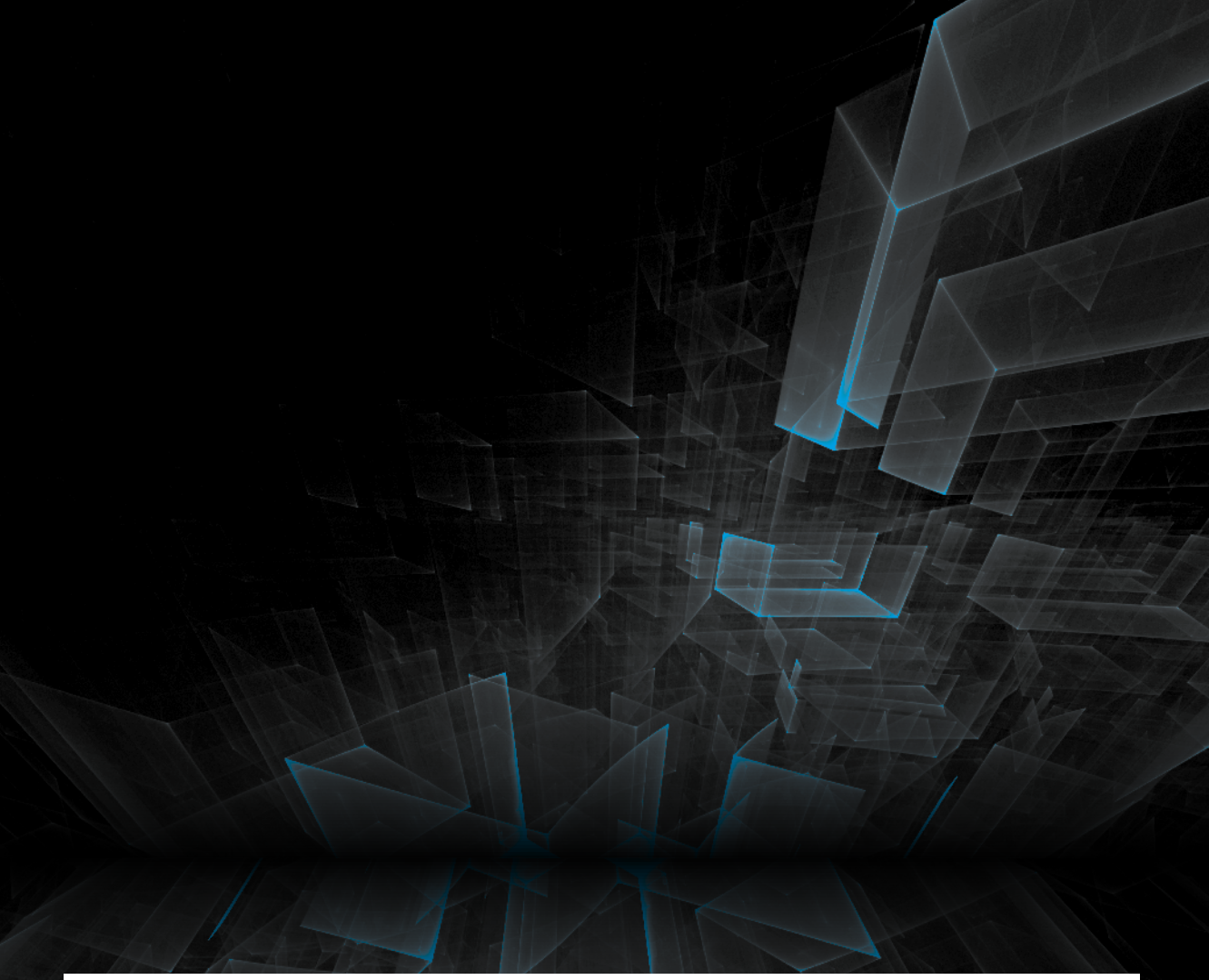

BOEING

L3 Technologies

Rolls-Royce

Defence Bank

Proceedings of the 2018 Air Power Conference

Air Power in a Disruptive World

20–21 March 2018
National Convention Centre, Canberra

Air Power in a Disruptive World

PROCEEDINGS OF THE 2018 RAAF AIR POWER CONFERENCE

NATIONAL CONVENTION CENTRE, CANBERRA
20-21 MARCH 2016

Disclaimer

The views expressed are those of the authors and conference participants, and do not necessarily reflect the official policy or position of the Department of Defence, the Royal Australian Air Force or the Government of Australia, or the official policy or position of the respective armed forces or governments of the overseas participants. The Commonwealth of Australia will not be legally responsible in contract, tort or otherwise, for any statements made in this record of proceedings.

Release

This document is approved for public release. Portions of this document may be quoted or reproduced without permission, provided a standard source credit is included.

National Library of Australia Cataloguing-in-Publication entry

Published by:

Air Power Development Centre
Department of Defence
PO Box 7932
CANBERRA BC ACT 2610
AUSTRALIA

Telephone: + 61 2 6128 7051 Facsimile: + 61 2 6128 7053
Email: airpower@defence.gov.au Website: www.airforce.gov.au/airpower

THE AIR POWER DEVELOPMENT CENTRE

The Air Power Development Centre (APDC) was established by the Royal Australian Air Force in August 1989 at the direction of the then Chief of the Air Staff. Originally known as the Air Power Studies Centre, it was renamed the Aerospace Centre in 2000 and then became the Air Power Development Centre in 2004.

Its function is to promote a greater understanding of the proper application of air and space power within the Australian Defence Force and in the wider community. This is achieved through a variety of methods, including development and revision of indigenous doctrine, the incorporation of that doctrine into all levels of RAAF training, and increasing the level of air and space power awareness across the broadest possible spectrum.

Over the years, the APDC has evolved into an agency that provides subject matter expertise for air and space power education and has a well-developed publication program.

Comment on these proceedings or inquiry on any other air power–related topic is welcome and should be forwarded to:

The Director
Air Power Development Centre
Department of Defence
PO Box 7932
CANBERRA BC ACT 2610
AUSTRALIA

Contents

Notes on Contributors

Air Marshal Leo Davies, AO, CSC

Air Marshal Leo Davies joined the Royal Australian Air Force as a cadet Navigator in 1979 and graduated to fly P-3B and P-3C Orion aircraft with Number 11 Squadron at Edinburgh in South Australia. In 1987 Air Marshal Davies completed pilot training and after completing F-111 conversion course was posted in 1988 to Number 1 Squadron at RAAF Base Amberley.

In 1990, Air Marshal Davies was posted to Cannon Air Force Base, New Mexico, to fly F-111D aircraft on exchange with the United States Air Force. On return to Australia in 1993 Air Marshal Davies was posted to Number 1 Squadron as the Operations Flight Commander followed by one year as Operations Officer at Headquarters Number 82 Wing during 1996. After a posting in 1997 and 1998 as the Executive Officer at Number 1 Squadron, Air Marshal Davies completed RAAF Command and Staff Course. In 2000, he commenced two years in Capability Systems within Defence Headquarters.

In 2002 and 2003, Air Marshal Davies' long association with Number 1 Squadron was again rekindled when he returned as Commanding Officer and achieved 2000 hours flying the F-111. He was the Staff Officer to the Chief of Air Force during 2004, before taking up the post of Officer Commanding Number 82 Wing at RAAF Base Amberley, where he was awarded a Conspicuous Service Cross (CSC) for outstanding achievement.

Air Marshal Davies worked as Director Combat Capability within Air Force Headquarters in 2006 and 2007, during which he was deployed to the Middle East to work within the Combined Air Operations Centre. In 2008 he was the Director General Capability Planning within Air Force Headquarters until 2010, when he was posted to Washington as the Air Attaché where he was awarded the United States Legion of Merit – Officer for his work. Air Marshal Davies returned from Washington in January 2012 to commence his appointment as Deputy Chief of Air Force.

Air Marshal Davies was appointed an Officer of the Order of Australia (AO) in 2014 for distinguished service to the Australian Defence Force in senior command and staff appointments. He was promoted to Air Marshal and appointed to Chief of Air Force on 4 July 2015.

He is married to Rhonda who is a Registered Nurse and they have two children; Erin who is herself a Registered Nurse (midwife) and Jacob.

Senator the Hon Marise Payne

Marise Payne is Australia's 53rd Minister for Defence.

She was sworn in on 21 September 2015 after previously serving as the Minister for Human Services for two years.

She has more than two decades Parliamentary experience after filling a casual vacancy in 1997 to represent the people of New South Wales in the Australian Senate.

During her parliamentary career she has served as Shadow Minister for Indigenous Development and Employment, Shadow Minister for COAG [Council of Australian Governments] and Shadow Minister for Housing.

She has been a member of a number of Joint and Senate committees, including 12 years on the Joint Standing Committee on Foreign Affairs, Defence and Trade, including a period as Chair of its Human Rights subcommittee.

Prior to entering Parliament Minister Payne worked as political adviser before working as a public affairs adviser in the finance industry.

A member of the Liberal Party since 1982, she was the National Young Liberal Movement's first female President. She also served on the NSW Liberal State Executive for 10 years and at branch and electorate levels.

She and her partner, NSW Minister for Western Sydney, WestConnex, and Sport, Stuart Ayres, live in western Sydney.

Mr Bilahari Kausikan

Mr Bilahari Kausikan is currently Ambassador-at-Large at the Ministry of Foreign Affairs. Prior to this he was the Permanent Secretary of MFA from 2010 to 2013, and Second Permanent Secretary from 2001. He has also held various positions in the Ministry and abroad, including Singapore's Permanent Representative to the United Nations in New York and Ambassador to the Russian Federation.

Mr Kausikan has been awarded the Public Administration Medal (Gold) and the Pingat Jasa Gemilang (Meritorious Service Medal) by the government of Singapore. He has also been awarded the 'Order of Bernardo O'Higgins' with the rank of 'Gran Cruz' by the President of the Republic of Chile and the Oman Civil Merit Order by the Sultan of Oman.

Air Vice-Marshal John Blackburn, AO (Retd)

John Blackburn is an expert in strategic policy, planning, operational command, capability development and material acquisition. He has held many senior positions in the Defence industry and actively consults with the Department of Defence and Industry. A recent publication for NRMA analyzed Australia's Liquid Fuel Security. As Deputy Chief of the Royal Australian Air Force he was responsible for the operations of RAAF headquarters including the whole of RAAF strategic and capability, personnel, financial, logistics policy and planning, as well as the oversight of airworthiness regulation and technical airworthiness.

Rear Admiral Neil Morisetti, CB (Retd)

Neil Morisetti joined University College London in January 2014, initially as the Director of Strategy for the Department of Science, Technology, Engineering and Public Policy, and since September 2016 as Vice Dean (Public Policy) Engineering Sciences. Before that he worked for the UK government, both as an officer in the Royal Navy, where appointments included, Commander UK Maritime Forces and Commandant of the Joint Services Command and Staff College, and latterly in the Foreign and Commonwealth Office. Between 2009 -2013 he acted as the UK Government Climate and Energy Security Envoy, and then the Foreign Secretary's Special Representative for Climate Change. He is a member of the Advisory Boards for the Carbon Disclosure Programme and the Carbon Tracker, whilst in the US he is a member of the Military Advisory Board of the Washington DC based think tank CNA.

Professor Ramesh Thakur

Ramesh Thakur is Director of the Centre for Nuclear Non-Proliferation and Disarmament and Professor in the Crawford School of Public Policy, The Australian National University. He was formerly Senior Vice Rector of the United Nations University (and Assistant Secretary-General of the United Nations). Educated in India and Canada, he has held fulltime academic appointments in Fiji, New Zealand, Canada, and Australia and been a consultant to the Australian, New Zealand and Norwegian governments on arms control, disarmament and international security issues. Professor Thakur was a Commissioner and one of the principal authors of *The Responsibility to Protect* and Principal Writer of Secretary-General Kofi Annan's second reform report; a Distinguished Fellow of the Centre for International Governance Innovation and Foundation Director of the Balsillie School of International Affairs in Waterloo, Ontario; and is presently Co-Convenor of the Asia–Pacific Leadership Network for Nuclear Non-Proliferation and Disarmament (www.a-pln.org), a 90-strong nuclear policy advocacy group that includes several former prime ministers, foreign and defence minister, foreign secretaries, military chiefs and United Nations under-secretaries-general from Asia–Pacific.

Mr Todd Harrison

Todd Harrison is the director of the Aerospace Security Project and the director of Defense Budget Analysis at the Center for Strategic and International Studies in Washington, DC. As a senior fellow at CSIS, he leads the Center's efforts to provide in-depth, nonpartisan research and analysis of space security, air power, and defense funding issues. He has authored publications on trends in the overall defense budget, military space systems, civil space exploration, defense acquisitions, military compensation, military readiness, nuclear forces, and the cost of overseas military operations.

He previously worked at Booz Allen Hamilton where he consulted for the Air Force on satellite communications systems. Mr. Harrison served as a captain in the U.S. Air Force Reserves. He is a graduate of the Massachusetts Institute of Technology with both a B.S. and an M.S. in aeronautics and astronautics.

Dr Thomas X Hammes

In his thirty years in the Marine Corps, T. X. Hammes served at all levels in the operating forces to include command an intelligence battalion, an infantry battalion and the Chemical Biological Incident Response Force. He participated in stabilization operations in Somalia and Iraq as well as training insurgents in various places.

