the protection of national interest, not the protection of organisational political and material interests, or indeed the individual self interest of senior members of the ADO. Until the traditional and appropriate prime imperative of the ADO is restored, pervasively and unequivocally, back to protecting the national interest, the manifest and universal problems observed in the ADO, over the last fifteen years will persist, and their impacts on Industry, and become further exacerbated over time.*

Conclusions

There are many conclusions that can be drawn from the above and the enclosed Risk Assessments.

However, the bottom line, from an Australian Defence, Industry, and Academia perspective as well as the perspectives viewed at the Grand Strategic and Competitive Strategic Levels, in relation to the effects the DTCA 2012 will have on all these aspects of the Australian nation may best be summed up by the following:

"**The DTCA of 2012 in its current and proposed amended form (DTCB 2015) will almost certainly result in Australia becoming uncompetitive, globally, and more particularly in our region.**"

As before, APA looks forward to the opportunity to discuss and provide further evidence to the Committee.

Yours Sincerely,

Peter Goon  
Principal Consultant/Advisor  
Head of Test and Evaluation  
Co-Founder, Air Power Australia

"*Scientists discover the world that exists; Engineers create the world that never was.*"  
Theodore Von Karman, Aerospace Engineer
References and Supporting Papers/Submissions:


## SAMPLE OF ASSESSED RISKS TO COA/INDUSTRY/ACADEMIA/AUSTRALIAN INNOVATION ARISING FROM NEW DEFENCE TRADE CONTROLS LEGISLATION (DTCA2012/DTCB2015)

Risk Assessment performed in accordance with:
- **DMO Liability Risk Assessment (LRA) Process - V1.1 (Downloaded 11 March 2015),**
- **DMO Project Risk Management Manual (2010),**
- **DSTO Technical Risk Assessment Handbook (TRAH) 2010,**
and the associated Risk Assessment Tables and Templates

