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

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

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

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[iiiiiii].

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[ivv]. 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[vivii].

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[viii].

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[ix].

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[x];

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[xi];

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[xii];

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[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[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[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."[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."*[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.

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.

AUSTRALIA' DEFENCE TRADE CONTROLS ACT (DCTA) 2012

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 system[xx].

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.

Cite[xxi]:

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

```
31          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:

```
15 DSGL technology.

16    technology relating to goods means:

17          (a) information relating to the design, development,
production,

18          manufacture, assembly, operation, repair, testing,

19          maintenance or modification of the goods (including

20          information in the form of blueprints, drawings, photographs,

21          plans, instructions, specifications, algorithms or

22          documentation); or

23          (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 <u>not</u> be classified**",

....and...,

"**If there is significant doubt about the appropriate level of classification, it <u>shall be classified at the lower level</u>.**"

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 engineering[xxii].

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 Trade[xxiii].

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 enactment[xxiv].

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[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." [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.

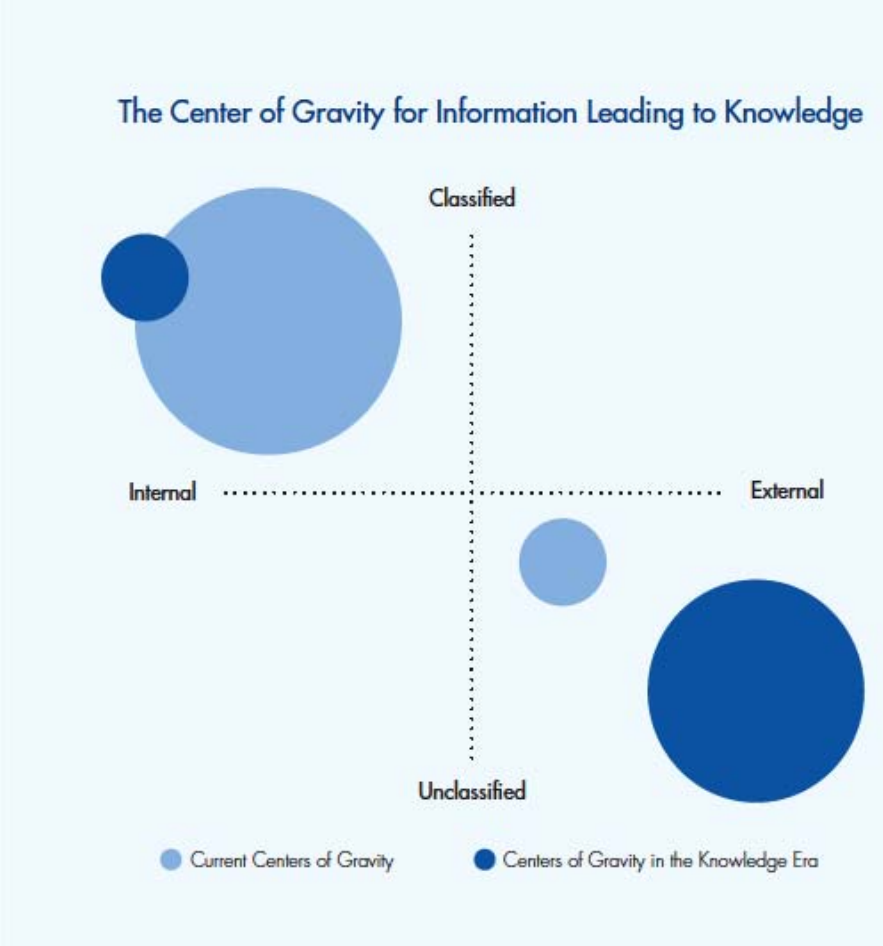
In Canada, researchers at the University of Toronto identified the large scale Ghostnet hacking network, involving penetrations of government facilities on a global scale, and continue to produce valuable research detailing cyber-operations globally.

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.****"*



Source: ISNA

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."*

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'.

Senate Inquiry into Defence Procurement Procedures
Hansard Transcript, 07 October 2011, Page 10

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.

L*egislation 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 solutions[xxvii].

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.