Hammes has a Masters in Historical Research and a Doctorate in Modern History from Oxford University. He is currently a Distinguished Research Fellow at the Institute for National Strategic Studies, National Defense University.

Mr Marc Ablong

Marc Ablong joined the Department of Defence in 1993 after an early career start in the finance and banking industry. During his time with Defence, Marc has held positions in capital equipment & acquisition policy, international policy, military strategy, maritime capability development, Air Force long-range planning, national support, information strategy and futures, strategic reform and strategic policy.

During the development of the 2009 Defence White Paper, Marc was Chief of Staff of the White Paper Team. He was responsible for the coordination of White Paper activities and the provision of strategic advice to the Principal Author.

From March to May 2016, Marc undertook the Advanced Management Program at the Harvard Business School. In July 2016 Marc was appointed First Assistant Secretary Naval Shipbuilding Taskforce to lead the development and delivery of the National Shipbuilding Plan; and from 10 July 2017 concurrently held the role of First Assistant Secretary Defence Industry Policy. On 28 October 2017, Marc commenced in his current role as acting Deputy Secretary Strategic Policy and Intelligence

Major General Kathryn Toohey, AM, CSC

Major General Kathryn Toohey joined the Australian Army in 1987, graduating from the Royal Military College – Duntroon in 1990. Major General Toohey was assigned to the Royal Australian Signals Corps and commenced her military career as a troop commander with the 2nd Signals Regiment.

Major General Toohey went on to serve in the 7th Signals Regiment (Electronic Warfare), the 1st Brigade Headquarters and in the Strategic Operations Division of Headquarters Northern Command. Her other appointments have included a posting as an instructor at the Royal Military College – Army as the Aide-de-Camp to the Governor-General of Australia. In addition, Major General Toohey deployed for a 13 month period as a troop commander in the Force Communications Unit as part of the United Nations Transitional Authority – Cambodia

In 2012, Major General Toohey was assigned directorship of the Capability and Technology Management College (CTMC), an advanced education college providing mid-ranking officers and public servants Masters-level education and training and preparing them for capability lifecycle leadership within CDG and CASG. This role was expanded to include administrative

command of Australia's Federation Guard; command of the Defence Force Chaplains' College and responsibility for the Defence sponsored post-graduate students at UNSW Canberra.

In 2016, Major General Toohey took leave from the Army to assume the statutory appointment of Deputy Electoral Commissioner in the Australian Electoral Commission. Upon her return to the Army in 2017, Major General Toohey was appointed the Head of Army's Land Capability division.

Major General Toohey holds an Executive Masters in Business Management, a Masters of Management in Defence Studies; a Graduate Diploma in Information Technology and a Bachelor of Electrical Engineering (Hons). She is also a graduate of the Australian Joint Command and Staff College.

In 2017, she was conferred with the Medal of the Order of Australia for her service to the Australian Defence Force in the fields of capability development and education.

Vice Admiral Tim Barrett, AO, CSC, RAN

Vice Admiral Tim Barrett, AO, CSC, RAN joined the Royal Australian Navy in 1976 as a Seaman Officer and later specialised in aviation. He assumed command of the Royal Australian Navy on 1 July 2014.

A dual-qualified officer, Vice Admiral Barrett served in Her Majesty's Australian (HMA) Ships *Melbourne, Perth* and *Brisbane* and HMS *Orkney* as a Seaman Officer and then as Flight Commander in HMA Ships *Stalwart, Adelaide* and *Canberra*. His staff appointments include Deputy Director Air Warfare Development, Director Naval Officer's Postings and Director General of Defence Force Recruiting.

Vice Admiral Barrett has served as Commanding Officer 817 Squadron, Commanding Officer HMAS Albatross, Commander Australian Navy Aviation Group, Commander Border Protection Command and as Commander Australian Fleet.

Vice Admiral Barrett was awarded a Conspicuous Service Cross in 2006 for outstanding performance as Commanding Officer HMAS *Albatross* and as Chief of Staff Navy Aviation Force Element Group Headquarters. Vice Admiral Barrett was appointed as a Member of the Order of Australia in 2009 and subsequently promoted to Officer of the Order of Australia in 2014 for his leadership of Border Protection Command and the Australian Fleet.

Vice Admiral Barrett holds a Bachelor of Arts in Politics and History and a Masters of Defence Studies, both from the University of New South Wales, and has completed the Advanced Management Program at Harvard Business School. He recently published *'The Navy and the Nation: Australia's Maritime Power in the 21st Century'* in which he outlines the extensive opportunities for Navy and Australia as steps are taken to implement the planned investment in naval capability outlined in the Defence White Paper 2016 and the National Shipbuilding Plan over the coming decades.

Vice Admiral Barrett and his wife, Jenny, have two daughters.

Vice Admiral David Johnston, AM, RAN

Vice Admiral David Johnston, AM graduated from the Royal Australian Naval College in 1982 as a seaman officer, later specialising as a Principal Warfare Officer. His operational tours include serving as Commanding Officer of HMAS *Adelaide* (FFG 01) and HMAS *Newcastle* (FFG 06). The latter command included deployment on Operation *Quickstep* to Fiji in 2006.

His staff appointments include Command and Control specialist staff positions in Australian Defence Headquarters, Operations Manager at Sailors' Career Management and later as Director Joint Plans in Strategic Operations Division, where he developed the military response options for consideration by Government.

Vice Admiral Johnston was appointed Commander Border Protection Command in December 2011. As commander of the whole of government multi-agency organisation he was responsible for the security of Australia's maritime domain utilising resources from both the Australian Defence Force and the Australian Customs and Border Protection Service.

Vice Admiral Johnston assumed the appointment of Chief of Joint Operations in May 2014. His current role is to plan, control and conduct military campaigns, operations, joint exercises and other activities in order to meet Australia's national objectives.

Vice Admiral Johnston is married and has two children. He holds a Master of Science in Operations Research from the USN Postgraduate School in Monterey, California and a Master of Arts in Strategic Studies from the Australian Defence College, Weston Creek. He participated in the inaugural Australian Security Executive Development Program in 2009.

Air Vice-Marshal Warren McDonald, AM, CSC

Air Vice-Marshal Warren McDonald was born in Hay, NSW and joined the Royal Australian Air Force at the age of 15 as an apprentice motor transport fitter. In 1989, he was commissioned and underwent pilot training, flying his first operational tour on the P-3C Orion at No 11 Squadron. In 1993, he was posted to Canada to fly the CP-140 Aurora at 415 Squadron.

In 1996, he returned to fly the P-3C Orion with No 10 Squadron and was then posted to No 92 Wing's Maritime Test and Evaluation Unit to introduce the AP-3C Orion. In 2002, he was posted to Butterworth Malaysia, as the commander of 92WG's Detachment Alpha. This was followed by promotion to Wing Commander and a posting as Deputy Director of Project Air 7000 Phase 1.

In 2007, Air Vice-Marshal McDonald was appointed Commanding Officer of No 11 Squadron, for which he was awarded the Conspicuous Service Cross. He commanded No 92 Wing until October 2011, when he deployed to the Middle East as the Australian Air Component Commander for Joint Task Force 633 in support of Operation *Slipper*. With over 5000 hours on the P-3, he has served four operational tours in the Middle East, each one in a different command position.

Upon his return from the Middle East in May 2012, Air Vice-Marshal McDonald was promoted to Air Commodore and appointed Director General Capability Planning - Air Force, before appointment as Commander Air Mobility Group. In June 2015, he was appointed a Member of

the Order of Australia (AM) for exceptional performance as Officer Commanding No 92 Wing, Director General Capability Planning - Air Force and Commander Air Mobility Group.

On promotion to Air Vice-Marshal in July 2015, he commenced as Deputy Chief of Air Force. Air Vice-Marshal McDonald is currently serving as the Chief of Joint Capabilities within the Australian Defence Force Headquarters.

He is married to his very understanding wife, Sarah.

Mr Peter Jennings

Peter Jennings is the executive director of the Australian Strategic Policy Institute (ASPI). He led the 'External Expert Panel' appointed by Government in early 2014 to advise Ministers and the Defence Department on the Defence White Paper, released in February 2016. Peter was awarded the Public Service Medal in the Australia Day 2013 Honours list for outstanding public service through the development of Australia's strategic and defence policy, particularly in the areas of Australian Defence Force operations in East Timor, Iraq and Afghanistan. In February 2016 Peter was awarded the French decoration of Knight in the National Order of Legion d'Honneur.

Professor Genevieve Bell

Professor Bell is the Director of the 3A Institute, Florence Violet McKenzie Chair, and a Distinguished Professor at the Australian National University (ANU) as well as a Vice President and Senior Fellow at Intel Corporation. Prof Bell is a cultural anthropologist, technologist and futurist best known for her work at the intersection of cultural practice and technology development.

Professor Bell joined the ANU's College of Engineering and Computer Science in February 2017, after having spent the past 18 years in Silicon Valley helping guide Intel's product development by developing the company's social science and design research capabilities.

Professor Bell now heads the newly established Autonomy, Agency and Assurance (3A) Institute, launched in September 2017 by the ANU in collaboration with CSIRO's Data61, tasked with building a new applied science around the management of artificial intelligence, data, technology and their impact on humanity.

Professor Bell is the inaugural appointee to the Florence Violet McKenzie Chair at the ANU, named in honour Australia's first female electrical engineer, which promotes the inclusive use of technology in society. Prof Bell also presented the highly acclaimed ABC Boyer Lectures for 2017, in which she interrogated what it means to be human, and Australian, in a digital world.

Professor Bell completed her PhD in cultural anthropology at Stanford University in 1998.

Mr Mike Manazir

Mike Manazir is Vice President, Navy Systems for Boeing's Defense, Space and Security organization headquartered in Arlington, Virginia.

Mike is responsible for all products and services within the Navy portfolio and is also responsible for bringing the Navy customer's perspective to each Boeing business division leadership team to assist with strategy, technology, investment and business decisions in the pursuit of new Navy business opportunities for The Boeing Company.

Manazir joined The Boeing Company after retiring as a Rear Admiral after 36 years of distinguished service in the United States Navy. He commanded VF-31, USS *Sacramento*, USS *Nimitz*, and Carrier Strike Group Eight in USS *DD Eisenhower*. That service included 15 overseas deployments from both coasts; 3750 fighter hours, qualified in the F-14A/D and the F-18E/F; 1240 arrested landings; five tours in the Pentagon, four of these in Navy requirements.

Mr Alastair MacGibbon

Alastair MacGibbon was appointed the Head of the Australian Cyber Security Centre in July 2017 and the first Special Adviser to the Prime Minister on Cyber Security in May 2016. In these roles, he provides national leadership and advocacy on cyber security policy and the implementation of the Government's Cyber Security Strategy. Alastair worked for 15 years as an Agent with the Australian Federal Police, including as the founding Director of the Australian High Tech Crime Centre. Along with private sector roles such as Senior Director of Trust, Safety and Customer Support at eBay, Mr MacGibbon was a Director of the Centre for Internet Safety at the University of Canberra.

Gregory Charles Allen

Greg Allen is an Adjunct Fellow at the Center for a New American Security, where he focuses on the intersection of Artificial Intelligence, cybersecurity, robotics, and national security. His writing and analysis has been published by the Council on Foreign Relations, CNN, Foreign Policy, WIRED, Vox, and The Hill. His report, 'Artificial Intelligence and National Security,' a study conducted on behalf of the US Intelligence Advanced Research Projects Activity (IARPA) was published through the Harvard Belfer Center for Science and International Affairs. Mr Allen holds a joint MPP/MBA degree from the Harvard Kennedy School of Government and the Harvard Business School.

Lieutenant General John Shanahan

Lieutenant General John N.T. 'Jack' Shanahan is the Director for Defense Intelligence (Warfighter Support) (DDI (WS)), Office of the Under Secretary of Defense for Intelligence, Pentagon, Washington, D.C. The DDI (WS) ensures combatant commands (CCMD) have the intelligence policy, processes and resources they need to plan and conduct successful operations and campaigns.

General Shanahan previously served as the Commander, 25th Air Force, Joint Base San Antonio-Lackland, Texas. In his position as 25th Air Force Commander, General Shanahan also served as the Commander of the Service Cryptologic Component. In this capacity he was responsible to the Director, National Security Agency, and Chief, Central Security Service, as the Air Force's sole authority for matters involving the conduct of cryptologic activities, including the spectrum of missions directly related to both tactical warfighting and national-level operations.

General Shanahan is a master navigator with more than 2,800 flying hours in the F-4D/E/G, F-15E and RC-135. He is authorized to wear the master intelligence occupational badge.

Jennifer McArdle

Jennifer McArdle is an Assistant Professor of Cyber Defense at Salve Regina University and a Fellow in Defense Studies at the American Foreign Policy Council. Jennifer currently leads a research project that explores computer network operations and the military's synthetic training environment. She currently serves on Congressman James Langevin's Cyber Rhode Island Advisory Committee.

Jennifer was previously at the Potomac Institute for Policy Studies, where she served as a contractor for the Department of Defense, Defense Microelectronics Activity on cyber hardware and supply chain security. She has formerly held positions at the American Association for the Advancement of Science and the US National Defense University, in addition to working in New Delhi, India at two defense research institutions. She is currently a PhD candidate in War Studies at King's College London and was a recipient of the RADM Fred Lewis doctoral scholarship in modeling and simulation from I/ITSEC. She holds a M.Phil in Politics from the University of Cambridge and a BA in Political Science and Justice Studies, summa cum laude, phi beta kappa, from the University of New Hampshire.

