Submission No 167

Inquiry into potential reforms of National Security Legislation

Organisation: A Halter

The Parliamentary Joint Committee on Intelligence and Security. Equipping Australia Against Emerging and evolving Threats

personal submission to the committee.

Prepared by Mr A Halter, Retired Naval Officer.

The following references are relevant to this submission.

A "Equipping Australia Against Emerging and evolving threats" – July 2012 Public discussion paper to the PJCIS.

B. Terms of Reference for the Inquiry

C. "Making a Submission" – April 2011

D. Privacy Act 1988 [Cth] 2004

E. The Criminal Code Act [Cth] 1995 / and Espionage amendments 2002

F The Crimes Act 1914

G. Crimes Legislation Amendment (Telecommunications Offences and Other Measures Act 2004.

H. Evidence Act [Cth] 1995 Sec 130

I. ***Axis of Deceit*** – Andrew Wilkie 2004

J. ***The looming Tower Al Qeda's road to 9/11*** Lawrence Wright - Penguin 2006

K ***Target Iran*** – Scott Ritter 2006

L. ***Papers in Australian Maritime Affairs No 19*** – The Relevance of Maritime Forces to Asymmetric Treats LCDR J Wright 2006

M. My personal experience as a Naval Officer from 1996 – 2007. [ADF]

N. Fildes, Jonathan (23 September 2010) BBC News - "Stuxnet worm 'targeted high-value Iranian assets"

O. Halliday, Josh (24 September 2010) London *The Guardian* –Stuxnet worm

P SBLT Delisle Canadian Armed Forces Intelligence infomation Leak – The Australian 25 Jul 2012

Caveat's – A great deal of effort has gone in to ensuring this document does not in any way reveal any information that is classified. Any sections that could possibly contain be classified or sensitive material will be marked as such in the standard ADFP 102 Manner. To **comply with Reference C**. [U Unclassified R Restricted C Confidential S Secret] – All information used in this proposal is OPEN SOURCE. Highlighting paragraphs however provides the committee the opportunity to scrutinise the information and sanitise where appropriate. This is offcourse provided that the document is not altered to present a different argument. – I have not had access since 2003 (TS) 20007 – (S)

An executive summary has been prepared. When considering the content of this submission the summary is a ***very summarised version.*** To gain a complete understanding of the content and arguments presented one should read the entire document. Whilst it is highly technical in nature so to is the discussion paper and strategic argument at hand.

Executive Summary

U -Australia's security landscape is at an important technical, historic and moral juncture. It is a reasonable time to be considering matters of internal security and our strategic posture in the Asia Pacific region, particularly as the 2013 defence white paper is being completed. Moreover there has been a dramatic shift in technological capability in a general sense that has to be considered in future security decision making. It is clear from the discussion paper before the committee, that it is these very questions that the committee is seeking to address.

U –Australia has a robust legal system which is unique in the region. It attempts to protect the rights of the individual whilst ensuring the ability of the commonwealth to make and enforce laws to protect Australia and its interest's. This is a difficult balancing act. My submission looks at this difficult balancing act with specific reference to current events and recent history in the technical and social landscape that is modern day Australia.

U -One of our countries' biggest challenges is that our legal system is often slow to keep pace with technological changes. Communications technology changes almost on a daily basis. It is unfortunate that our legal system moves far slower. There can often exist an imbalance between the legal authority of the state vice the capabilities of an individual or group of interest or indeed the intelligence agencies themselves.

U - Sea Lanes of Communication (SLOC), Domestic Terrorism and Crime, Model democracy, ICT interception, Computer Virus and worms such as ***Stuxnet.***[Iranian Uranium centrifuge interference]. Current media issues before the Levinson Inquiry [UK], Australian examples such as ***MEDIVET.*** Social media and its environs, and potential monitoring. The discussion paper and its terms of reference all shape this document. All of these are counterparty issues before us, provide an interesting opportunity. I urge you to take the 15 Minutes to read the whole submission.

U -In this summary I can not possibly cover all of the above. However I pose one very important question. How much power should a state have to monitor its own citizens in a healthy democracy such as Australia? We are a progressive modern nation that often has robust political and ethical debate. Issues before the committee in their consideration and ultimate resolution should all heed the legal protections granted to citizens of any healthy democracy.

U -The strategic question is this. What are reasonable powers of a state vice the rights of privacy and freedom of expression of its citizens? That is the real question to be satisfied. What are the expectations of all Australians – Sociologically, is the state more important than the individual? Do the inferred desires of the nation's population override the rights of the individual? These are relevant questions for any governmental intelligence agency.