POTENTIONAL 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

i Kopp C., *PLA-AF and PLA-N Flanker Variants*, APA-TR-2012-0401, Air Power Australia, April, 2012.
ii Kopp C., *The role of Russian industry in the Asian arms race*, Controlling arms and terror in the Asia Pacific, eds Marika Vicziany, Edward Elgar, Cheltenham, UK, pp. 247-265.
iii Kopp C., *The Cruise Missile Proliferation Problem*, Technical Report, APA-TR-2007-0708, Air Power Australia, July, 2007.
iv Joby Warrick and Carrie Johnson, Chinese Spy 'Slept' In U.S. for 2 Decades, Washington Post, Thursday, April 3, 2008.
v Department of Justice, *Hawaii Man Sentenced to 32 Years in Prison for Providing Defense Information and Services to People's Republic of China; Former B-2 Bomber Engineer Helped PRC Design Stealthy Cruise Missile,* Office of Public Affairs, Department of Justice, 25th January, 2011.
vi Kopp C., *Almaz-Antey S-300PMU2 Favorit Self Propelled Air Defence System / SA-20 Gargoyle*, Technical Report, APA-TR-2009-0502, Air Power Australia, May, 2009.
vii Kopp C., Technological Strategy in the Age of Exponential Growth, *Joint Force Quarterly,* Issue 66, 3rd Quarter, July 2012.
viii Kopp C., Evolving technological strategy in advanced air defense systems, *Joint Force Quarterly,* vol 57, National Defense University Press, Washington DC USA, pp. 86-93.
ix Kimball G.E. And Morse P.M., Methods of Operations Research, Chapter 4, March 1981, Peninsula Publishing, Los Altos Hills, CA, reprinted from a 1951 edition.
x John Prados, The Navy's Biggest Betrayal, Naval History Magazine, Vol.24, No.3, US Naval Institute, June, 2010.
xi Gus W. Weiss, The Farewell Dossier; Duping the Soviets, Studies in Intelligence; Central Intelligence Agency;
xii Matt Schudel, Cold War Spy Tale Came to Life on the Streets of Moscow, *Washington Post*, Sunday, April 20, 2008 ;
xiii Christopher Goins, *Chinese Hackers Stole Plans for America's New Joint Strike Fighter Plane, Says Investigations Subcommittee Chair*, Cybercast News Service, 25th April, 2012, URI: http://cnsnews.com/news/article/chinese-hackers-stole-plans-americas-new-joint-strike-fighter-plane-says-investigations ; accessed November, 2012.
xiv Media release, Fact Sheet: Major U.S. Export Enforcement Actions in the Past Year, Department of Justice, United States, 11th October, 2007, URI: http://www.justice.gov/opa/pr/2007/October/07_nsd_807.html ; Media release, Fact Sheet: Major U.S. Export Enforcement Prosecutions During the Past Two Years, Department of Justice, United States, 28th October, 2008, URI: http://www.justice.gov/opa/pr/2008/October/08-nsd-959.html;
xv Dominic Gates, *Separation anxiety: The wall between military and commercial technology,* The Seattle Times: Business & Technology, Seattle Times, 22 January, 2006.
xvi Major General Robert Dickman (USAF, Ret), *Impacts of U.S. Export Control Policies on Science and Technology Activities and Competitiveness*, Testimony to the Committee on Science and Technology United States House of Representatives, 25 February 2009; URI: https://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/National_Security/ITARTestimony022509.pdf accessed November, 2012.
xvii Brian Dubie, Fix ITAR to Protect our National and Economic Security, Space News, 26 November, 2007.
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 dissemlnallon 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."

xix ITAR Frequently Asked Questions, Briefing Document, American Institute of Aeronautics and Astronautics, URI: https://www.aiaa.org/Secondary.aspx?id=14328&terms=ITAR; U.S. International Traffic in Arms Regulation (ITAR), Briefing Note, Institution of Electrical and Electronic Engineers, URI: http://www.ieee.org/about/corporate/compliance/regulatory/itar.html accessed November, 2012.

xx Refer Page 20, DEFENCE TRADE CONTROLS BILL 2011
EXPLANATORY MEMORANDUM, THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA,
HOUSE OF REPRESENTATIVES, October, 2012.

xxi Defence Trade Controls Bill 2012, A Bill for an Act to regulate dealings in certain goods, services and technologies, and for related purposes, The Parliament of the Commonwealth of Australia.

xxii Procurement procedures for Defence capital projects, Inquiry, URI: http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=fadt_ctte/completed_inquiries/2010-13/procurement/index.htm, accessed November, 2012.

xxiii Refer Submissions received by the Committee, Defence Trade Controls Bill 2011 Inquiry, Senate Website, URI: http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=fadt_ctte/trade_controls/submissions.htm; accessed November, 2012.

xxiv Media Release, Defence trade controls research trial an improvement, Universities Australia, 31 October, 2012, URI: http://www.universitiesaustralia.edu.au/page/media-centre/2012-media-releases/defence-trade-controls-research-trial-an-improvement/

xxv Media Release, Former University of Tennessee Professor John Reece Roth Begins Serving Four-Year Prison Sentence on Convictions of Illegally Exporting Military Research Data, Federal Bureau of Investigation, United States Government, URI: http://www.fbi.gov/knoxville/press-releases/2012/former-university-of-tennessee-professor-john-reece-roth-begins-serving-four-year-prison-sentence-on-convictions-of-illegally-exporting-military-research-data, accessed November, 2012.

xxvi Intelligence and National Security Alliance, “Expectations of Intelligence in the Information Age”, White Paper, October, 2012.

xxvii *“The Dunning–Kruger effect is a cognitive bias in which unskilled individuals suffer from illusory superiority, mistakenly rating their ability much higher than average. This bias is attributed to a metacognitive inability of the unskilled to recognize their mistakes.”*, Wikipedia, URI: http://en.wikipedia.org/wiki/Dunning%E2%80%93Kruger_effect