JD McCreary

A native of Coronado, California, JD McCreary was commissioned in 1991 from the United States Naval Academy and received a degree in Physics. In 1993, he was winged as a Naval Flight Officer in Pensacola, receiving orders to NAS Whidbey Island, WA and the EA-6B Prowler community.

JD McCreary has served in operational tours including Operations *Southern Watch*, *Deny Flight*, *Deliberate Force*, *Enduring Freedom*, and *Iraqi Freedom*. He has planned and executed tactical, operational and strategic Electronic Warfare in support of both conventional and special operations.

He currently serves as Chief, Disruptive Technology Programs for the Sensors and Intelligent Systems Directorate at Georgia Tech Research Institute. Key initiatives include advising DOD leadership on future Force Design and the role of artificial intelligence in warfighter Decision Superiority.

Mark Laity

Mark Laity has been involved with the media, information and latterly Strategic Communication for four decades, both as a journalist, mostly with the BBC, and then in a variety of posts as a spokesman and senior manager for NATO. His experience covers all levels, from the political and strategic, to the frontlines of major operations.

He is now the Director of the new Communications Division at SHAPE. Previously he was the first Chief Strategic Communications (StratCom) at SHAPE, and the leading figure in first establishing and then developing StratCom within NATO, especially the military. His Chief StratCom role followed the first of three Afghan tours in senior communication posts. Previously he had been Chief of Public Information at SHAPE, the first civilian postholder.

From 2000, Mark Laity was for four years Special Adviser to the NATO Secretary General, Lord Robertson, and NATO's Deputy Spokesman. He had a wide variety of defence policy and information roles including a year as NATO spokesman. In 2001, with civil war threatening, he was sent to the Former Yugoslav Republic of Macedonia as personal adviser to the Macedonian President, and later he became Media Adviser to the NATO commander and civilian spokesman for Operation Essential Harvest.

Mark Laity joined NATO after 22 years in journalism, including, from 1989, 11 years as the BBC's Defence Correspondent, when he reported from the frontlines of most major conflicts of the nineties, but particularly the break-up of Yugoslavia, and the 1991 Gulf War.

Mr Bernard Salt

Bernard Salt is widely regarded as one of Australia's leading social commentators by business, the media and the broader community.

Bernard heads The Demographics Group which provides specialist advice on demographic, consumer and social trends for business. Prior to that Bernard founded KPMG Demographics.

He writes two weekly columns for *The Australian* newspaper and is an adjunct professor at Curtin University Business School. Bernard also holds a Master of Arts degree from Monash University.

Bernard Salt is one of the most in-demand speakers on the Australian corporate speaking circuit and has been so for more than a decade.

He is perhaps best known to the wider community for his penchant for identifying and tagging new tribes and social behaviours such as the 'Seachange Shift', the 'Man Drought', 'PUMCINS' (pronounced pumkins) and the 'Goats Cheese Curtain'. He was also responsible for popularising smashed avocados globally.

Bernard has popularised demographics through his books, columns and media appearances. His body of work is summarised in six popular best-selling books. Bernard appears regularly on radio and television programs and recently hosted a business television program 'The Next Five Years' on SkyNews Business Channel 602.

He was awarded the Member of the Order of Australia (AM) in the 2017 Australia Day honours.

Air Vice-Marshal Gavin Turnbull, AM

Air Vice-Marshal Turnbull is a pilot with more than 3600 flying hours on rotary wing and fast jet aircraft. He completed his basic training in 1984 and spent the next four years flying UH-1H helicopters as a member of No. 9 Squadron which was then based at Amberley. This period included a short tour with the ANZAC Contingent of the Multinational Force and Observers based in the Sinai Desert.

Air Vice-Marshal Turnbull deployed to the Middle East in March 2007 as Chief of Staff in the Australian National Headquarters, Baghdad serving a six-month tour; followed by appointment as Officer Commanding No. 81 Wing from 01 November 2007. Following his command tour, Air Vice-Marshal Turnbull was appointed Director, Military Strategic Commitments from January 2011. He deployed to the Middle East in January 2012 completing a tour as Director, US Central Command 609th Combined Air Operations Centre where he was awarded the United States Bronze Star Medal. He returned to Australia in May 2012 to take up the dual appointments as Director General Air Command Operations (Headquarters Air Command) and Director General Air (Headquarters Joint Operations Command). Air Vice-Marshal Turnbull was appointed as the Air Commander Australia on 12 September 2014, conducting duties as the senior operational commander in Air Force. On 1 May 2017, Air Vice-Marshal Turnbull was appointed as the Deputy Chief of Air Force.

Air Vice-Marshal Turnbull was appointed a Member of the Order of Australia (AM) for exceptional service to the ADF in air combat capability development and support to military operations in the Australia Day 2016 Honors and Awards.

Air Vice-Marshal Turnbull is married to Jackie, has four sons and one daughter.

Opening Address

Air Marshal Leo Davies, AO, CSC

Good morning, Minister Payne, ladies and gentlemen; to Auntie Tina and Uncle Harry - a fantastic welcome to the country. Thank you! I'd like to say thank you to all those folks who are here with us at the 2018 Air Power Conference, and for the grand start yesterday at the Last Post ceremony and the reception at the arboretum. I thank you also for the opportunity this morning to set the scene.

It is absolutely my view that we live in an age of disruption. The information and communications revolution, the global increase in economic development, economic linkages and independences, and the competing forms of political and ideological movements have together made the 21st century a more dynamic strategic environment. Nowhere is this more evident than right here in our region of the Indo-Pacific. With this unprecedented sharing of economic wealth and technical development, it gives the wherewithal for more players, states, actors, businesses, and communities to exert some influence.

This means that sometimes, these disruptors cause friction and this friction requires management; shaping when necessary, but certainly influencing and, at times, real action. The air power characteristics of reach, speed, and precision effects remain important elements of a nation's defence strategy. The question for us to ponder at this 2018 Air Power Conference is whether we are postured to apply this significant capability in a way that counters these disruptors. So, as we open up Pandora's Box, we'll be asking also whether there are any possibilities and solutions for us to explore.

Let us begin with the strategic environment. In one of the most significant developments in the modern era, we are experiencing a shift of the geostrategic centre from the North Atlantic and Europe into the Indo-Pacific. This is the biggest shift in the global balance of power since the end of World War II. There is a myriad of factors driving this change. I'd like to focus on two. These key factors are altering the security landscape and creating a disruptive world.

The first of these factors is the relative rise of the economic military and political power of the Indo-Pacific. The growth of the Asian economy, led initially by Japan and more recently by China and Korea, has significantly elevated the strategic influence of nations in our region. In the past 20 years, Asia's share of global manufacturing has increased from around 30% to just over 50%, and rising economic powers will continue this transformation.

We must be mindful, however, that economic prosperity has typically been associated with increased military capability and, at times, international competition. The United States of America, a prevailing underwriter of global security, is refocusing its foreign policy. The US national defence strategy identifies the re-emergence of long term strategic competition with revisionist powers as its principle priority. This is a shift away from its more recent focus on asymmetric warfare, including counterterrorism operations and the makings of peace and order in an otherwise relatively stable global environment.

Dealing with the very real threat of major powers, as well as many ongoing security issues, requires support to the US global network of alliances and partnerships. This is the backbone of global security. Alliances and partnerships are of particular importance in our region, which is home

to five of the US's seven bilateral defence arrangements. Excluding the particular arrangements of NATO, our region is home to more and more varied formal defence relationships with the US than any other region in the world.

The impact of economic power will become even more pronounced as military power grows to match. Prosperity has enabled nations throughout the region to invest significantly in militaries, a legitimate response aimed at protecting their national interests. They also have easy and affordable access to sophisticated technologies, enabling pre-industrial societies to leap straight to the digital age, and bypass industrial development. More nations are investing in high-end war fighting capabilities and challenging what has historically been a Western advantage.

Investments in stealth, networks, ISR, and precision weapons are no longer a guarantee of capability overmatch. We now need to seek alternative solutions to reinstate military superiority. Indo-Pacific nations now have greater means by which to pursue their national agendas. This new power balance is emboldening some states to challenge the post-World War II international rules-based order. The legitimacy of multinational security organisations and global arbitration systems is being questioned, thus challenging the future of the international liberal and rules-based order that has been the basis of stability for the best of the last century.

The second trend is the growth in depth and breadth of security issues. Today, would-be aggressors are seeking means to threaten all aspects of national power. Terrorists and organised crime have always looked for ways to get around the system. We are used to them not playing by the rules. But now, some actors are also looking to operate in the grey zone, exploiting the vulnerabilities of free societies, markets, and global communications. Historical Indo-Pacific security frameworks are coming under increasing pressure, in many instances from frontiers beyond the comprehension of those who designed them.

The ubiquitous nature of contemporary communications is seeing propaganda as an effective element of information warfare, giving rise to the exploitation of fake news as a means to incite a response; everything from the use of chemical weapons to civilian working strikes and even the presence of mass conventional troops in other countries. Technology is providing the means to contest every domain by integrated kinetic and non-kinetic effects, often originating from an asymmetric platform.

Social networks now provide the means for ideologies to unite globally, challenging state boundaries and the basis of the Westphalian system. The Indo-Pacific region has never been more complex or challenging and the rate of change is faster than in any other time in our history. The convergence of these trends is creating a new set of national security challenges. We have new and historical strategic actors who continue to abide by the international rule of law. It is, however, the emergence of new strategic actors, perhaps like ISIS, who don't abide by the international rule of law, who are the catalyst to this disruptive world that confronts us. Our challenge is to adapt and respond to this new order.

The role of the Australian Defence Force to protect Australia and its national interests remains as relevant as ever in this dynamic world. For Air Force, this equates to the delivery of the seven air power roles: control of the air, strike, air mobility, ISR, command and control, force protection, force generation, and sustainment. We have seen that air power can strike deep and, integrated with the joint force, generate decisive effect. Today, we provide support to troops on the ground and critical visibility for commanders. It is the analytical situational awareness and

communications capabilities that increasingly provide the full range of air power support to our joint and coalition engagement.

However, we needed to do more. Our air force is already capable, but is now facing the greatest evolution of air power in its history. The 2016 Defence White Paper has committed around $195B to new defence investments, of which almost $100B will directly support air power systems employed across the ADF. This will not just bring into service new platforms, but also a transition to information warfare with unprecedented demands on data collection, processing, and exploitation.

We now must be able to integrate and C2 a networked force, not just a physical one. Effective employment of an integrated and networked force to gain decision superiority and enable manoeuvre, despite any intent to deny the same, is the hallmark of a fifth generation force. Such a change demands ingenuity, requiring a workforce that is empowered to think and act outside of the traditional norm. Innovation is essential to the realisation of the full potential of this investment. Our next generation of airmen and airwomen must develop professional mastery that extends beyond mission specialisations. It must promote critical thinking, strategic understanding, innovative problem solving, collaboration, and leadership. This is not business as usual.

Air power begins and ends with people and teams. A technical network alone is nothing. This 2018 conference is both a strategy and an air power conference. It is structured to aid our collective understanding of emerging challenges—many of which I've already discussed—and, perhaps, our possible solutions. This conference is deliberately designed to take a measured approach to the problems that we are presented with. But this is no closed loop. Despite the challenges, we are not destined for war. But the complexity of the environment and the severity of the possible consequences means we cannot be complacent.

In the Royal Australian Air Force, we are tackling this through our own dynamic strategy. We need a broad community to help us shape this strategy. We need your help. This is my call to like-minded chiefs. Those of us who share these challenges and common values, I ask to engage collaboratively to better understand and shape the role of air power as an instrument of national security. This disruptive world is presenting new challenges to the role of air power.

I don't know what the next conflict will be. But I do know many of the tools of trade are now more freely available to potential adversaries than ever before. In future conflicts, we can expect bases, support infrastructures, including civilian infrastructure, to be targeted through the use of physical and nonphysical effects. These resources are no longer sanctuaries immune from attack. Emerging technologies will revolutionise the application of air power, but also give rise to new challenges. Success in the future battle space requires the coordination of joint effects across all domains—a system of systems.

Air power must be comprehensively integrated across the joint force to contribute meaningfully to the future fight. These obstacles and challenges are real, but so are the visions and the ideas we will bring to meet them. I have confidence in our airmen and airwomen to realise our vision. I'm reminded of the words of Henry Parks, our Father of Federation, as he looked to the challenges at the creation of our nation: "In the one hand, I have a dream. In the other, I have an obstacle. Tell me which one grabs your attention." My proposition, ladies and gentlemen, is that we grab both and collectively chart a new path for air power in this disruptive world.

Thank you, ladies and gentlemen, for allowing me the presentation and also now to begin our program, by introducing our first speaker. Ladies and gentlemen, it's my pleasure to introduce Senator, the Honourable Marise Payne. She is our Minister for Defence. She has guarded not just our hardware development since taking office in September of 2015 but, more importantly, and in the context of this conference, the education, the technology, the SNT development that has been able to support a contemporary air force, a contemporary Australian Defence Force, and, indeed, a future force.

Ladies and gentlemen, that commitment has been quite substantial. Minister Payne, could I invite you to address this conference?

Minister's Address

Senator, The Hon Marise Payne

Good morning ladies and gentlemen. Let me begin this morning by acknowledging the traditional owners of the land on which we meet and pay my respects to their elders past, present and future. Let me also thank Auntie Tina for her very informative welcome; for those of you who are visitors to Australia, I think that was one of the most educational welcomes to a country I have ever enjoyed. Let me also thank Uncle Harry very much this morning as well. It is always a pleasure to see you. Thank you for your recruiting efforts and please keep it up.

