SPEECH

Disruption can be caused by the smallest of things - all it needs is to find a way in. In the hands of an enemy disruption is always looking for an opportunity.

To demonstrate this point I will play a short video clip – viewer discretion is advised – as some will find this footage very disturbing.

Play video

Yes they are my children

Distinguished Guest Ladies and Gentlemen

Disruption and Resilience are two words that we - in the military - should be familiar with. We should also be aware that they are inextricably linked.

Generally speaking - those who have faced significant disruption are the most resilient – and those who wish to disrupt…had best be resilient.

So, using the link between disruption and resilience – have we as airmen - paused and thought ‘how resilient is modern Air Power’. For decades Air Power - in most conflicts since WWII – has - over the battlefield largely had its own way.

Over that same period we have pursued, sometimes blindly, the advantages of a fully networked system – both airborne and on the ground. Has the establishment of air superiority - and the lack of a sophisticated electronic warfare threat that we have become accustomed to in Afghanistan and Iraq - added to this blindness?

Have we been too quick to adopt technology that offers improved networking and communications while paying lip service to resilience?

As technically focused professionals we as airman must remember our weakness – which is that we pursue technology without always thinking deeply about the complexities and vulnerabilities it imports. Today – more than ever, the benefits of technology must be balanced against the risks.

The largely unopposed use of airpower in the Middle East saw the fielding of unmanned systems without encrypted links. While the Taliban had little capability to intercept these links - we forgot that others on the periphery did – and that they gained a bird's eye view of tactics and procedures - and in some cases full platform ownership.

My opening question on the resilience of modern Air Power would lead the listener to think that I am going to focus my speech skyward – I am not.

I will focus on the need to improve our resilience against cyber and information warfare threats - regardless of the domain.

You might be surprised to learn that - for an Air Force officer - the outcome that I seek is not to buy – yet - another piece of equipment at the expense of the other Services---------- - But that I call to arms all our Service personnel to awaken to the threat – adopt the right attitude - stand your ground – remain vigilant against a clever and elusive enemy – and to take up the fight and protect your Nation.

While such words should **motivate** all concerned the human psyche - while complex - is dominantly primal. Therefore, we must **educate** our psyche about this new threat called cyber – a threat - that has no physical form. This way we can begin to address the challenges of delivering air power in an age of disruption.

You are well aware of the rapid proliferation of asymmetric cyber capabilities, which, due to reducing barriers of entry, are now readily available to a wide spectrum of actors.

I need not stray into sensitive areas but note that our own Defence systems have been subjected to intrusion and deliberate targeting. So too, have many high profile Australian businesses. Likewise, there is a wealth of open source data on operations against the Ukraine. All of which are instructive.

Such operations are well within non- aligned nation's capabilities and they, along with other powers - whose interests are harmful to ours - are rapidly developing capabilities and doctrine to exploit us.

2017 saw a 15% increase – over 2016 figures - in cyber security incidents. Of the 47,000 events in 2017 - **671** of were considered serious enough to warrant an operational response from the Australian Signals Directorate.

All of what I have just said, when mixed with Hollywood movies and the media, would lead one to think that to exploit a modern military, and undertake cyber-attacks, requires a highly sophisticated adversary and that our only defence is to have an equally sophisticated response and impervious systems.

Let us not forget context – so while it is true that we must have sophisticated responses and strong systems - leaving it to advanced training and systems architecture to mitigate weaknesses - largely ignores the major problem. I offer a more pedestrian way to substantially improve our security – **How?** - We can do it by changing our attitude. **Why?**

‘**Because we are making it too God damn easy for the enemy’.**

Exploitation and disruption are not that complex to achieve – particularly when the electronic environment is so pervasive. The **'in'** that an adversary may use is generally along the seams that we, through the blind pursuit of social acceptance, technological advances, convenience and commercial gain have made available.

Now - when we add the human element – which was the **'in'** that lead to the compromise of the enigma machine – then a more pedestrian solution to improve our resilience begins to stack up.

So strong is our focus on the technical that, to our peril, we can fall into the trap of defining cyber as an exclusively technical issue.

Stripped of all technical jargon we should remember that most cyber operations involve age old elements of war, such as subversion, sabotage and espionage.

While funding efforts to improve network resilience makes sense - we have the awkward propensity to overlook one of the biggest threats – ourselves.

Humans need context to shape their actions and responses --- but when the context is difficult to grasp –--- difficult to see – or when it is so pervasive that it becomes normalized – then we can lose focus.

This is equally true in other areas – as I am sure many of you in this room - whilst in the Middle East - have witnessed the widespread use of mobile phones and open lines to discuss the movements of aircraft and other important events.

How will we all fare when the stakes are higher? Are we capable of changing destructive habits – habits that have been learnt over the past 15 years?

Additionally, many do not think twice about posting information on social sites – all of which can be used by an adversary – the integration of technology into our lives has been so rapid and so pervasive – the convenience has been like a drug - that we resist at first - but then quickly succumb to and forever forget the risks.

When you add an insidious trend -- where some maladjusted people think - perhaps motivated by those who wish to access our data – 'that all classified information should be made available' then you are open to disruption and cut the throat of resilience.