### Primary Source of Risks:
- DTCA2012/DTCB2015

### Principal Controls of Risks:
- Oversight and Legislative Powers of the Australian Parliament

<table>
<thead>
<tr>
<th>LSN</th>
<th>Identified Risk</th>
<th>Source</th>
<th>Risk Category</th>
<th>Impact Highlights</th>
<th>Likelihood</th>
<th>Consequence</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-1</td>
<td>More significant if not massive increases in cost to the CoA for defence materiel and defence support services compared with the increases due the ITAR regime, as interpreted by overseas prime and principal contractors.</td>
<td>Primary + Overseas Prime/Principal Contractors</td>
<td>Cost</td>
<td>Much higher costs for defence materiel and defence services to the CoA with little if any value added to the Defence acquisition/procurement processes.</td>
<td>Almost Certain</td>
<td>Severe <em>Catastrophic</em></td>
<td>Extreme</td>
</tr>
<tr>
<td>LSN</td>
<td>Identified Risk</td>
<td>Source</td>
<td>Risk Category</td>
<td>Impact Highlights</td>
<td>Likelihood</td>
<td>Consequence</td>
<td>Risk Level</td>
</tr>
<tr>
<td>-----</td>
<td>----------------</td>
<td>--------</td>
<td>---------------</td>
<td>-------------------</td>
<td>------------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>C-2 CoA</td>
<td>More significant if not massive increases in schedules and schedule overruns for provision of defence materiel and defence support compared with those due to the ITAR regime, as interpreted by Defence, DMO &amp; overseas prime and principal contractors.</td>
<td>Primary + Defence / DMO + Overseas Prime/ Principal Contractors</td>
<td>Schedule</td>
<td>Much longer lead times for the provision of defence materiel and defence support services to the CoA with little if any value added to the Defence acquisition/procurement processes.</td>
<td>Almost Certain</td>
<td>Severe Catastrophic</td>
<td>Extreme</td>
</tr>
<tr>
<td>I-1 ADI</td>
<td>Significant increases in the costs and time associated with Industry doing business with Defence, with little if any value added.</td>
<td>Primary + Defence/ DMO/ DECO</td>
<td>Cost + Schedule + Performance /Capability + Safety (of SMEs)</td>
<td>Reinforces the Australian Defence Industry position - being at the top of the endangered species list. Further decline in the capacities and capabilities of the Aust Defence Industry.</td>
<td>Almost Certain</td>
<td>Severe Catastrophic</td>
<td>Extreme</td>
</tr>
<tr>
<td>I-2 ADI</td>
<td>Significant increases in the cost/time associated with all Australian Industry activities related to technologies listed under the dual usage category of the DSGL.</td>
<td>Primary + Defence/ DMO/ DECO</td>
<td>Cost + Schedule + Safety (of SMEs)</td>
<td>Places Aust Industry under the control of Defence/ DMO/DECO unnecessarily, with little if any value added. Additional cost burdens on Defence/DMO/DECO</td>
<td>Highly Likely</td>
<td>Severe Catastrophic</td>
<td>Extreme</td>
</tr>
<tr>
<td>LSN</td>
<td>Identified Risk</td>
<td>Source</td>
<td>Risk Category</td>
<td>Impact Highlights</td>
<td>Likelihood</td>
<td>Consequence</td>
<td>Risk Level</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------------------------------------------------------------</td>
<td>-----------------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>----------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>I-3</td>
<td>This Law will stymie and suppress if not obliterate participation in critical debate and the provision of countervailing views by Industry and Academia in all but the most innocuous Defence Matters.</td>
<td>Primary + ADO Culture</td>
<td>Safety (of, as Acting CEO of the DMO calls “the little guys”) + Performance /Capability + Reputation</td>
<td>Extant Westminster governance mechanisms are predicated on the presence of open public discourse and debate on Defence Matters, which will be closed down for all matters of substance</td>
<td>Very Likely to Almost Certain</td>
<td>Severe Catastrophic</td>
<td>Extreme</td>
</tr>
<tr>
<td>U-1</td>
<td>Departure of non-Australian academic personnel, and inability to recruit academics and PhD students overseas, denying primary source for personnel replenishment</td>
<td>Primary</td>
<td>Cost + Performance /Capability + Reputation</td>
<td>Inability of HEd sector to compete in global marketplace, while exacerbating extant problems with age demographic in research and teaching personnel</td>
<td>Almost Certain</td>
<td>Severe Catastrophic</td>
<td>Extreme</td>
</tr>
<tr>
<td>U-2</td>
<td>Cascade Failure Effect: Will produce a deleterious cascade effect of deskilling and downsizing across HEd sector, crippling research, and later, teaching.</td>
<td>Primary</td>
<td>Performance /Capability + Reputation</td>
<td>Inability of HEd sector to compete in global marketplace, while exacerbating extant problems with age demographic in research and teaching personnel</td>
<td>Almost Certain</td>
<td>Severe Catastrophic</td>
<td>Extreme</td>
</tr>
<tr>
<td>LSN</td>
<td>Identified Risk</td>
<td>Source</td>
<td>Risk Category</td>
<td>Impact Highlights</td>
<td>Likelihood</td>
<td>Consequence</td>
<td>Risk Level</td>
</tr>
<tr>
<td>-----</td>
<td>----------------</td>
<td>--------</td>
<td>---------------</td>
<td>------------------</td>
<td>------------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>A-2</td>
<td>Pariah State Effect: Will destroy Australia’s extant reputation as a good place for research and open public discourse, alienating Australia amongst Western democracies</td>
<td>Primary</td>
<td>Reputation</td>
<td>Global media criticism, and refusal of overseas commercial industry and HEEd sectors to engage with Australian organisations, impacting investment and innovation</td>
<td>Almost Certain</td>
<td>Severe <em>Catastrophic</em></td>
<td>Extreme</td>
</tr>
<tr>
<td>A-1</td>
<td>Cascade Failure Effect: Will produce a deleterious cascade effect of further deskilliing within Defence/DMO and the loss of capabilities and the requisite skill sets across all sectors of Australia’s innovation community that are subject to this Law.</td>
<td>Primary</td>
<td>Cost + Performance/Capability + Reputation</td>
<td>With no ability to replenish with highly skilled personnel produced by HEEd and industry, Defence/DMO will lose any capacity to overcome extant problems on staffing and current problems will accelerate</td>
<td>Almost Certain</td>
<td>Severe <em>Catastrophic</em></td>
<td>Extreme</td>
</tr>
</tbody>
</table>

**Legend:**

ADI: Australian Defence Industry/Australian Industry  
AUS: Australian Nation  
CoA: Commonwealth of Australia  
UnI: Australian Universities/Australian Innovation
Inquiry into planned acquisition of the F-35 Lightning II
(Joint Strike Fighter)