R – I have personally witnessed the damage done by poor intelligence interpretation, collection and use of irrelevant facts or allegations by DSA in the PV and NV process. Increased access for individuals not capable of understanding raw intelligence can do a great deal of damage tactically and strategically to various capabilities. This too bears careful consideration in the granting of extra surveillance powers. Who can preform the surveillance, and for what reasons?

Introduction.

U - Intelligence its collection, evaluation, distribution and review, form the back bone of Australia's policy stance over the last few decades of 'Defence in Depth'[Policy], its strategic posture in the Asia Pacific region, and most importantly its security.

U - Australia has a complex, in depth intelligence apparatus, presently in place to preform all the necessary functions in the Intelligence Cycle. In considering the need for change in collection powers, as highlighted by the discussion paper and its terms of reference, there must be due diligence paid to the rights of individual Australian citizens to go about their lives, with out inappropriate interference or surveillance. The argument of, 'just in case' is not conducive with the spirit *[Jurisprudence]* of our legal system, which, is based on the premise of procedural fairness and natural justice for all before the law.

In this submission I intend to outline:

1, My Strong Objections to increased powers of surveillance by the state on its Citizens, with out strong reasonable cause.
2, My understanding of the complex intelligence landscape, as well as the current legal framework. In addition, its the legal safety regarding to public privacy.
3. The need for strong defined privacy controls on all information regardless of its origin.
4. Current technology is already capable of achieving outstanding results with out increased surveillance powers on ordinary citizens.
5. The need for balance in the argument. The state does need to monitor criminal activity and strategic military and intelligence threats. This is a vital function of Government and defence. This should and must be balanced against citizens individual rights.
6. With rights come responsibilities, for all parties Government and citizens alike.

Strategic considerations of a Geopolitical nature.

Sea Lanes of Communication (SLOC)

U- The North west approaches to Australia have traditionally been seen as the potential origin for any threats. Jindalee OTHR and other apparatus pay heed to this threat. Australia is a Maritime dependant nation. 97% of trade is maritime in origin, and strategic changes, such as separatist movements; people smuggling and international maritime crime, represent a potential threat to the movement of trade through the traditionally important straights such as the SUNDA and LOMBOK Straights. Because of this strategic reliance on trade these **SLOC's** and their protection is vital to Australia and its interests. As such monitoring them are of vital importance.

U - Scenario's such as **JI** [*Jemah' Islamiah'*] taking control the strategic straights, thus, forcing maritime trade from Asia to take another route, prices of commodities would quickly rise, and perhaps create a degree of instability with in Australia its self. This type of threat is with in the prevue of the ADF and its intelligence Agencies.

U - Movement of People through the North\ Western sea approaches is also a threat to national security, and needs to be monitored. People smuggling and persons with un checkable backgrounds attempting to enter Australia for what ever purpose, also pose a significant threat, particularly if the individuals concerned wish to 'continue the fight' here on Australian soil. Movement of people through the Northern Approaches is within the responsibility of the ADF and its intelligence apparatus as well as, the Dept of Foreign affairs and its various operational methodologies.

R - It is worth noting that traditional Naval power can not police littoral waters where terrorist activity is often rampant. In fact the presence of a warship of the coast may assist recruitment drives in poor marginalised areas to our North. Intelligence may serve to assist the effort against terrorism, but traditional ADF resources are limited by physical constraints and international legal constraints. International law also governs the activities of intelligence gathering. Innocent passage of warships being a case in point.

Australia's Internal Intelligence landscape.

Domestic Terrorism and Crime.

U - When contemplating terrorism, one is forced to the conclusion that acts of terrorism are by their very nature criminal acts. Committed on a sovereign nations soil against a perceived 'Target' by issue motivated groups weather they be of a radicalised nature or a criminal element. Unfortunately Australia's has not been immune to domestic terrorist attacks. The Brisbane Wisky A Go Go attack in the 1970's and the National Crime Authority attack in South Australia in the late 1980's are two such acts that come to mind.

U - These events were very definitely in the criminal category. The role of Organised crime in these attacks can not be over looked. My view on a criminal act may differ from that of supposed experts. The stock standard non state actors committing these acts, In these matters it is best to take the simplest approach. Regardless of its reasons for occurring in my considered view, they are designed to have devastating criminal like outcomes, in Physical death and injury and on going suffering, often for no tangible reason for the victims.