To the members of the International Military Leadership who are here today, to senior members of industry, to current and former members of the Australian Defence Force, particularly the leadership of the Royal Australian Air Force; the chief of Air Force, Air Marshal Leo Davies; the deputy chief of Air Force, Air Vice-Marshal Gavin Turnbull; the Air Commander of Australia, Air Vice-Marshal Zed Roberton; and Air Vice-Marshal Tracy Smart right in front of me as well. Welcome to you all. Chief of Air Force, Leo Davies, thank you very much for the opportunity to address this very important conference today, the largest ever air power conference, I believe you indicated on my arrival this morning.

I want to acknowledge your leadership, and I want to acknowledge your very pertinent remarks this morning, in your opening speech. Thank you very much for setting the scene for the discussion, the conversation about air power in a disruptive world. I want to echo the Chief's welcome to the delegates who are going to be participating in this conference over the next two days, and, as I said, particularly welcome our international delegates, and specifically, the 11 visiting Chiefs of Air Force. The Royal Australian Air Force has developed a valuable network of relationships throughout the region reflected by your presence here today, and the Government of Australia is absolutely committed to strengthening these links.

So, it is excellent to see so many international delegates. Your presence here over the next two days is an important opportunity and also a reflection of the need to work together to address the challenges that we are facing in a disruptive world. This year's conference will, as the chief of Air Force has said, address some of the most significant challenges that we face today, some of which have the possibility to change quite fundamentally our approaches to and understanding of security on a national and global scale. That you have been able to assemble a programme of speakers with such diversity and depth of expertise, speaks volumes about the degree of integration we can achieve to make best use of a fifth-generation force.

I spoke at the 2016 Air Power Conference just a few days after the prime minister and I launched the 2016 Defence White Paper, which set out our plans to modernise the Australian Defence Force, including the RAAF, so that we are best able to respond to the increasingly complex strategic environment. It's fair to say that only two years since that speech feels like an aeon in strategic terms. The Defence White Paper at the time identified six key drivers shaping the future security environment for Australia and having the greatest impact on Australia's strategic interests.

First, the roles of the United States and China and the relationship between them. Second, challenges to the stability of the rules-based global order.

Third, the enduring threat of terrorism. Next, state fragility including within our immediate neighbourhood. Then, the pace of military modernisation and the development of more capable, regional military forces. And finally, the emergence of new complex non-geographic threats, such as in the cyber and space domains. So, since I last addressed the Air Power Conference, all of these drivers have continued to affect the security of the region, if not the world.

For instance, we know that North Korea has made significant progress towards an intercontinental ballistic missile capability. We have seen Daesh itself try to get a foothold in our region, as demonstrated by the siege of Marawi in the Southern Philippines. We also continue to see unprecedented technological disruption, which is affecting all parts of society, including the military and the Air Force. But whether you're in any service industry, in the accommodation sector, in transporting communications, or the military, technological disruption is having a profound effect on the way that business is done.

For defence, unmanned systems, hypersonics, and laser technology are some of the areas presenting new challenges and opportunities. While some of the technologies to be discussed over the next two days remain somewhat futuristic, requiring significant development before they would be considered viable, let alone mature, history shows that science fiction can become science fact very quickly. We are, without doubt, living in a period when the rapid advance of technology is fundamentally reshaping the way air forces receive and process information, the way we communicate with each other, and the way we protect and promote our national and regional interests.

Technology has always played a major role in Australia's approach to national security. We're a large country, with a small population that takes an active role in our region, and globally. This presents us with unique demographic and geographic challenges. We rely on technology to enable us to defend Australia and contribute to regional security. In what is a period of rapid change, we must continue to embrace the benefits of innovation, and this has a number of implications for Air Force. First, air power can no longer be viewed in isolation; it must be integrated.

We are in the process of completely modernising almost all of Air Force's fleet. We have the new Spartan battlefield airlifter aircraft in service and the EA-18G Growler electronic attack platform. I'm pleased to announce that our P8-A Poseidon maritime surveillance aircraft has reached initial operating capability five months ahead of schedule. It's already on operations. And, of course, from December this year, the first two Australian F-35A Lightning Joint Strike Fighters will be permanently based in Australia. These platforms will underpin the creation of a fifth-generation Air Force that will enable these platforms: the Wedgetail, the Poseidon, the JSF and the Growler, to integrate their picture of the battle space.

But it isn't just, as you well know, about Air Force. These new platforms are giving us the ability to work with commanders on the ground and at sea to deliver combined strikes and disrupt the enemy in ways that have not been possible before. Here, we will soon have a glimpse of the power of this integration, with the delivery of the second air warfare destroyer, HMAS Brisbane, and with the introduction of the cooperative engagement capability or CEC. In very simple terms, this brings together, as a new capability, radar data from ships, from aircraft and ground-based units and combines this information into one integrated picture.

This single picture then provides all units with CEC in the taskforce, with complete visibility of the total battle space. This significantly improves air defence capabilities, not by adding new radars or weapon systems, but by distributing existing sensors in a significantly more effective

manner. Currently, our new P8-A Poseidon and Growler aircraft are equipped to integrate into this system. As part of our whitepaper plans, we'll look to upgrade other Air Force platforms such as the Wedgetail. We're also investing in a number of complementary technologies for Air Force, including the recently announced investment in the world-leading Jindalee Operational Radar Network (JORN).

This investment will extend its life and provide better situational awareness. While JORN is run by Air Force, its surveillance of Australia's northern approaches benefits all three services and contributes to our ability to work as an integrated and joint force. JORN is also benefiting from our recent government investment in the development of Australia's space capability. In September last year, Defence invested over $10 million for Air Force in the University of New South Wales (UNSW) to develop new ways to enhance Australia's future defence space capability. In November last year, I announced the successful launch of Buccaneer Cubesat by US Delta II rocket in a collaborative effort between Defence and UNSW.

This low-cost miniature satellite will perform calibration activities for JORN. The investment in JORN and space-based technologies will benefit all three services, with improved situational awareness. Longer term, our additional investment is planned in space-related capability, including new radars and sensors to enhance our space situational awareness. This will give us a better ability to protect our space-based assets, which underpin the vital communication links for our military in the field. But there are, of course, risks to our comprehensive embrace of technology.

Twenty years ago, our thoughts would not necessarily have gone to the need to protect our aircraft from cyber security threats, but that is exactly what we are now doing for our F-35s and other aircraft. Thirty-five years ago, when the secret US military space-based navigation system called GPS was first opened to civilian use, we didn't really contemplate that one day all emergency services, vehicles and virtually every new car, every new smartphone, even smart watches would have satellite navigation built into them. So much so, our economy now depends on GPS satellite navigation for safety and productivity growth. And in saying that, it's worth noting that smartphones, as we know them today, only arrived on the market in 2007.

This exemplifies the challenge of technology. As we increase our reliability on it, we also become vulnerable to attacks on it, and then we have to defend it. The second challenge, I think, is information overload. How do we process, prioritise and share the information we collect? How do we ensure the relevant critical information is not buried in a sea of noise? So, solving these complex problems is going to require us to repurpose, to grow and to train cohorts of the defence workforce. As we also announced in the 2016 Defence White Paper, enhancements and intelligence in cyber and space will require around 900 ADF positions, including in intelligence collection and analysis, in communications, in supporting the information requirements of new platforms like the JSF, in surveillance aircraft and Navy ships, and to better support Special Forces and cyber security.

All of these areas will require a workforce with skills in STEM: in science, in technology, in engineering and in mathematics. Developing the talent and skills of Australians in STEM areas is one of the key pillars supporting our national approach to innovation, to maximise the benefit of emerging technologies while minimising the threat they pose to national security. It is also a personal passion of mine. So Defence, in the development of the white paper and since, is placing a priority on STEM engagement and recruitment. We have one of the largest STEM programs in

Australia and we promote STEM-related roles to schoolchildren, and provide work experience, opportunities and scholarships, as well as maximising career learning and development for STEM occupations.

We have made progress, but there is absolutely more to do. This is the challenge not just for the ADF, not just for Air Force, but for all of you to ask for specific defence initiatives, and include partnering with the Australian Mathematical Sciences Institute to provide internships for up to 100 post-graduates over the next four years; to hold defence technical scholarship camps, with Year 11 and 12 students, their teaching staff and their parents to showcase Navy, Army and Air Force engineers and technicians at work; and to offer employment for early career postgraduate researchers in priority science and technology areas such as computer sciences, autonomous systems, electronic warfare and information systems.

For the Australian Defence Force Academy, students in non-STEM related degrees are required to undertake STEM subjects irrespective of their primary degree stream. This provides our future leaders with a foundation in scientific and technical knowledge upon which they are able to build throughout their career. Our educational institutions provide the building blocks, the intellectual building blocks, but it's up to the individuals and the organisations within which they work to build on these foundations and to support the drive for innovative thinking and creative problem-solving that will be the keys to success into the future.

They need to be given the opportunity to be innovative. On this, I note and I commend Air Force on Plan Jericho, which has succeeded in a few short years in energising the innovation spirit within Air Force, as well as across the joint force and defence industry. By encouraging bottom-up innovation, Air Force is creating an organisational culture that supports divergent and disruptive thinking, and aligns technological and engineering solutions with an understanding of the operational and organisational challenges that Australian air power is facing. What this highlights is that, if we provide the opportunity for Australian creativity, an innovative spirit, the sky is no longer the limit.

Our relationships and our ability to integrate and work with our international friends and allies is critical to addressing the challenges that will emerge over the years and decades to come, some of which we will be able to anticipate, others that we will not. Our international defence relationships and arrangements are vital to reducing the risk of military conflict and in developing interoperability with our partner forces to respond to shared challenges of maintaining the international rules-based order, combating terrorism, and providing humanitarian assistance and disaster relief.

Indeed, in our own region, in recent weeks, in fact, in the last fortnight, in this example, Royal Australian Air Force C-17 delivered aid to Papua New Guinea in the wake of their tragic earthquake. An Army CH-47 Chinook, a C-130, and B300 King Airs continue to transport supplies and personnel between Port Moresby and the Southern Highlands of Papua New Guinea. In February, RAAF C-17s delivered approximately 140 000 kilograms of aid to Tonga in the wake of Cyclone Gita, while an AP-3C Orion conducted damage assessment flights from the same cyclone over the outlying Fijian Islands, at the request of the Fiji Government.

Australia was also able to provide AP-3C Orion surveillance support to the Philippines during the crisis and siege of Marawi last year. The commanding general of the Philippines Army, General Batista, made clear to me just a week or so ago, when I met him in Brisbane, that, when his ground troops fighting in Marawi knew the AP-3C was overhead, their morale lifted, their confidence

and incumbent actions improved, because they instinctively knew that timely intelligence, surveillance and reconnaissance information would soon be available to their ground-battle planners.

There is, though, room for improvement. We want to move from "soon be available" to "sharing data in real-time." With new platforms and integrated capabilities, this sort of data will be part of in-flight, air-to-surface downlinks and near real-time uplinks of updated surface sensor and data feeds. This new technology is a genuine, combat-force multiplier on land and at sea. Beyond technology, our rapid assistance to friends and Pacific neighbours was made possible due to the mutual trust between our nations, through our continued bilateral engagements and participation in institutions that are part of the regional architecture, such as the Pacific Islands Forum and ASEAN.

It is a reminder that, against modern national security threats, no single nation can standalone and hope to defend itself completely. We are deepening our already strong relationships with our partners to develop our war-fighting capabilities to meet the demands of modern conventional conflict. Later this year, more than 2,500 personnel from more than 13 of Australia's partners and allies will take part in Exercise Pitch Black 2018 in the Northern Territory to build our understanding and our interoperability in high-end war fighting. The month-long exercise enables us to test and improve our ability to integrate with partner nations in a range of offensive and of defensive scenarios.

These exercises reflect the strong relationships that Australia has with partner air forces that the Royal Australian Air Force, the ADF and that the government has built– as well as the high value we place on regional security, and fostering closer ties throughout the region. I want to end briefly with one final thought. Some of the concepts to be discussed at this conference and this weighty program, algorithmic warfare, digital natives and security would have seemed based in theory two decades ago. Twenty years ago, the idea of artificial intelligence, or AI, as a serious consideration for national security might have been regarded by some as something out of a Hollywood movie.

But today, in 2018, we find ourselves discussing these matters with the consideration and attention that they rightfully deserve. This year's air power programme is a graphic picture of the breadths and the challenges that face all of us in the decades ahead, from space to cyber, and from energy security to digital advancement. Through this period of intense disruption, the Australian Government is investing heavily in our defence force to ensure that it stays at the cutting edge, and we are building the work force that is able to exploit the full potential of this new technology. We can't master all the challenges alone, and we will need to leverage our international partnerships if we want to have the most effective Air Force possible.

So, over the next two days, I encourage everyone to embrace the spirit of innovation and collaboration that will be required to successfully navigate the challenges of technological disruption. You have a very impressive array of speakers ahead of you; I'm sure they will challenge and provoke. I certainly hope so. I wish, in fact I would much prefer, to be able to stay and enjoy some of those addresses, but the Senate is in session this week, and I must attend that.

Ladies and gentlemen thank you very much for the opportunity to speak this morning, and I wish you all the best for the Air Power Conference.