Submission
on
Terms of Reference (ToR) Item f.
Other Related Matters:
Regulatory Considerations and Impacts
26 January 2016

EVIDENCE TO THE
PARLIAMENT
AND
THE DEFENCE TRADE
CONTROLS ACT

“The ITAR (International Traffic in Arms Regulations) has gone a long way to markedly reducing the international competitiveness of America’s Defense Industry. European defence contractors proudly market their wares as ‘ITAR free products’. Another effect has the US Defense Industry even more stove piped and inwards looking than has been induced by the ‘cold war peace dividend’. This situation is made worse by the way major defense contractors, with their legions of ITAR administrators, managers and lawyers, interpret the regulations; leading to the costs to manage/administer/certify the ITAR ending up more than the direct cost for producing the part. The adage about ‘making money for old rope’ doesn’t come close to describing this game.”

“While as bad as this is, the senior defence officials inspired DTCA is something else, again.”

“Put simply, the DTCA is the equivalent of ITAR on steroids, EPO and blood-doping that is then administered under a regime driven by ‘self before service’ and, like all defence abuse matters, is just as pernicious to Australian citizens and the Nation, alike.”

APA Assessment of the DTCA, circa 2012
In late October, 2012, *Air Power Australia* started closing down all research projects, all collaborations, and all new publishing activity in all areas of military science, military capabilities and technological strategy, to accommodate the introduction of the Defence Trade Controls Act 2012. The bulk of the source research material in APA submissions to this Inquiry was published between 1998 and October 2012.

The language in the DTCA legislation is very specific and not open to interpretation. Publishing or disclosing to the publicly any of the type of forensic analytical research that APA has performed, using public open source materials, could be arbitrarily and unilaterally deemed by defence officials to be a criminal offence under 14A (1) and (2)\(^1\)\(^2\).

The requirement, under the 14A (3), for Ministerial Approval to disseminate any such material makes any effort to continue such research and publishing non-viable.

The monetary/time costs of defending against an allegation by a defence official that the Act has been breached, even if the publication only disclosed that what was previously published overseas, are too prohibitive for a non-profit volunteer organisation like APA to carry.

Given the current Defence culture, the expectation that some if any senior defence official could act as impartial and objective censors under 14A (3) is at best optimistic.

The track record of senior defence officials since 2003 displays a consistent pattern of muddling public discourse on Defence Matters with vendor propaganda, ideologically motivated beliefs, errors of fact, misleading distractions, and simple nonsense, the intent of which invariably appears to be distraction of Parliament, media and public, to draw attention away from prior mistakes or erroneous advice to Governments by senior defence officials.

The observed track record in public statements by senior defence officials reflects the policy within the ADO of misconduct being defined as that what “brings the reputation of an individual, a group or organisation [in the ADO] into disrepute”. Therefore hiding any adverse realities that might bring the ADO into disrepute is considered “Appropriate Conduct”, no matter that doing so might be unethical, dishonest or unlawful\(^3\).

Put bluntly, Defence are confronted with implicit conflicts of interest if they are to act under the DTCA as a censor of all public discourse in DSGL matters, as defined by 14A (3) of the DTCA. Defence personnel tasked with censoring third party publications that might by their analytical content expose shortcomings in Australian capabilities will be compelled to censor out or disallow such content, or be subject to internal allegations of misconduct.

This problem is further compounded by the obvious deskilling within the Canberra based agencies of Defence; especially in performing critical, independent forensic technical assessments of military technologies, foreign and domestic, then determining its importance.

The DTCA regime is closest in its operation and design to the censorship regime employed in the Soviet Union, and as of late 2015 employed in Russia. No such censorship regime exists in other Western democracies.

Defence officials have never explained why Australia must be subject to any such censorship of public discourse on defence capability topics that are unregulated in other Western democracies, such as the United States or United Kingdom.

The DTCA strikes at the heart of open public and professional discourse on the management, governance and implementation of Defence Matters, and especially renders any robust, critical discourse on procurement of military equipment infeasible. It will result in further opacity in the Defence Debate, as anything published must first be approved by Canberra, if the author is not to become exposed to the draconian search and seizure investigative powers, let alone prosecution under the DTCA.
The provision of informed professional quality evidence to Parliamentary bodies, and submissions to inquiries, such as this one, presents significant problems under the DTCA.