C - Outlaw Motorcycle gangs and other gang type organisations have represented a significant and increasing threat both through potential violence and control of the drug trade, Illegal weapons and other vice. These groups represent a very real danger to the community. These organisations tend to have international partners, and a well developed corporate structure. A cooperative approach is needed, that is obvious. But a genuine risk to the safety of the community must exist, and evidence to that effect has to support this view. Un published legislation all ready exists to deal with this exact threat. The AFP can already call on the ADF Intelligence apparatus through a warrant and other legal avenues to collect against these groups with in Australia. It already exists. Why erode the privacy rights of the majority because of the few?

R - The right of association is a valuable and important political right afforded to Australian Citizens. It is enshrined in law. It a very important part of the democratic process. Reasonable suspicion, and sound logical legal arguments, rather than emotive arguments, are what deliver a warrant. These groups are communications savvy. HUMINT often is the only avenue to collect and understand the structure and ***modus operandai*** of a target group or organisation. Although it is fair to say that ICT Penetration of standalone laptops can offer an insight to the business model of these groups. Again this should be a last resort and heavily governed by a warrant and its independent oversight.

U- Criminal acts fall into the jurisdiction of the AFP and to a lesser extent ASIO. The Australian Defence force and its associated intelligence agencies are not equipped, or even allowed under various sections of legislation to "collect' against Australians on a wide scale. with in Australian Territories, that is with out a particular kind of Warrant. Members of the ADF at this point in time are not trained to deal with internal issues. Nor should they be. The Joint Intelligence Committee needs to really think this one though. OMG legislation has already caused an uproar in many circles.

[R] – There is a body of law of a sensitive nature within the intelligence community, that provides its governance. But from the strict jurisprudence prospective how can one comply with a law that not reasonably known or available to an individual or organisation. This goes to the heart of our legal system. ASIO's Powers were tested in dealing with *Mohammed Haneef.* From a community prospective serious questions were raised, in relation to - examination of Evidence, - challenging it in court, and - examination of those who make the allegations. This is the basic operating premise of our court system in Australia and its criminal justice system, or *Heabeaus Corpus.*

The Lucky Country – Model democracy

U - Australia's domestic democracy is often touted as a model system, which other nations in the region should seek to emulate. Australia is often critical of Military Junta's or Governments in Sovereign nations that are clearly involved in Human Rights abuses, Australia, has in the past been very critical of internal intelligence apparatus used to monitor the political behaviour or association of their own citizens. To maintain this 'moral high ground' Australia should not embark such surveillance measures with in Australia particularly with the stated aim of protecting Australian citizens. When it has the appearance that security may not be the primary motivator. It would perhaps be better received if this motivation was clearly and unambiguously articulated. Who stands to gain, and who or what is in the sights.

U - Any Government which seeks to use its military or military apparatus against its civilian population, in **ANY** way, is travelling down a very dangerous road. Aid to the civil community [ADF] is not the same. Aid to the civil community is well received and appreciated by the community at large in times of need, such as natural disasters and the like. Not national security.

U - The Australian public at large, if fully informed of the plans for unbridled surveillance will emphatically reject the premise that the government needs these types of surveillance powers against the very public that elects them. It is arrogant at best and dangerous and undemocratic at worst. The ADF is not suited to policing role with in Australia.

Legal protection from unlawful interception or interference.

U- Legal Warrants issued for intelligence or evidentiary purposes are issued by an independent arbiter, a member of the judiciary. This is a vital part of the legal system that goes to the very heart of *Habeas Corpus* rights. Those very basic rights that so many have sacrificed their lives or health for; against various regimes, over the last century that have sleeked to remove basic human rights from a populace.

U - With a degree of scrutiny, comes legal surety in a collection process that ultimately delivers evidence that is '***Legally Sound***' and in accordance with the relevant act of Legislation. Members of the Judiciary are there because they uphold expected community standards. The 'TIA' is legally complex for two obvious reasons. The common law precedents and the legal protections built in to the Act are as important now as they were in 1979, and should be important in 2079.

U - Simplifying warrants so that members of the AFP/ASIO/state police services can safely, with respect to the *Privacy Ac*t 1988, respecting the communities right at large to privacy be issued. Simplifying or streamlining Modernising ect should and **must not** signal a cart blanch freedom to collect on every citizen. The logistics of such would be horrendously expensive. And highly inappropriate. Australia does not need a J Edgar Hoover Dosser type compiler as the vanguard of Australia's domestic security. There is no need what so ever to maintain 'files' on individuals who are not suspected of committing any crime. The view in the discussion paper of 'Just in case' or discovering plots before they reach critical mass is simply rubbish.

