COMPUTING RESEARCH & EDUCATION
1a Adelaide Street
Footscray, Victoria, 3011
www.core.edu.au
ABN: 79 455 832 902

18th December 2013

Senator Alan Eggleston
Chair, Senate Foreign Affairs, Defence and Trade Committee
Parliament House ACT 2600
Email: fadt.sen@aph.gov.au

Re: Implementation of the Defence Trade Controls Act 2012 (Cth)

Dear Senator Eggleston

The *Computing Research and Education Association of Australasia* (CORE) is deeply concerned about the impact of the DTCA 2012 on the computing research and education sectors in Australia.

CORE is an association of university departments of computer science in Australia and New Zealand, and thus represents computing research and education focused entities in universities, institutes of technology, colleges of advanced education, institutes of technical and further education, and similar groups in the public sector, industry and commerce.

There are a number of key concerns that CORE has about the DTCA 2012, which can be summarized thus:

1. Restrictions imposed upon foreign nationals in research and higher education:
    a. In Australia, as in most OECD nations, computing disciplines rely heavily on staff, but especially graduate students, who are foreign nationals. Restrictions imposed on the basis of nationality will produce crippling effects, as it will be impossible to staff all positions with Australian nationals, and graduate research will also be heavily impacted.
    b. Given that breaches of the DTCA 2012 are criminal offences, it is likely that filling positions vacated by foreign nationals will be extremely difficult, as researchers will mostly prefer to work in areas that are not so encumbered. This will have a very serious impact on Australia's research productivity and focus.

2. Restrictions imposed on overseas collaborations in research, due to the yet to be proclaimed controls on "intangible technology transfers":
    a. Australia, like most OECD nations, performs much research as part of a global network of academic research activities. Research teams are frequently formed internationally, to solve a problem, on an ad hoc basis, pooling talent as required

from many nations. Constraints on communications, and exclusions on foreign research partners, will produce crippling effects. This will impact not only specific Australian computing research groups but research capacity in the sector overall. The heavy reliance on ICT across disciplines further increases this impact.

b. The process of peer review of research publications, and the examination and publication of PhD theses, both heavily reliant on overseas researchers, will not be workable in an environment where these are subject to controls of the type imposed by the DTCA 2012.

3. Changes over time to the Defence Strategic Goods List (DSGL):
    a. The pattern observed in the United States with the ITAR controlled goods list has been that it periodically accretes and thus grows over time. Often this happens when some nation finds a creative military or "dual use" for some technology until then considered benign. The Australian DSGL can be expected to closely follow ITAR prohibitions. This presents very serious long term risks to researchers working in areas not controlled by the DTCA 2012, who may suddenly find themselves working in an area which has become controlled. This will be a strong disincentive for researchers in any cutting edge research to remain in Australia, if the research is in any area with any potential to become controlled. Specific examples encompass but are certainly not limited to robotics and artificial intelligence, two of the largest ICT research areas in Australia as evidenced by the ERA 2012 review.

4. The problem of "applied" versus "basic" research:
    a. The DTCA 2012 imposes controls on "applied" research, but exempts "basic" research, attempting to resolve by administrative process a distinction, which is often difficult for experts to make.
    b. In computing disciplines, even where research is unambiguously "basic" in nature, the effort to convert an algorithm or research tool into an application may be very small, and thus much basic research confronts the risk of being treated as if it were "applied" and thus subject to controls. Examples include artificial intelligence, cryptography, computer security, networking, data analytics, and high performance computing.

CORE's assessment is that the DTCA 2012 will produce severe impacts upon computing research and graduate education in Australia, and presents a risk of a "cascade failure" event across many important computing research areas.

We trust that our observations, and the appendices to this submission, will be helpful to the Committee as it considers the implementation of the DTCA 2012.

Yours sincerely

Professor John Grundy, PhD FASE FIEAust
President, CORE

Appendix

1. APA Discussion Paper APA-DP-2013-0801, dated 29th August 2013, entitled "Exploring the Impacts of the Defence Trade Controls Act 2012" (provided with permission);

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

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.

governance functions, and ongoing assessments of effectiveness and impact in implementation [3]. The DTCA 2012 lacks proper protections against misfeasance, and malfeasance, in the regulatory organization, and is designed to minimize parliamentary 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 unsupportable 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"*[2].