We must remind ourselves that cyber and information warfare are a threat - and when they are done well they are almost imperceptible.

Importantly we must also remember that we are meshed in a conflict with no end-date. Cyber and information warfare is not something that is not going to happen - it is happening now – it will always happen.

We set the scene well when we enter a conflict zone – pre-deployment training, weapons handling and IED awareness - and we generally have an end date – all of this provides context – it frames our responses – it gets us into the right mindset to deal with a threat.

The context now for our sailors, soldiers and airman is that – deployed or otherwise – they must have the right security mindset every single day, because there are no physical borders associated with cyber and information warfare.

Disappointingly for some – improvements to our security require no additional funding or personnel – it requires the adoption of a warrior's mindset.

For a warrior would not stick a dongle they found in a carpark into our computer system – **the naive would** – a warrior would not put their password on a sticky label – **the weak would** – a warrior would not activate WIFI on a sensitive network – **a moron would**.

I estimate that we spend - at the very minimum - 60 000 hours a year undertaking weapons training – not to be better shots but to prevent us from shooting ourselves - or worse those on the same team.

The old adage of 'familiarity breeds contempt' is as relevant to the breaking of the enigma machine as it is to cyber intrusion and electronic intelligence gathering.

Only last year, the number of security breaches detected by our cyber Red Teams, on Talisman Sabre, were simply unacceptable. Very early in this exercise, locations of named individuals and the movements of units were discovered on an embarrassing scale. The most egregious act was the posting of a battle map on social media. **No warrior would do that!**

Not having your head in the fight sees you think that your life is so interesting and important that everyone on social media should participate in it – it's like flipping the safety off your rifle and pointing it at the head of your best friend.

So what is the problem here? Does it come back to the human psyche - **in that we have trouble understanding the intangible** - something like cyberspace that we can neither see nor touch.

To elaborate this very point let us talk about a recent example of a tangible security incident.

Most of you would be aware of the recent loss a classified filing cabinet in Canberra. This story gained considerable traction in the media. On this incident we - and the general public – instantly grasped the issue and the resultant security ramifications. There were images of a filing cabinet - data was visible ----- **How very Primal.**

However, at the same time there were actors seeking ways to extract volumes of data from public and government systems that would dwarf that found in the cabinet.

Over that same period I wondered how many people left their computer unlocked while they walked away from their desk - if all system administrators were diligently sanitizing their networks - how many **'ins'** had we provided the enemy.

We also have trouble understanding how something - such as connectivity - can harm us – as it seems to the majority to be a benefit. The same could be said for alcohol. Is it that we enjoy the benefits of what this networked world provides - both publically and in the military - and that we are subconsciously placing convenience ahead of security?

We must therefore have a discussion about convenience over security. The only difference between Unclassified and Top Secret is inconvenience.

If we have a mindset of convenience over security with our networks then we must think how far we interconnect these systems. This is a challenge for all domains. As the more you connect - the greater is your exposure to the risk of disruption. You open seams and provide **ins.**

Inconvenient – **absolutely** – but to go down the path of full connectivity without thought - disarms us as warriors.

If you decide to expand and interconnect your networks then you must invest in resilience. To do otherwise ignores that the enemy is awake and hunting.

A vital part of resilience is raising awareness of risk without creating alarm. ‘Loose Lips Sink Ships’ so very old school - so very effective.

We must reassure people that we can and will develop redundancy and alternatives for a range of activities we take for granted. Wishing this problem away is not a solution. The ADF bears a special responsibility in this domain.

Work has begun to improve our resilience --- Defence is cyber certifying existing platforms and networks before they can be used in operations. This will take considerable effort ------but it is a sign that we are awake to the threat, and acknowledge the need to prepare our forces to operate in all warfighting domains --including cyberspace.

Additionally, discussions have begun on how far Defence pursues connectivity – this is an important discussion that has in the past not had the level of debate it should have. Previous discussion centred on benefits rather than risks. We must have a more deliberate and informed debate on such matters. This applies equally to the public space.

In 2017 Defence formed a Joint Cyber Unit - in January this year it established the Defence SIGINT and Cyber Command.

Additionally, Defence continues to strengthen relationship with key Government agencies so as to fully understand potential **seams and ins** in our systems --This is a Team effort.

With the assistance of US Cyber Command a succession of accelerated – defensive - cyber courses are underway. Also we are strengthening our cyber and information warfare awareness campaigns – we will shortly come phishing for you!

We continue to **imbue** our sailors, soldiers and airmen with the initiative to improvise and to carry on when our systems are disrupted. ‘Fight Hurt’ is a catch cry of the Unites States Marine Corp. We would do well to adopt it.

People are the key to all forms of warfare. And resilient people are right at the heart of it. By raising the awareness of the threat we will know where resilience ceases to be a technical issue and becomes a human one.

In the end resilience is about attitude – it is about being a warrior at home and when deployed.

To achieve the best level of resilience----**and that must be our collective goal** - we must first wake up and realise that we are in a fight – every single day – and those things called cyber and information warfare are real.

Remember - while you sleep your enemy studies your weaknesses.

Slide on twitter