R - With extremely powerful ICT capabilities in the Deakin Defence Building and DSD provide an amazing detection tool that is often tagged as ESCHELON. Now this is a Hollywood title. But key word and .EXE file search techniques are well reported in open source resources. Such highly advanced capabilities in the modern Cyber context have lead to prosecutions and investigations. It is a well known capability. Why does there need to be an increase in this already very advanced capability, that is clearly inward looking on Australia's ICT Network.

The domestic Intelligence landscape

Communications Interception

U - Communications between persons has been at the heart of Intelligence agencies activities for centuries. HUMINT COMINT ELINT SIGINT and so on, are reliant on interception of communication. The Australian apparatus has long had a focus on intercepting and analysing strategic communications emanating from nation states usually traffic that is military or diplomatic in nature. This is well known and well reported in open source mediums.

U -Where the water gets a little murky is the interception of telephony [voice] between individuals. The interception of communications on the Public Switched Telephone Network or the PSTN again is well known. In 1979 the 'TIA' was created with the aim of collecting evidence against criminal organisations. Largely it was the responsibility of the Police to collect warrants to 'Tap' a phone line. Times have indeed changed. So has technology as well as community standards.

[R] -The proliferation of wireless technology has seen a massive jump in the volume and the complexity of the medium. It is not simply Analogue voice but a range of data packets that may not necessarily be reconstruct when intercepted. In addition there are a number of various communications paths taken by service providers. Various companies sell space / time to service providers to access their companies communications links, such is the example with Queensland Railways providing Optus access to QR's data link. And there are a range of others. Basically to have access to all of this data, the network required would be massive, The cost will be horrendous, which will no doubt be passed on to consumers, again, like another price on something, that wasn't going to happen.

U -How ridiculous a premise, that is to have to pay a levy or fee so the government or their appointed agency can monitor your sensitive private communications. The premise is just ludicrous and begs the question Why? What is so important to the government to have access to that will require the consumer to pay a levy to facilitate the surveillance.

U - When looking at the interception regime analytically are there deeper motives at play here. Asking companies to develop and maintain a system of records of communications transactions and the data passed will in its self be a large expensive undertaking. But the recent phone hacking scandal at **News of the World** and others in the UK should serve as a timely warning about the dangers of the un regulated access to stored communications data and communications transactions.

U - The simple fact of physics is that if it is technically possible in the UK it is possible here. In fact no doubt it has happened and is still happening as the Finkelstine report hinted at. Not every employee in the telecommunications industry is beyond reproach. Selling access to private communications transactions, to make a quick buck, and a story from private communications, is in my mind so far from reasonable it verges on the Insane. The testimony before the Levinson Inquiry in the UK, is very frightening, indeed, one would hope the Intelligence community and the Government are watching that very closely.

Intelligence issues and problems.

U -Recently, we have seen many examples of when intelligence gets the picture wrong or worse yet intelligence is twisted in to propaganda. In his book "Axis of Decit" Wilkie did not paint a rosy picture of the miss use and deliberate miss interpretation of intelligence in the recent conflict in Iraq.

U -This is not Isolated. Countless commentators at the time stated there were no weapons of mass destruction WMD in Iraq. Al jezzera accurately reported at the time, when its office was Bombed in Bagdad, that the war was more about removing one government no longer friendly with the west and replacing it with another regime that made energy security to the US far easier. Intelligence was miss used and many 'lies' were told. This is plainly on the public record now. – A valuable lesson. What is past is prologue.

U - At the famous UN Security briefing by Colin Powel Just prior to the War comes to mind, Complex graphics talking of special phone Intercepts and the like. Was all fabricated. Some of the transcripts played did not even translate in to the script that was played. Al Jezzeria reported on this at the time and whilst it gained little traction

in the western media it certainly gained traction in the non western government controlled media. It was embarrassing to say the least, and placed the intelligence community at odds with its government. A bit of a concern.

U - Professional intelligence officers take a great deal of pride in their finished product, to twist and turn it, is a slap in the face to the men and women that work so very hard in that field to present the most accurate picture possible to decision makers.

U - Scott Ritter in his Book "Target Iran" also carefully explains how intelligence has been twisted to suit an agenda rather than the truth. And eventually how this miss representation of intelligence was so costly that the blunder allowed Iran to develop a potential Nuclear capability thanks to Pakistan's Nuclear program. When it could have been stopped, it wasn't because there was a complete lack of faith in the information being provided.