Keynote Address

Mr Bilahari Kausikan

Air Marshall Davies, ladies and gentlemen, Auntie Tina, Uncle Harry, I must begin by thanking the Royal Australian Air Force for inviting me to talk to you this morning. I only hope that, after you've heard me, you do not conclude that it was an act of reckless folly on their part. Some of you may think that the title of my talk, which I've modified slightly from what you saw on the screen; the title of my talk, *How to think about geopolitics in East Asia* is somewhat provocative, if not pretentious. Let me assure you that my intention is not to educate anyone's grandmother about eggs.

My intention is only to draw attention to something that I think has received insufficient emphasis. This is what could be called the binary fallacy. The binary fallacy is a mode of thought in which something must be one thing or another. If not A, then it is B. It's collateral is a certain mechanistic determinism. If not A, it must necessarily be B, and only B, and never C, D or Z. Now, the binary fallacy provides far too much analysis of geopolitical developments in East Asia, whether in the media, academia or by governments. In a sense, such a mode of thought is understandably prevalent because US-China relations are undoubtedly the main axis of the East Asian geopolitical equation.

The US and China are grouping towards a new *modus* vivendi; the adjustment's underway between these two major powers, and between them and other countries in East Asia will preoccupy our region for decades to come. This is precisely why we must think about US-China relations clearly and clinically.

Binary thinking is simplistic and ahistorical and hence inaccurate and inappropriate. Under some circumstances, it could be dangerously misleading. For a start, US-China relations defy facile characterisation. They are neither natural partners nor inevitable enemies. Their relationship is simultaneously profoundly interdependent and infused with strategic mistrust. Such ambivalence is in fact the most salient characteristic of most post-Cold War international relationships. To different degrees, ambivalence also characterises Sino-Japanese relations, Sino-Indian relations, Sino-South Korean relations, Sino-Australian relations, and the attitudes of smaller countries such as the members of ASEAN towards all the major powers.

Moreover, the US and China, while extremely important actors, are not the only actors. They operate in an increasingly complex global and regional environment which influences, and is influenced by, many other bilateral relationships in ever more complex dynamics. Free of Cold War imperatives, even the closest US ally does not now define its interest in exactly the same way as the United States. Even small countries, economically dependent on China are not without agency and given any opportunity, will exercise it. The binary mode of thought perhaps represents an unconscious hankering after the simplicities of Cold War international relations. It was a very dangerous period. Irrespective of which side of the ideological divide we stood, even if we pretended to be non-aligned, there was never much doubt of how we should position ourselves.

Well, that clarity is gone; it cannot be recreated by imposing simplistic patterns onto a complex reality. All this ought to be obvious; however, two developments in 2017, Mr Donald Trump's inauguration as the 45th president and Mr Xi Jinping's consolidation of power evident at the

Chinese Communist Party's 19th Party Congress and recently underscored at the National People's Congress, threatened to overwhelm the obvious and cloud our capacity for dispassionate analysis. These developments reinforce a tendency to think about US-China relations in binary deterministic terms, in which anything regarded as adversely affecting the United States must necessarily rebound to China's advantage. A particularly egregious example was a foreign policy article, published a day after the 2016 election under the ridiculous headline, "China just won the US elections".

More than a year later, too much of that attitude persists. The US and China are both changing and changing the world. A more symmetrical US-China relationship is certainly emerging in East Asia. But international relations are not sporting events in which a win for one side is necessarily a loss for the other. China's rise is not America's decline, except relatively. In absolute terms, both will remain substantial powers. Neither is without weakness. Neither future development is going to be described as a straight-line trajectory, either up or down. Simply put, the US under Mr Trump is not as bad as the American Media and large parts of the American establishment, still anguishing over his unexpected victory, portrays.

China under Mr Xi Jinping is not the juggernaut that the Communist Party's propaganda apparatus would have us believe. This again ought to be obvious, but the obvious is clouded by the emotional shock of Mr Trump's election and the confidence with which Mr Xi proclaimed China's ambition for a new era. There have certainly been serious disruptions to American policy, particularly in the area of trade. China's rise and ambition are real. The idea that China's rise is necessarily America's decline is advocacy, not balanced analysis. The American media and establishment or, at least, substantial parts of it, present almost everything Mr Trump does as wrong because they want him to fail, to vindicate themselves.

China presents ambition as an already existing reality because persuading others that it is so, goes some way towards making it so. There's a curious coincidence of agendas within China's Communist Party and at least some sections of the American media and establishment. Now, please don't misunderstand; I'm not suggesting conscious collaboration, but the arguments certainly reinforce each other. An example is trope, so pervasive in the Western media and academia as to be taken as almost axiomatice, almost self-evident, and this is that the Trump administration's retreat from leadership globally and in East Asia, has undermined the so-called Liberal international order and given China an advantage.

This supports the insistent Chinese line that America is an unreliable partner, which has become more unreliable under Mr Trump. These are superficially persuasive arguments but they don't stand up to close examination. It cannot be denied that the Chinese political system is better placed to consistently pursue long-term goals than the American political system that has always been subject to disruptions, some very major, every four years, even if the same President or party remains in office. It is not as if the Chinese system has not also been subject to major disruptions in the past, or is somehow now immune to future disruptions. Mr Xi Jinping's consolidation of power, the move away from the post Xiaoping principle of collective leadership, the greater emphasis on Party discipline, and the discarding of the two-term limit has been compared to Mao Zedong.

I think the comparison is false, but the potential for something akin to a newer Maoist single point of failure may now have been reintroduced into the Chinese system.

We should not let Mr Trump's outsized personality and his penchant for, how shall it put it politely, extravagant statements, exaggerate the extent of discontinuity that his administration represents. The Trump administration's national security strategy published in December last year, and the summary of the National Defence Strategy published in January this year are, to my mind, largely mainstream documents that make clear that the US has not eschewed American leadership or has entirely disavowed the current global order. However, it is clear that the Trump Administration has a different, a narrower and less generous, concept of leadership that puts America first and stresses a more robust approach to competitors and a return to an old strategy of peace through strength.

How and whether this strategy will work is, of course, yet to be determined and one may well have reservations about the concept of leadership that these documents embody. They cannot really be accurately described as a retreat from leadership. It would be a mistake to place too much responsibility on a single administration. It's not as if all was milk and honey in US policy before Mr Trump. There's nothing that has been as disruptive of international order as President George W. Bush's invasion of Iraq in 2003. This was the denouement of the hubris that began to infect American foreign policy in the immediate post–Cold War era under the Clinton Administration.

The ensuing wars in the Middle East exhausted Americans, discredited the American political establishment and set the stage for Donald Trump's election and that of Mr Obama before him. A similar trajectory from hubris to dysfunctionality can be traced in Europe. My conclusion is that, if the liberal international order is under stress—and I think it is—President Trump is a symptom, not a cause. The pressures on the liberal international order have deeper roots than Mr Trump's administration.

Setting aside trade policy for the moment—and I will return to it; I don't mean to underplay the significance of trade policy, but setting aside trade policy for the moment—to my mind, continuity has been as evident as disruption in some essential aspects of foreign and security policies. In some respect, there have been improvements over his predecessors' policies. The Trump Administration has reaffirmed its alliances with Japan, South Korea and Australia. It has given the Seventh Fleet greater latitude to conduct FONOPs, ie Freedom of Navigation Operations, in the South China Sea to challenge China's claims and has done so without quasi–metaphysical public debates about whether a particular action was really a FONOP or not. They undermined their effect and highlighted divisions between the White house and the Pentagon during the Obama administration, the second Obama administration.

I do not see any sign that the US is preparing to withdraw or retreat from East Asia. The Guam doctrine of 1969 was a far more serious re-orientation of US security policy in East Asia than anything Mr Donald Trump has said during the campaign or since done. Well, the cancellation of the TPP, ie the Trans Pacific Partnership, was undoubtedly a grievous blow to American credibility, but no less serious than Mr Obama's failure to enforce the red line he drew in Syria. President Trump's decision to bomb Syria while at dinner with President Xi Jinping, did much to restore the credibility of American power. Without credible power, there can be no leadership.

On North Korea, the Trump Administration, it seems to me, is shifting away from a quarter century of failed policy of denuclearization, and preparing to deal with a nuclear-armed North Korea by deterrence. Mr Trump uses extreme language, "fire and fury", "annihilation", but it nevertheless expresses the essential logic of deterrence. And his willingness to meet Mr Kim Jong Un is a risk, of course it's a risk, but I think it's a risk worth taking. I do not think North Korea

can be dissuaded from acquiring the capability it believes it needs for regime survival. Nuclear armed, ICBMs are able to reach the continent of the United States. It's impossible to dissuade a country from a course of action it believes to be existential, since any cost that can be imposed is necessarily less than the cost of proceeding, if you think the course of action is existential.

So, the alternatives are therefore pre-emption, in which the horrendous price of American security will be paid by America's closest East Asian allies, which would irrevocably destroy American credibility in East Asia and perhaps globally, or the means by which all relationships between nuclear weapons states have been managed, which is deterrence. And to be stable, deterrence must be coupled with diplomacy. I think that, while it is a risk to be willing to meet Mr Kim, it is a risk worth taking.

Now, competition and cooperation have always co-existed. The Trump Administration's national security strategy and national defence strategy can perhaps be criticised for over-emphasising competition. This is perhaps an over-correction to the second Obama administration's somewhat naïve belief that to secure China's cooperation on issues such as climate change, it was necessary to de-emphasize competition. Well, democracies always over-correct. The end of the Cold War and the collapse of the Soviet Union freed China from the constraints of its ***de facto*** membership of the US-led anti-Soviet alliance or coalition to relentlessly pursue its own interests.

There are now three competing visions of East-Asian order. Faced with a rising China—actually, I prefer the term, re-emerging China—the US has sought to preserve as much as possible of the East-Asian ***status quo*** built around its hub-and-spoke system of allies and friends in which America is clearly dominant, but dominant within the Westphalian norm of formal sovereign equality. This is a norm always more honoured in the breach than in its observance, but the norm of sovereign equality nevertheless maximises the scope for smaller states to exercise agency provided no vital American interest is at stake. The term rules-based-order or, more recently the broader concept of a free-and-open-Indo-Pacific describes this American goal.

Now China wants its new status acknowledged and this is a reasonable and legitimate aspiration. But China holds the concept of sovereign equality only lightly if at all, and seems to want its status acknowledged not merely as a geopolitical fact But as a new Sino-centric or hierarchical norm of East-Asian international relations with China at the apex, and this is an entirely different matter from recognising a geopolitical fact. China now insistently promotes the Belt and Road Initiative (BRI) as an overarching vision or an overarching strategy in which all roads lead to Beijing.

A third idea of regional order representing the aspirations of the smaller countries of South East Asia is encapsulated in the concept of ASEAN centrality. This is a term more often used than understood, so let me explain in a little more detail. ASEAN centrality is not, it is not, a reflection of ASEAN strategic weight in the East-Asian geopolitical equation. South East Asia lies at the intersection or major power interests and, hence, of major power competition. ASEAN centrality is best understood as a means of coping with this uncomfortable reality.

Unlike ASEAN's earlier aspiration, the unkind would say delusion, to make South East Asia a zone of peace, freedom and neutrality, ASEAN centrality does not futilely seek to exclude or limit the major powers. Instead, it tries to leverage on the unavoidable. By inviting all the major powers to participate in ASEAN–created forums, such as the ASEAN Original Forum, the East-Asia summit and ASEAN Defence Ministers' meeting and making all the major powers its dialogue partners, ASEAN can be useful. That is to say, central, because these forums and ASEAN itself

are coherent enough for the major powers to regard them as occasionally useful, while not so strong as to be able to stymie their most important interests.

All the major powers have professed support for ASEAN centrality but, in 2016, a Chinese Vice–Minister blandly told the ASEAN foreign ministers that, as far as the South China seas was concerned, ASEAN was not central. The Vice–Minister was perhaps rude but he was not wrong nor was he expressing a position unique to China. For more than two decades, ASEAN was certainly not central to the American approach towards military-ruled Myanmar, although the US was usually a bit more polite about it. The concept of ASEAN Centrality, as I have explained it, nevertheless preserves some autonomy in the midst of great power competition by promoting an omni-directional balance of major powers in South East Asia. It gives ASEAN some degree of voice and agency. The degree of centrality varies from issue to issue and ebbs and flows over time and this not ideal, but the ideal is only to be found in heaven, if there is a heaven.

Any effort to perpetuate any *status quo* indefinitely is futile. China's rise cannot be denied. The East-Asian *status quo* has already changed. But I do not think that any of these three ideas of regional order will prevail in their entirety. America's friends and allies do not have exactly the same conception of what should constitute a free and open Indo-Pacific. The US, Japan, India and Australia may all harbour concerns about rising China, but I do not think they are exactly the same concerns or held with the same intensity. Anxiety about China is, in any case, too narrow a basis for the concept to attract wide support. In all countries in East Asia, concern is coupled with recognition of the need for a close, or at least stable, relationship with China. In any case, the concept awaits clearer definition, and has so far generally been regarded with a certain degree of agnosticism by other countries. However, it is also improbable that China will be able to impose its preferences on East Asia either.

The South China Sea has become something of a proxy for the contest between American and Chinese ideas for regional order. It must be admitted, that ASEAN has not covered itself with glory on this issue. It is beyond ASEAN's capability to resolve the disputes in the South China Sea. This is a big-boy's game. At the strategic level, the South China Sea is, in my view, a stalemate. Nobody can make the Chinese drop their claims to almost the entire South China Sea or make them dig up the artificial islands it has constructed and draw the sand back into the sea. Beijing will certainly deploy military assets on those islands, perhaps only periodically, perhaps permanently.