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,

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.

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' 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 do[3].

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.

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 retirement[4].

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 WiiLAN 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*

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 Electonics, 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.

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, coauthored 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

1. Smith, S., *Explanatory Memorandum, Defence Trade Controls Bill 2011*, Office of the Minister for Defence, 2012, Parliament of Australia: Canberra.
2. Bushell, E.J. and Goon P.A., *THE UNINTENDED CONSEQUENCES OF THE DEFENCE TRADE CONTROLS ACT 2012; Submission to Inquiry into the Implementation of the Defence Trade Controls Legislation*, Senate Foreign Affairs, Defence and Trade Committee, 2013, Department of the Senate. p. 25.
3. *Principles-based regulation* Regulating Privacy / Regulatory Theory 2013 [cited 2013 26 August 2013]; Available from: http://www.alrc.gov.au/publications/4. Regulating Privacy/regulatory-theory.
4. Korb, K.B. *Australia's Act of Intellectual Terrorism: DTCA 2012*. 2013 [26th August 2013]; Available from: http://bayesian-intelligence.com/bwb/2013-07/australias-act-of-intellectual-terrorism-dtca-2012/.
5. Bushell, E.J., *Annex B, Draft Submission, Analysis of DMO MPR 2011-12, Submission to Joint Committee on Public Audit and Accounts*, 2013.
6. Criss, P.J., *Submission No. 3, Review of the Defence Annual Report 2006/2007*, Joint Standing Committee on Foreign Affairs, Defence and Trade, House of Representatives, 2007: Canberra.
7. Goon, P.A., *The Root Cause of What Ails Defence Today.* Air Power Australia Analyses, 2005. **2**(1): p. 1.
8. Bushell, E.J. and Kopp, C., *The RAAF's Professional Mastery Problem: Symptoms, Causes and Measures to Reskill the RAAF.* Air Power Australia Analyses, 2008(6): p. 1.
9. Bushell, E.J., *The Widespread Consequences of Outsourcing.* Air Power Australia Analyses, 2010. **7**(3): p. 1.
10. Orme, C., *Beyond compliance : professionalism, trust and capability in the profession of arms : report of the Australian Defence Force Personal Conduct Review*, Department of Defence, 2011, Department of Defence: Canberra, A.C.T.
11. Rumble, G.A., et al, *Report of the Review of allegations of sexual and other abuse in Defence.* 2011, Department of Defence: Canberra, A.C.T.
12. Bushell, E.J., *Rebuilding the Warrior Ethos.* Air Power Australia Analyses, 2008(10): p. 1.
13. Gates, D., *Separation anxiety: The wall between military and commercial technology,* in *Seattle Times,* 2006, Seattle Times: Seattle, United States.
14. Dickman, R., *Impacts of U.S. Export Control Policies on Science and Technology Activities and Competitiveness*, in *Committee on Science and Technology, House of Representatives,* 2009.
15. Dubie, B., *Fix ITAR to Protect our National and Economic Security*, in *Space News,* 2007: United States.
16. AIAA. *ITAR Frequently Asked Questions*. ITAR Frequently Asked Questions 2012; Briefing]. Available from: https://http://www.aiaa.org/Secondary.aspx?id=14328&terms=ITAR.
17. IEEE. *U.S. International Traffic in Arms Regulation (ITAR)*. 2012; Available from: http://www.ieee.org/about/corporate/compliance/regulatory/itar.html
18. Green, D.G. and Heng A.T.N. *Cascading Failure*. 2007 26th August 2013]; Available from: http://vlab.infotech.monash.edu.au/simulations/networks/cascading-failure/.

19. Lewis, T. *Critical Infrastructure Protection Metrics and Tools; Why Do Networks Cascade? [June 5-7, 2008] [video]*. 2008; Available from: http://www.chds.us/?player&id=1781.
20. Ouyang, M., et al., *A methodological approach to analyze vulnerability of interdependent infrastructures.* Simulation Modelling Practice and Theory, 2009. **17**(5): p. 817-828.
21. Motter, A.E. and Lai Y.-C., *Cascade-based attacks on complex networks.* Physical Review E, 2002. **66**(6): p. 065102.