MEDIVET

U - A bit closer to home, a medical company is having difficulty in complying and implementing ICT security under the current Privacy Act. This company was allowing its information on sensitive private Paternity or Illicit Drug testing to be cached by Google. This is a very clear example of locally incompetent ICT procedures that can be exploited. Increasing the availability of surveillance and monitoring powers will not stop or decrease incidents of the above nature, rather it will only serve to increase the potential for violations of security and or very sensitive leaks, as is the present case, reported by the Australian Newspaper 05 Aug 2012.

Stuxnet worm – Iranian Neculear program.

R – I am reluctant to comment to much on this topic. However it does illustrate the capabilities that are out there. State generated Malware to intefere with industrial processes[Seimens PLC and plant systems software]. It may have been warranted in the case of Iran. But requiring communications to be routed over a particular network or network feature [discussion paper], Malware can and or could be inserted to achieve a stratigic or tactical aim. It also illustrates that intercepts can be created.

R - It is clear that this legislation before the committee is to prehaps legalise or legimimise the current murky practices by state players, and Australia dabbles in this too, is a really freighnening prospect. The power available in this case, the ability to even create the kinds of data traffic that would draw suspicion is of grave concern. The internet is almost limitless, so to is the potential for practices and actions by state players that are really concerning. These kinds of practices are coming out of the shadows. Remote access, remote control Remote action is a part of this landscape that has to be considered with the rest to the TIA and the communications interception changes planned.

The discussion paper and Terms of Reference

U - Interestingly in the Terms of reference for the discussion paper on the proposed reforms "*As a result, Communications can not be guaranteed to pass over any particular path and therefore it may be necessary to attempt to direct the communications over a particular path to facilitate Interception*" Would this also enable altering of the communications to suit the particular addenda or tactical need?

U - Social Media collection demands illustrate that it is motivated by something other than security of the state. This is where the intent is truly unveiled. Perhaps security of the proletariat or a political outcome. Social media is about the expression of ideas, and personal communication. Why would it be necessary to police monitor and collect information on peoples ideas and thoughts and feelings if there was not a higher goal in mind, to prepare files on every person in the nation of Australia.

U - At a glance this seems so far out and outlandish. It just could not happen in Australia. **At the moment**. But recent events in the Middle East perhaps have served as a wake up call. The Arab Spring as it has been coined started as a social media event. This possibly has governments worried that true democracy, the consistent voice of the citizens that PAY the wages and entitlements, provide a power base and support the proletariat, are in the sights. Are seen as unhelpful, Are seen as a risk. and needs to be monitored because an individual may have a face book page that does not suit the governments view. No that is not the Australia I fought and defended. It sounds a bit like China though. Where political dissidents are put in 'Protective Custody' their online details are fished through looking for any dissent against the party. Supported by Google and Microsoft. Commercial imperatives supporting basic human rights abuses. Suppression of ideas, and freedom of assembly.

U - Is this where we want to go with monitoring. Because it will all go wrong very quickly from that point on. The freedoms and values of the Australian public have been hard fought and won. A technocratic government using the agencies of the ADF intelligence community to collect on our own citizens, is a very precarious position for any nation state to be in, where fear and abuse of power, are the hallmarks rather that positive, progressive leadership of a well established and safe democracy.

Conclusions

U - Intelligence and its use is important to Australia's ongoing safety security and prosperity. There have been many recent abuses and misuses of intelligence and intelligence related material. Requiring ISP and Phone providers to increase their records to satisfy something that might perhaps happen, is outlandish. It will increase cost and red tape to communications consumers. With constant increases in the cost of living Australian citizens don't need this extra burden for no real tangible reward.

U - It is a matter of public record that a number of Terrorist attacks have been foiled by the outstanding work of the Intelligence community and AFP/State police forces. I don't however see the need for local enforcement agencies dealing with very low level compliance offences having a need to access this kind of stored communications data. Clearly, by the actions of the relevant agencies in foiling these attacks there is enough capability in the hands of those who need it. Imagine the local council intercepting communications because there is a face book page about how to get around parking fines and environmental levies. Whilst this is not the intent of the proposed reforms, but once the flood gates are open it is difficult to close them again.

U - The legal system may be complex with regard to the TIA, the definition of a computer, and other communications interception needs. But the law needs to be. The AFP and ASIO need to remember that they are public agencies, serving the public interest. Not the other way about. If matters are complex, then so be it. I do not see the need to Modernise or Streamline to make things easier, to address lack of

planning or some other issue with in those organisations. They have a responsibility to the tax payers of Australia to work with in the law. It is there to protect everybody, from the exact kind of technocratic super state, where personal rights and freedoms are not important. That is not a country I would choose to live in.