Crucially, China cannot stop the US and its allies from operating in, through and over the South China Sea without risking war. If war breaks out, those islands and the military assets on them are only targets. Overall, the US is still militarily dominant and will remain so for the foreseeable future. China cannot prevail in a war and a loss or even a draw will put the rule of the Chinese Communist Party at some risk. The preservation of Party rule is the core of all China's interests. I doubt Beijing will gamble. The stakes are simply too high. Stalemate in the South China Sea is not ideal and militaries must plan for worst-case scenarios. But for most situations short of war, that is to say for day–to–day diplomacy, a stalemate, while not ideal, preserves manoeuvre space for smaller countries. As long as the US is present, no ASEAN claimant can be forced to give up its claims or accept subordination. Much of the commentary on President Xi's China, and in particular, his 19th Party Congress speech, focuses on China's global ambition and the abandonment of Deng Xiaoping's policy of biding time. There is nothing unusual to my mind

about a big country having big ambitions. It would only be unusual if a big country did not have big ambitions.

The overwhelming focus of the 19th Party Congress speech was, in fact, domestic. Insufficient emphasis has been given to the Presidency's definition of the new principal contradiction facing China. To quote his speech: "The contradiction between China's unbalanced and inadequate development and the people's ever growing needs for a better life and consequently on the urgent imperative of revitalising the Chinese Communist party to meet those needs." The new principle contradiction prescribes an extremely complicated domestic, economic, social and political agenda, which, as the speech made clear, is connected to the continuation of Party rule. The agenda includes moving industry up the value chain, cutting over–capacity, promoting innovation, improving the environment, revitalising the rural sector, promoting balanced regional growth, and dealing with an ageing population, healthcare and social security, promoting social stability, improving education, housing and food safety, dealing with corruption, diffusing social tensions and expanding orderly political participation. Each of these issues is itself a major challenge and this list which I've just read to you is just partial. I took the list from the party speech.

Moreover, the 19th Party Congress speech referred only obliquely to a key question left over from the 18th Party Congress in 2012. This is, what is the appropriate balance between market efficiency and Communist Party control? The 19th Party Congress offered no clarity and indeed, there are no clear answers, because nobody has had to face this question before. President Xi affirmed his commitment to economic efficiency but his stronger insistence on Party discipline and the Party's leading role may have sharpened the challenge. The challenge is fundamental, perhaps even existential, because there's no practical alternative to Communist Party rule for China.

The Brick and Road Initiative (BRI) is as much about dealing with this central challenge as it is a new global strategy or manifestation of ambition. The BRI is essentially the externalisation of a growth model heavily dependent on state-owned enterprise-led infrastructure investment. The 18th Party Congress had recognised that this model was unsustainable within China itself. A new-growth model requires structural changes that Beijing is unsure how to make without risking internal instability that could jeopardise Party rule. Taking this BRI and exporting it buys some time for Beijing to deal with this fundamental question. It remains to be seen how it will be dealt with by President Xi.

It is however becoming evident that transplanting the Chinese model overseas can result in serious liabilities for both China and the recipient countries: the debt trap among them. The Chinese presence often evokes as much resentment as admiration or gratitude and China suffers from a persistent deficit of soft power.

In South East Asia, concern over the terms of agreement have led to delays in several projects, anecdotes about the overbearing Chinese presence and it's undesirable consequences are in fact common in Southeast Asia. There's resentment and pushback even in countries highly dependent on China.

Let me give you a couple of examples. In January this year, the Governor of Sihanoukville in Cambodia wrote a letter to the Interior Ministry complaining about how Chinese investment had increased crime, causing insecurity in the province. This letter was a highly unusual event in Cambodia and, equally unusually, the Chinese embassy in Cambodia publicly acknowledged that

there were indeed problems, although it argued that, overall, Chinese investment was positive, as it is. Laos is a fellow Leninist state and has a close relationship with China. Still, in 2016, at the 10th National Congress of the Lao People's Revolutionary Party, Choummaly Sayasone, a Politbureau member and Deputy Prime Minister lost his positions; he is ethnic Chinese and reportedly overly pro-China.

China's activities among overseas Chinese communities in South East Asia, leads Beijing into some very sensitive, indeed dangerous, territory. The goal of such activities was neatly summarised by the title of a 2014 speech by President Xi for the Seventh Conference of Overseas Chinese Associations. The title reads as follows, "The rejuvenation of the Chinese nation is a dream shared by all Chinese." In plain language, overseas Chinese should identify their interests with China's interests. In January this year, at the National Overseas Chinese Affairs Conference, Yang Jiechi who is now a Politbureau member, called upon the government to expand and strengthen, and I quote, "…overseas Chinese patriotic friendly forces in the service of the great rejuvenation of the Chinese nation."

This is clearly, in effect if not formally, a significant shift away from the PRCs overseas Chinese policy that has helped since 1955. A deliberate blurring of the distinction between the (31:56) that means PRCs citizens and Huaren(31:56) which means Ethnic Chinese. That policy began to change as early as 1998 when vicious anti-Chinese riots in Indonesia forced Beijing to very gingerly admonish Jakarta. The shift of policy has become more apparent under President Xi and has raised concerns, even if they are not always articulated in public. Concerns are particularly serious in Malaysia and Indonesia where both the TNI (Indonesian Military) and political Islam remain suspicious of China. Concerns also exist in Brunei, Vietnam, Myanmar and Thailand.

For Singapore, my own country, it raises existential issues of national identity on which we cannot compromise. I don't think that Chinese diplomats in South East Asia are oblivious to the complications and dangers. But, since the re-orientation of policy towards the overseas Chinese, has been linked to President Xi's China dream and the great rejuvenation of China, there is reason to wonder what exactly is being reported in the context of President Xi's firmer insistence on party discipline. A return to the previous overseas Chinese policy may not be easy or timely. It may take a crisis, which could be extremely damaging to China's position in South East Asia. Now, ladies and gentlemen, in drawing your attention to these issues, my point is not that China will fail. I do not think that China will fail. But the BRI in south East Asia, as in other regions, is going to face competing demands on Chinese resources which are vast but not infinite, will pose problems both for China and recipient countries, and its implementation will therefore be patchy and will not unfold along a smooth trajectory.

Some BRI projects will work better than others. Some will succeed, some will stall and some will fail. This is the normal state of affairs for a strategy, if it is a strategy of such vast scope. Every country in East Asia wants to benefit economically from China's growth. We would be foolish not to do so. But no-one is going to accept a relationship with China that curtails the autonomy to pursue other interests and other relationships. The US, Japan, India, Australia and South Korea, among others, are not suddenly going to disappear from East Asia. They are all substantial economic partners and while contiguity and strategic weight will always give China significant influence in South East Asia and indeed in East Asia as a whole, significant influence is not exclusive influence, or even dominant influence. As in the previously mentioned cases

of Cambodia and Laos, while some small independent countries may not have much room for manoeuvre, they will use what room exists.

The basic diplomatic instinct of South East Asia was best summarised by what a senior Vietnamese official once told me. I had asked him what a change of leadership in Hanoi meant for Vietnam's relations with China. He replied, "Every Vietnamese leader must be able to get along with China and stand up to China and, if anyone thinks this cannot be done at the same time, he does not deserve to be the leader." In the Philippines, President Duterte has re-calibrated the relationship with China and I think he's correct to do so. But despite his penchant for downplaying American importance, he retains the alliance with the US and has cultivated a closer and a stronger relationship with America's principal East Asian ally, Japan. China has reportedly bought large amounts of Malaysia's One MDB debt but the Seventh Fleet still calls at Malaysian ports and American aircraft still fly missions over the South China Sea from Malaysian airfields.

As a big country, Indonesia has its own vision of its role in the region and globally, and it's diverse and active. Free and active foreign policy is an integral part of Indonesia's national identity. Vietnam exists because, throughout its history, it has refused subordination to China. Similarly, in North East Asia, a core element of Japanese and Korean national identities is the refusal over many centuries to accept permanent incorporation in the Chinese regional order. India is as big a country as China and as ancient a civilization. It has its own concept for regional order that it is never going to be subordinate to anyone else's ideas, be they of China or America.

The main risks that have emerged under the Trump administration are in trade. The greatest weakness of the Trump Administration's emerging strategy is the failure to make the connection between security and foreign policies and trade policy. In East Asia, trade is strategy. The Trump administration's de-emphasis of multilateralism in favour of bilateralism and on fair, not free, trade and its declared intention to retaliate robustly against what it perceives as unfair trade carries serious risk for all countries in East Asia; for all countries in East Asia but the main target— as in those two documents I sighted earlier, the national security strategy makes clear—is China.

China cannot replace US leadership. The US led by being open and generous. The universality of the American or, in general, the Western model, was a delusion. Still, American openness allows adaptations of it, particularly its economic aspects to develop around the world and more or less voluntarily link themselves in one way or another with the United States while retaining considerable autonomy. America, under the Trump administration, is clearly now less prepared to be generous.

Despite its win-win rhetoric, the Chinese approach is far too transactional to replace American leadership. It engenders resistance as well as compliance. Moreover, the Chinese model is built around the structure of a Leninist state of which only five remain in the world, and it's too deeply, far too deeply Chinese in its characteristics to be widely replicable elsewhere. In Davos in January last year, and again at the APEC summit in Vietnam in November last year, President Xi Jinping delivered eloquent defences of globalisation, suggesting that China was ready to lead if the US was not. President Xi's speeches were rhetorical extensions of his great rejuvenation narrative rather than settled propositions. They were as much indirect expressions of anxiety about what it may mean for China if the current global order should unravel as they were expressions of confidence or leadership.

China was the main beneficiary of the US-led post-Cold War of globalisation and the international multi-lateral trading system. It could also be the main loser if that order descends into further uncertainty because of a lack of leadership. China's rise and the Belt and Road Initiative (BRI) are built on the foundations of the current open US-led order. Can an open order be maintained on the basis of a still largely closed model? It is precisely how much more and how China should open up, that Beijing is yet to decide. The BRI is not a practical alternative to the current order. Can the BRI succeed if the US and China stumble into a trade war, or the world turns protectionist? I don't think so.

Even though China criticises the American alliance system as a Cold War relic, insofar as that system is an inextricable component of the broader global order, China's attitude is, in reality, more ambivalent. If we keep this firmly in mind, one of the most prevalent, perceived binary choices between the US security provider and China as a major trading partner, will appear less stuck or daunting. In any case, trade is not a favour one country does to another. If there be no mutual benefit, there will be no trade. Again, I'm not suggesting that China will fail or never exercise global leadership. China ought to have a greater share of the burdens of global order from which it has benefited.

China will certainly play an increasingly important role in global institutions such as the UN, the World Bank, IMF and the WTO. It has created its own supplementary institutions such as the AIIB. My argument is only that, for the foreseeable future, it is to my mind far more credible to envisage China playing a bigger role within the existing order than see it displacing the US as leader, or China replacing the current order with its own order. China is not happy with every aspect of the current order. It has no reason to whole-heartedly embrace an order it regards, not without justification, as successor to the order responsible for what it calls, 100 years of humiliation and which it had no say in establishing. I do not see China as a clearly revisionist power. I do not think China is eager to kick over the table; it has benefited from the table; it is content to let Russia take the lead in confronting the West in Europe, while it tries to stabilise its relationship with the US in East Asia. This does not mean that China will not pursue its own interest at times very assertively, but it is not reckless and it is not looking for trouble.

In the South China Sea for example, a ritualised pattern of FONOPs and interceptions seems to be emerging. Admiral Harry Harris, Commander of PACOM, said in 2016 on the sidelines of the Shangri La dialogue in Singapore that unsafe incidents in the South China Sea were in fact rare. East Asia is a complex and diverse region. Complexity and diversity makes for a natural tendency towards multi-polarity, not bipolarity, let alone uni-polarity. The period when there appeared to be only one US–led regional order was in historical terms, brief and exceptional.

We are now in a period of transition to a more historically normal situation. There's good reason to belief that East Asia's future would be multi-polar. I believe that the future East Asian security architecture is likely to consist of multiple overlapping frameworks. This is messy but East Asia is a messy region. In messiness, there is greater resilience than in any single framework, if a single framework can in fact be imposed on a diverse region, which I doubt. Any single framework may be brittle and an architecture of multiple overlapping frameworks is in line with the omni–directional balance embedded in the concept of ASEAN centrality, and provides greater manoeuvre space for small countries. However, meanwhile, until such architectural multiple overlapping frameworks emerge, we will have to navigate a period, but how long no– one can tell,

of more than usual major power competition, more than usual complexity and more than usual uncertainty.

Ladies and gentlemen, I began by stating that the binary framework is an inappropriate mode of analysis. I trust that I have said enough to persuade that this is so, particularly in periods of uncertainty. I also said at the beginning that, under some circumstances, the binary fallacy could be dangerous. Let me conclude by elaborating that statement. This leads me into some sensitive territory. Let me make the standpoint from which I speak absolutely clear—I am retired. I am a pensioner. I stand before you as a pensioner who speaks only for himself. Moreover, I speak analytically, and not from any moral pulpit. All major powers compete for influence. They do so in the same way as natural disasters occur. At least it appears so to small countries like mine. It is just a fact inherent in the structure of the international system of sovereign states and perhaps inherent in human nature.