Any analytical interpretation or conclusions drawn from public source materials could be, and likely would be, interpreted by some defence officials as breaches of the Act, as the Act explicitly exempts only that what has been previously disclosed as lawful.

Performing the necessary research to provide evidence to an inquiry is expensive and time consuming, and APA has in previous years produced the research, in part, as part of academic publishing activities, consultancies, and commercial publishing in the media.

None of the latter is feasible any more under the DTCA.

Specific publications APA terminated in late 2012, due to the DTCA, include:

A. A largely completed peer reviewed monograph on the future of Electronic Attack (EA), surveying extant and future capabilities, and comparing survivability of super-cruising and subsonic EA platforms in an A2/AD threat environment;

B. A draft peer reviewed paper on the kinematic performance modelling of long range Russian and Chinese Surface to Air Missiles, developed for A2/AD applications;

Specific research projects APA planned for and did not pursue, due to the DTCA, include:

A. Performance and observables modelling of the Shenyang J-31 fighter;

B. Further costing analysis and modelling of the JSF Program with a principal focus on the working thesis that the JSF Pricing Strategy/Model has ‘a never ending price’ baked into the JSF designs;

C. Kinematic performance modelling of long range Russian and Chinese Surface to Air Missiles in the 250 km – 400 km performance envelope;

D. Modelling of deep fading effects in long range microwave propagation, and their impacts on Electronic Attack operations;

E. Further collaboration with colleagues overseas on a range of performance, system capability and tactical employment matters of 5th Generation air combat aircraft and related developments with a focus on the further evolution of this class of weapon and the associated weaponry.

F. Updates of extant Technical Reports on the T-50 PAK-FA, J-20, S-400 Triumf, S-300VM/V4, 96K6M-Pantsir SM, Su-34 FULLBACK, Su-35S FLANKER, and various Russian and Chinese guided munitions, including new cruise missiles;

G. New Technical Reports on the J-31 fighter, the S-350 Vityaz Surface to Air Missile system, and new guided munitions such as the Kh-59MK and Grom E1/E2.

H. Production of a seminal dissertation on what ails and is broken in Defence, today, with the evidentiary proofs from PARCA and Risk Based Assessments of the increasingly moribund and dysfunctional environment Australian Scientists, Engineers and fellow Technologists must contend with on an increasing basis.

Such research could have usefully contributed to this inquiry, and other Parliamentary inquiries as well as to the all important contestability and governance of Defence itself.

The principal beneficiaries of the DTCA are Russia and China, as the capabilities and shortcomings of their military systems that could and should be examined via independent expert forensic analyses and assessments, will not be subjected to such.

Inquiry into the planned acquisition of the F-35 Lightning II
Endnotes

1 Defence Trade Controls Act 2012, No. 153, 2012: (as amended)

14A Publishing etc. DSGL technology

(1) A person commits an offence if:

(a) either:

(i) the person publishes DSGL technology to the public, or to a section of the public, by electronic or other means; or

(ii) the person otherwise disseminates DSGL technology to the public, or to a section of the public, by electronic or other means; and

(b) the person does not hold an approval under this section authorising the publication or dissemination of the DSGL technology.

Penalty: Imprisonment for 10 years or 2,500 penalty units, or both.

Exception

(2) Subsection (1) does not apply if the DSGL technology has already been lawfully made available to the public or to the section of the public.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the Criminal Code.

Approvals

(3) The Minister may, in writing, approve a person publishing or otherwise disseminating specified DSGL technology to the public or to a specified section of the public. The Minister may give an approval only if the Minister is satisfied that it is in the public interest to do so.

(4) If the Minister gives an approval under subsection (3), the Minister must give the person the approval.

Note: Section 67 deals with giving approvals under this Act.

2 DTCA Definition of “DSGL technology”: “technology relating to goods means: (a) information relating to the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of the goods (including information in the form of blueprints, drawings, photographs, plans, instructions, specifications, algorithms or documentation); or (b) software relating to the goods”; This definition, intended to control “intangible technology transfers” effectively covers anything of any substance relating to any item in the DSGL – whether the controlled item itself, or any software/technology in a “catch all” clause, thus effectively prohibiting any discourse other than “dual use” publications exemptions in DTCA2012/2015;