U - Strengthening public privacy, and not just lip service, but actual, gazetted laws that enforce privacy from abuse. That is the only increase in powers I would advocate, and support. Privacy is important, it is valuable, and once lost can never ever be replaced. In a sense it is part of the Australian identity. There must be a balance struck between the needs of the state in security matters and the rights of Citizens who are doing nothing wrong in the first place.

U - Consideration should also be given to the psychological burden on ADF members being required to spy on Australian Citizens with in Australia. ADF Members at large are not keen on this. They well know of overseas examples of internal military monitoring. These Australians are Motivated, keen loyal and Intelligent. They well know the risks. Imagine the situation where a member is required to monitor or intercept information on their neighbours friends ect. This Psychological cost needs consideration. And is does represent a very real issue.

U - Vetting and Psychological assessment goes some way to mitigate this. Vetting aside, this is a very stressful position to put those members in to when they are already in a risky profession. They don't receive the training that Police and Civilian governmental agencies receive. And at a time where there numerable defence cutbacks on various programs including ADF Health, this is an added cost burden. If this regime were to go ahead would this health issue just be brushed aside. These members are highly valuable, and should be well looked after. A home grown PTSD would not auger well for the ADF.

U - And vetting does not always work, a recent example, SBLT Delisle in the Canadian Armed Forces as reported in the Australian and other papers had some personal issue or motivation, and leaked information that was VERY damaging to some programs here. Whilst Psychological checks are made during the PV and increasingly the NV process protecting against this kind of leak falls back on good old personnel security management practices that have seemed to fall by the way side as DSA peruse the more glamorous; Counter Intelligence roles.

R - I know this from personal experience during my YEARS as a USO at various units handling vetting packs, and DSA's, seeming inability to deal with information. It has been reported widely that DSA has made some improvements. The PV Process is quite in depth, it is designed to be. Not withstanding this there are 3 Australian cases in the last 10 yeas, and numerous cases overseas where vetted individuals have gone along fine then, for one reason or another, revealed information they should not have. Conversely the DIG PV has seen fit to withhold clearances on clearly suitable loyal members of the ADF who are deemed immature or don't have life experience.

R - It was, later explained to me [by DSA, now known as AGSVA],as not having a degree or such other life experience. So what can be expected when DSA openly prefers the university graduates who have been probably exposed to university politics, or radicalised in one way or another. Students are often exposed to this during their degrees at one time or another a protest seems like a good idea until they are in a cell some where. Some of these ideas and deep ideology can be held privately for many years until the right trigger comes along. And unfortunately it does often arise, as we have seen in Australia over the past ten years with defence civilians trying to sell or reveal information, who in fact had their PV.

R - Again this is first hand experience where I witnessed a number of young Australians at RAN – RS complete their RAN RS training and were excellent Recruits, motivated, and observed very closely over 12 weeks. They were keen but young who had their clearance withheld. This had a devastating effect particularly on young females, who, were forced in to career choices that they didn't want. Going from an EWL to a steward is very embarrassing, when the individual has done nothing wrong. Perception is everything. I personally witnessed this at least 12 times, that I can readily recall.

R -This is highly relevant because, it is conceivable that increased surveillance powers would also be granted to vetting officers, who quite frankly could not assess raw or even processed intelligence. Trolling though candidates PC's remotely ect with out giving them a chance to explain or put their case forward. DSA has hindered ADF capability, by withholding clearances of a number of highly talented linguists who entered the ADF with very good highly prised language skills in a particular area different to the standard language training, which, at the very same time widely advertising that anyone with the particular target language should come forward. That was a disgusting sequence of events, and again highlights failures of analysis capabilities. So raw intelligence in the hands of those in a position to do damage but not in a position to actually understand it is a very real issue, relevant to the need to increase surveillance powers, and should be of great concern. [04 – 07] (*It should be noted I am not referring to my own PV experience, rather observed processes over a lengthy period)*

U - Public perception is everything. It changes governments and brings about social change. I am confident that the overwhelming public opinion on this matter would strongly reject the idea that increasing the TIA / ICT interception regime, casting the net wider and further 'just in case' will be seen as absolutely unacceptable, and unnecessary.

Submission by

A.A.Halter
LEUT,RAN (Retired List)
12 August 2012