Singapore has had to deal with influence operations by the United States. It was not so long ago that we had to expel an American diplomat for interfering in our domestic politics, as we have had to deal with influence operations by other big countries. It is to my mind as pointless to complain about attempts by major powers to acquire and exercise influence by any means available, as it is pointless to complain about earthquakes or floods or typhoons or other natural disasters. We just have to prepare ourselves for the eventuality and deal with it. If we do not prepare ourselves adequately, it is our fault and not that of the major power because they are what they are. To deal with this, we have to understand the nature of major power competition for influence. I think China understands better than any other major power that competition for influence is as a much, and perhaps even more, psychological as it is material.

Sun Tzu, the great Chinese strategist wrote, "To subdue the enemy without fighting is the acme of skill". China's insistent diplomatic tactic is simple but effective, and is deployed with great creativity—to pose false choices, and force choices between these false choices. It seeks to instil a sense of fatalistic inevitability about the choices presented. The general narrative within which this tactic is used is of China's inevitable rise and America's inevitable decline, and that East Asia should therefore place itself on the right side of history. This is a powerful narrative but a crude distortion of reality. The binary mode of thought, which oversimplifies complexity and is strongly deterministic, sets up an almost perfect framework for promoting false choices, particularly when coupled with unbalanced criticism of American policy under the Trump Administration, such as we are now experiencing.

Now, please don't misunderstand me. I am not arguing that we should not criticise US policy when criticism is due. Safe navigation of complexity requires a critical appraisal of the policies of all major powers and America should not be exempt. Trade is certainly one area that requires criticism. The Islamophobia that seems to infuse some sections of the Trump Administration is another. Safe navigation of complexity also requires calm detachment. I've tried to persuade my American friends—most recently a week ago when I was in Washington DC—that their unbalanced and sometimes emotional criticisms may be taken far more seriously than warranted and may well stampede some countries into accepting false choices. So far, I confess, without any discernible success in changing their minds.

On that note, I shall end, but not without thanking you for the patience and courtesy with which you have listened to the ramblings of this pensioner and remember that I am a pensioner.

Energy Security

Air Vice-Marshal John Blackburn, AO (Retd)

Chief of Air Force, distinguished guests, ladies and gentlemen, good morning. Energy security; if we don't have it, everything the chief said this morning about our fifth-gen force will not work. It is that fundamental. Without this, without resilient supply chains, we will not be able to operate, and our support infrastructure won't either.

Now, when you start these things, you're supposed to quote some air power theorist, so I'm going to quote an old friend of mine, great Captain Doc Miller (well he's a solid air power theorist!). This is what he wrote in a brief to Jeff Brown when he was chief, and it seems really obvious: "You know, Government and the Australian population expect Defence to operate when markets fail. We're not just there for fair weather". But you would not believe how this fundamental thought is fundamentally ignored in our approach to energy security in this country. I'd like you to think about that as I talk, but I'd also like you to think about this other issue. National security depends on energy security. Again, it's a blindingly obvious statement, but the energy industry here says it's not appropriate to connect the two of them. We have to keep them separate.

Now, what's happening in the world? We're undergoing a major energy transformation, and not just in the energy sector, because it's completely linked with other issues. Climate change is going to have a significant effect, and Admiral Morisetti will be going to much greater depth on this when he speaks after me. It's going to affect our supply chains; it's going to affect security eventually. But more importantly, if we continue to grow economies, and we grow populations, and we grow our energy consumption, because GDP growth and energy consumption are pretty closely matched as they grow, by 2050, we'll have somewhere between 50% or 100% more energy consumption.

We can't afford to use the types and mix of energy that we do today in 2050, because we will poison ourselves. The other issue is economic change. The transition in energy is going to cost money. Shell's study says there's about $55T worth of infrastructure, and fossil fuel infrastructure in the developed world. As we transition to a different energy mix, where's the money going to come from, particularly with stagnant economies? The other economic change that is going to really hit on a politics level, is that energy prices for East Coast consumers in Australia went up 12% last year, six times the average pay rise.

Now, that's the near-term political problem for people which has to be addressed. Technology changes will afford great opportunities for us if they're applied intelligently, and I will argue they're not being done that way, and we'll see changes in consumer behaviour and market reform. So, what we've got is this incredible spiral area that we're going to have to navigate. The question is, can Defence and our nation get secure and resilient energy supplies as we go through this transition over the next few decades?

Now, energy issues are so intertwined with other security developments that defence forces cannot ignore them. But it's not just about fuel stocks. When I talk to politicians, I ask how many days of stocks have we got in defence? It's far more complicated than that, because even if you double the stocks, if the interruption lasts longer than a period, you're still stuffed. The other

thing is to paraphrase Professor Ken Baldwin from the Australian National University—he runs the Energy Change Institute.

He says that defence organisations must understand this ongoing change of transformation in energy. The complex interactions between energy and geopolitics, as the ambassador spoke about this morning, is fundamental understanding, not only for the job in terms of military operations, but understanding how the world works. Foreign investment and ownership of supply chains is a critical issue for us to understand. We have to understand energy and cyber-attack, energy and resilience in the face of climate change; and we've already balanced some of the short-term issues with the longer-term opportunities. NATO, a couple of years ago, put up these three things that they were focusing on. I'm going to talk briefly about two approaches in the US military, and one in the US think tank that I think are excellent examples of how we should be addressing energy security. The US 2016 Operational Energy Strategy talks about increasing war-fighting capability by including energy throughout force development.

I can tell you that, as a defence consultant working at an industry, I see proposals coming out the door, and they could have been written in the 1990s as far as energy discussion goes in them. They want to reduce logistics and operational risks from operational energy vulnerabilities, so we need to understand it. This think tank, which is the Energy Security Leadership Council, is fairly impressive in the US. There's a whole bunch of retired generals and admirals on there, but a lot of existing business leaders. What they've said is, "Look, this market-driven approach is the best way to approach our economic challenges, but there are some things you cannot leave to the market alone."

The example they talk about is oil, and where foreign governments can control or influence your energy supplies, only government action can address those threats to your energy security. It's a pretty fundamental point. So, where do we look for our energy security and what the government policies are? Well the last paper was the 2015 Energy White Paper. When you read it, it's actually quite good. We're a growing energy superpower. We are actually the ninth largest energy producer in the world. We're endowed with vast energy resources, which they said will give us low-cost energy. I don't think it's quite worked out that way when you see what our cost prices are!

The Energy White Paper talks about our guiding principles that should be about leaving it to the market to operate freely without unnecessary government intervention. In fact, most of the Energy White Paper is about making sure the markets work effectively without government interference. It also says that the government will monitor energy security through a national energy security assessment; it was due to be published in 2015. Well, it didn't come out in 2015, it didn't come out in 2016, it didn't come out in 2017, and if it comes out this year, it'll be a miracle. So, the only energy security assessment we have was done in 2011. The world has changed significantly in the last six years and, that energy security assessment, I have argued repeatedly in public, was fundamentally flawed.

It didn't look at any of the scenarios; for example, we would look at in Defence to justify the $30B a year that we spend in the defence of our nation. In other words, we've worked out the technical and platform things we need to do, but the energy security assessment doesn't look at any of those scenarios. So, where do we stand within Defence about our policy and approach to this? Well, a logical place to start would be the Defence White Paper from 2016, but there's nothing in it about energy security. It talks about remediating problems in defence's energy—oh sorry, fuel infrastructure, largely, and resiliency problem, but it doesn't address it.

When I look around Defence, there are very good developments across defensive services and defence sciences, but in piece parts. Army's looking at deployable power; Navy's got wave generation on the West Coast, and Air Force has talked about some solar areas. Some good innovations are happening with the innovation hub, but that's all I could see. The Defence and state energy strategy is pretty good, but it looks at identifying energy consumption needs, changing behaviours, energy efficiency, some renewables and, while it does mention the need to look at the resilience of power supplies, for example, to our bases, it can't effect any change from where it stands. I was very impressed in 2016 when the Defence magazine published this about the defence energy integration framework—it recognised the large amounts of energy and the dependence we have on fuel supply lines. Now, I'm talking not just about fuel. It's electricity, gas, fuel, renewables, everything that we have in the country. It recognised the challenges and the vulnerabilities of them, and the aim of this framework was to ensure delivery of sustainable energy for operations both now and in the long term. Very enthused at looking at it.

So, since 2016, what's happened? It's faded from view. Folks tell me inside the organisation that it was never resourced. Now, that's not unusual. As we know, some of our change processes start out, but we don't resource them. That's disappeared. As of today, as far as I'm aware, or certainly as of December, there is no Defence operational energy strategy. So, let's go back to what the Americans are doing right now. There is no defence operational energy policy, and I can't work out who's got the lead. This is not something you chuck to CJLOG and say, "Well the LOGGIES take care of the enablers." This is a fundamental national security issue. Now, I've had a talk to CJLOG about this, and I admire the job he's doing, but it's not his job. This is a much bigger issue.

What do people outside of Australia think about this? The International Energy Agency (IEA)—we're one of 29 member countries—published their review of Australia's energy policies last month, and this is what they said. "Whilst we're endowed with natural resources, there are energy security risks across several sectors that have increased. The signs of the Australian energy system are showing signs of stress. The energy policy governance in Australia is very complex and fragmented." They also tell us that we're increasingly exposed to new challenges for maintaining security of supply and, if we'd had proper monitoring, analysis, and planning, these issues they're now seeing could have been signalled earlier and remedies could have been applied. That's a slightly different picture than when you read the Energy White Paper. They do go on to say, "We do need a strategy." That's fairly obvious. They then tell us that we're the only IEA member country, which is a net oil importer—we import 90% of our transport fuels—that solely relies on commercial stock holdings for the industry to meet our obligations.

It also notes that we're, as an IEA member country, unable to meet any of the two main obligations we have as a member: that's a certain level of stock holdings, and the ability to contribute to the release of stocks to the market in the event of a supply disruption that happened back in the '70s. It also said our country's oil stocks are at an all-time low. We're having no strategic oil stocks at all and we've not placed any stock holding obligations on industry. We're quite unique compared to developed countries. Most of them actually do this. Now, when I've been talking to politicians about this, they say, "Well if we run into a problem, we'll go down to the nearest Defence base and we'll access their stocks." I had to inform them that we don't have strategic stocks, and they were quite in shock.

They tell us that our policies in the oil sector, for example, about efficient and flexible markets, are unregulated in the business as usual. But when do you shift from business as usual to conflict?

I'd argue we're in conflict now for some reasons that I'll cover later. They also say that our focus on ensuring the oil market operates efficiently and flexibly is a good idea. But here is the rub. The IEA then told us this. It is less clear how we in Australia would respond in the event of a serious oil supply disruption leading to market failure. I ask you, do we have a secure and resilient energy system?

Now, these guys aren't amateurs. They, not only for IEA member countries, spend a lot of time analysing energy security around the world. Let's step back to the white paper. The 2015 Energy White Paper didn't refer, for example, to electricity supply security. If you step back to the 2011 NESA it did. It said, hey, we're going to get improved reliability of our electricity supply, as current infrastructure investments replace ageing network infrastructure. But it also said that it's not the government's job to do that; that's the market's job. Well, what happened? For the benefit of our foreign visitors: back in 2016, we saw ourselves confronted with a state-wide electricity blackout in South Australia. It was a systems failure, like rolling a bowling ball to a set of pins; things started to fail, it cascaded. In the end, it disconnected the South Australian and Victorian power supply connections. That was apparently considered a non-credible scenario before it happened.

This led to a huge reaction, mainly political fights and blame sharing, and the Finkel review, which looked at electricity markets and little bit of the gas market because, as you may or may not be aware, the electricity can't operate without gas. They've created an energy security board to look at the security of the system. There is no Defence representation on it. I've got to tell you, Defence and parts of ODG, in my view, are the two areas that actually do understand security rather than just market forces and should be included. When the IEA did its assessment of this, it said—and I'm paraphrasing here—there's a significant design weakness in the electricity networks and systems because it's all being done in pieces that can lead to power system disruptions. Well, it did, and it could be there again. We've got similar problems in Tasmania.

I think, though *The Sunday Age* came up with the best analysis of our power failures in South Australia that I've seen. If you are working in Defence and you look under your desk, you'll probably see something like this. And you do know from experience that when you kick out in frustration and kick one of these plugs out, things happen that are not good. Sticking another plug on the top called the booster—Australians would know what that is—is not going to make much difference.

Let's leave that aside. As our previous speaker said, I'm also a retired pensioner, so why am I bothering with this little stuff and talking about it? Well, after I left Air Force full-time service in 2008, I got involved with a series of think tanks and studies. One of the first ones I did along with Dr Gary Waters, who's floating around here somewhere, was to look at our cyber security challenge in Australia. I was at one point responsible for cyber policy in defence. I actually thought I knew a fair bit about it but, as I started to look at the broader national infrastructure, the assumptions I'd made about the resilience of systems were done from a Defence viewpoint. They were false; my assumptions were fundamentally wrong.

The fragility that I saw in this, which Gary and I saw in our national infrastructure and our supply chains, worried us. Here is a CERT report that came out looking at the vulnerabilities and attacks on our systems in Australia. Energy is the big red piece at the top there. Their report said that the energy and comms sectors had the highest number of compromised systems and the energy sector is one of the ones with the highest number of malicious emails. Now, it's not just an issue of ownership. Only half of our energy companies are actually wholly Australian owned. But there

is something going on here, and the resilience of it is a problem. If we don't have an electricity system, our bases don't operate, our support entities in this country don't operate, and we can't deploy. Just look at the news in the last week from the UK. This is the Guardian. The US has now accused Russia of a cyber-attack on the energy sector and imposes new sanctions. In other words, they found malware and problems in there. The UK finance, power, and water sectors are on the highest alerts for threats of a Russian cyber-reprisal. Is this business-as-usual peace time? No, it's going on every day. There's a state actor not operating in accordance with the rule of law.

After we did that study, I went over to Defence logistics because we were concerned about supply chains, and we found exactly the same problem on assumptions. When I was a Deputy Chief, I didn't think about this stuff. The LOGGIES were taking care of all of that; nice bunch of folks, and I asked senior LOGGIES how come I didn't understand? They said, "Well, we used to tell you we'd fix it and so you'd go away and we'd fix it." That's all right for reaction to reactive changes, but I realised I didn't understand probably one of the most important things for a military, and that's logistics. It's not built into a lot of, certainly pilots' DNA.

People were telling me at the time, when I did the study: we don't need to worry about field security because we've got contracts with industry. So, I went off and did three studies that were one of the triggers for the Senate inquiry of 2015 into energy security, particularly fuels. I asked the question, will market forces take care of it for us? I had the opportunity to meet with one of the CEOs of the four oil and fuel companies in Australia. I won't say who it was because it was a confidential) discussion. There are only four of them, and I said to him, "What do you think about energy security? In the market, you guys have got the triggers on this". He said, "Energy security is not my job." About then, I got a bit stunned, and he said, "Energy reliability for my customers and for my shareholders is my job. Energy security is not my job." When you listen to the industry talk about this, they talk about reliability of supply, not security of supply.

I'll show two diagrams from the reports I did to give a sense. This is a graph per month for fuel imported or oils imported over time. The top red line shows the growth in energy consumption of liquid fuels for transport. The higher part of the graph is what we were importing directly as refined fuels, largely from Singapore that time. The middle part of the graph is what we refined from imported oil. The bottom part is what we've been refining from Australian crude oil. Of the types of oil that we use in our refineries, three out of the four only use heavy crude. The resources are declining at a faster rate than is being replenished by discovery. The point here is that we went from 60% imports in 2000 to 91% of imports for our transport energy as we passed 2013. What's not shown on here is the refining industry. Between 2012 and 2015, we have closed three of the seven refineries. I went to the then Department of Resources, Energy and Tourism and I said, how many refineries should we have? What's the minimum number we need for resilience? The answer I got told was that we don't need any because it's cheaper to import fuel.

Hang on, a lot of other countries—Norway and a whole bunch of other countries—do have refineries even though they've got extensive stocks, because there's a reason for this with resilience. The other thing is that, when countries don't have a huge amount of stocks or they have concerns, they start to put other measures in there to give them resilience in their supply chains. This shows the number of days of fuel stocks that governments mandate their industries to hold. In Australia, it's zero. Look at Korea and Japan, look at Europe. This is back in 2014. If you're an EU member, you have to hold 61 days of imports. It's an important part of your resilience, but fuel

stocks alone aren't the answer because fuel flow is the answer. You need to assure a continuous supply sufficient to operate critical societal functions and, in our case, military functions.

The other way you do it is to hold strategic reserves. Again, we're very consistent here in Australia; we have none. Look at the figures underneath there: what other countries are doing. ASEAN+3 has been looking at a lot of stuff about fuel security in recent years. You look at what China was doing with fuel security and Japan and other countries. What is it that we know that gives us so much confidence that we don't have to mandate stocks, we don't have to hold stocks, and we don't need a refining industry when we're at the end of a very long supply chain? If we have a major problem in the electricity or gas sectors, despite everything in the market, the government can't intervene because the energy comes from Australia. If we have a problem in the fuel sector, the government can't do anything because 91% of the energy comes from overseas. So, a bit of a challenge there.

Whilst I was doing this, I had the opportunity to speak extensively with Dr Greg Calbert. He's a DSTG scientist who was the 2014 Secretary of Defence fellow and his studies were in fuel security. Just give me a sense; who's read his reports? Ooh, I can't see anybody. Okay. He makes a whole bunch of really interesting points. He talked about the shift of fuel product sourcing. We used to source most of our products from Singapore, but it's now shifted up into the north-east Asia region, from South Korea, from Japan. I think in the last year or two, we were importing 25% of our refined aviation fuel straight from China. He raises the point about the nationalisation of oil supply companies in the region. We're not dealing with companies now, we're now dealing with governments who are supplying us fuel from the area. He raised the point of the rise of tensions in the South China Sea: more than half of all our refined fuel products are coming through the South China Sea. The concerns he also highlighted were the dependence of Asia on the Middle East and North Africa crude for everything they do, and the emergence of strategic weapons systems in the area and what that means for our security of supply. Again, in the last week, Saudi Arabia announced that, if Iran goes and gets nuclear weapons, they're going to go and get them as well.

Just have a think at what they could do to some of the security supply. He talked about the closure of refineries in Australia, the growing fragility of our own fuel supply chain, and the decline in relative financial power. Projecting to the next decade, we have supply shortages. What's your relative economic power to get those supplies when there's competition? If there is a problem, are the countries who are holding strategic stock holdings going to release them to us? Why would they, if we've been dumb enough not to hold stocks ourselves? His bottom line is this: we're in a strategic warning period for fuel security. This is a diagram I presented to the Senate committee when we were talking about fuels. Now, energy of course is much bigger than this. I said look, we have a very poor energy security assessment; it's way out of date.

There are zero government-owned fuel stocks in a strategic sense—I'm not talking about Defence's training stocks and the zero mandated fuel stocks. We're 100% reliant on the market and there is no Plan B. If there's a market failure, we're stuffed. The IEA just said that, so it's not just me as a lunatic saying it. What's happened is we've actually passed the responsibility to industry.

At the Senate inquiry, the oil and fuel industry representatives said this: national security scenarios are not appropriate for fuel supply security assessments. The senators were fairly stunned. If we apply this in the military, we would never buy a JSF because all we'd do is look at

the last ten to 15 years operating against terrorists and we'd go off and buy something to operate against terrorists. But we are buying a very capable system in this country in Defence. But we're not thinking about that in terms of energy security. They also said, and this is what surprised me, it's not the role of fuel distributors to hold battle stocks, that's the role of the industry fuel users. That amazed me. Hang on, surely you should, if the Government says you hold stocks. No, that's not the case. Now state governments are the first line of respondents to fuel supply interruption. It's their responsibility. The Federal Government can step in later if they have to but there won't be anything left to step in on. But the West Australian government, for example, during its 2016 disruption report said look, the fuel supply system's really good, but it could get disrupted. That's beyond the state government's control, and what they recommend is that individuals, businesses, companies, and agencies work out what their fuel needs would be in the event of a supply disruption and take appropriate measures to get fuel.

The reason one of the politicians came to me is, I think, that one of his constituents went to him with my reports and said "What should I do?" What are you going to tell some pensioner who says "What am I supposed to do with fuel stocks?" Please do not do what a UK minister did in 2012, when well-meaningly suggested, in the event, which I think was a fuel tanker driver strike, go and get some jerry cans and put fuel in it and put it in your garage. Well some poor lady in York—and this is true, I've traced it down enough times—some poor lady in York was decanting one these jerry cans in the kitchen to get some fuel for her daughter's car and she had the gas stove on: 40% burns.

What I've said to politicians is please don't tell people to go and stock fuel at home, but that's what the West Australian government report says now. When you pass it to the users, the industry also said most users don't hold stocks because they think they're being held for them by government or industry or else they think they're going to be preferred users. In essence, the big users have passed the buck back up again. When I showed this to the senators, I said Monty Python couldn't write this script. It's real.

So, what's the vector as a result of that? The first recommendation of a Senate inquiry was that we have to do our comprehensive whole-of-government risk assessment of our fuel supply vulnerability. Now, I'll argue that we should look at energy as a whole. The last NESA was done by economists. Now, I'm not having a go at economists, but energy security is too important to leave to economists. You've got to have a mixed group, and you need people with an understanding of security involved in the discussion. Last week, the Joint Committee on Intelligence and Security, after reviewing our critical infrastructure bill, made this recommendation.

They've said that the Department of Home Affairs in consultation with Defence and the Department of Environment and Energy needs to review and develop measures to ensure Australia has a continuous supply of fuel to meet its national security priorities. I think we've got a challenge and a bit of a problem here. Where are we now? If you accept that the Government or people of Australia expect Defence to operate not just when the markets are hunky dory, but also when there's a problem, then we've got a few wishes. Our analysis of our resilience is poor, operational risks are high, energy security has been outsourced to the market, and it doesn't want that job, and the IEA says we have a problem.

Where is the upside? So now I'm going to get optimistic at the end. Is there something that we in Defence and in the type of thinking that's happened with Defence in recent years—and I refer to Plan Jericho here—and some of the work that's happening on integrated force design, is there

something that Defence can bring to the discussion of energy security in this country? I'm going to use the artificial construct of generations of capability. We talked about the JSF as a fifth-generation fighter and the F-18 as fourth-generation. Well, I had the opportunity in the Reserve to work on Plan Jericho for two years supporting AIRCDREs Chipman and Campbell, who I think are here today, and it was interesting. This wasn't just about buying more fifth-gen platforms, it was about using that transformational opportunity of a fifth-gen technology to actually integrate the fourth-gen platforms in a different way to improve their capability, and then, in turn, to amplify the capability of the fifth-gen as well.

It was a change in thinking. It was about integration, not just the platform level of stepping above it. We did realise early on, however, that, if you just did it for Air Force, that doesn't make sense. It really has to be a part of a fifth-generation integrative force. Again, as a Reserve Staff Officer, I had the opportunity to support some of the VCDF folks working on that in the last two years. It's about integrated design, and it's about a cultural shift away from the platform to thinking about the system level. There's a lot of good lessons that came out of this. Could we apply some of that integrated thinking to the energy sector?

Well again, I'm going to use that construct to describe energy. It's artificial, but still, I think biomass is gen-one. The vast majority of human history has been biomass energy. I call coal gen-two—about the 18th century. Oil and gas gen-three—19th, 20th century, and I call nuclear and renewables, even the latest technologies gen-four. Why? Because it's being acquired and fielded the same way that we were doing gen-four platforms. You buy all the technology pieces and you hope that something will integrate them together; LINK16 will solve all our problems, but not in the fifth-gen environment, it won't. What we're doing today is building energy in pieces not as a design system.

The question is, is can we—and again, I'll use the corny term—should we talk about a fifth-generation integrated energy system? Can we take that design thinking, change the thinking about it and push it there, and will the market provide for that? Two weeks ago, I sat in a very interesting meeting in Sydney between some advanced energy technology people and investment bankers. I appreciate that people think Defence is very hard to deal with because they can't understand acronyms and how we think, but I've got to tell you, investment bankers have got it all over us. I asked them that, when you're looking at investing at this new technology, what value do you put on the benefit to the security of the system, and the resilience of the energy system when you make that investment of huge amounts of money? The answer is we don't. We're interested in the return on investment for that piece of energy. Can I make money from that? And we'll look at the cyber-security of the system we're going to put on the ground. The bigger picture of the other things is not our job. That's the Government's job and they need to create the market incentives and directions and regulations to make it happen. Can you see a common theme here? This idea of an integrated energy approach is explored quite well I think in the ASPI report from last August (COL Neil Greet and Dr Paul Barnes). Again, if you're interested in this area, go and have a look at it. It talks about how you get resilience in our energy system in Australia and it's not just fuel; this is a much bigger picture.

I'm going to give you an example to finish off, of what I think fifth-generation energy could be. Here are the two points that come out of this report that I think are worthwhile looking at: we're fragmented and stay apart. The example that I want to give is solar and wind. Despite having the highest deployment of solar on domestic houses in the world apparently, solar and wind

contribute about one per cent each of our energy supplies. The trouble is they can sometimes provide more energy than you can use and so it's dumped. In some cases, our infrastructure can't handle the amount of energy that they can produce, and thus move it across the country. In other cases, our infrastructure doesn't produce energy when you need it. Is there some way of integrating energy to do something different? I think of hydrogen as an example. From the excess energy, you can produce hydrogen with the latest electrolysers and you can store it.

What I'm talking about here is a time and mode shift. Yeah, we can produce hydrogen and sell it; that's fourth-gen. Could we use this in a different way? Yes, we can. We can use it for power generation, hydrogen gas turbines; we can produce ammonia which is essential in Australia as a fertiliser source, but we also have engines that can use ammonia now; we can pump it into gas systems, that's being talked about in South Australia to amplify or to expand the amount of gas we're using, we can create a gas-run; we can use it with transport, with the new generation fuel cells—the first hydrogen in cars will be in the market in Australia this year, the US military is already testing Army vehicles based on hydrogen; and we can export it. Japanese government has a large plan, a significant plan to use hydrogen, green-sourced hydrogen, eventually, as a part of their energy system. There's going to be a huge export market. The analysis here in Australia is that it could equal our liquid natural gas exports; that's large. Our advantage here is our solar footprint compared to most other countries.

We can use all that but we can do it different scales. In Italy, two years ago, I saw a small system that used hydrogen, solar and batteries between one kilowatt and ten kilowatts for emergency services, HAD, and the military. Imagine deploying to an area where we can actually generate your energy and store it and use it in different ways rather than having to have the fuel come from the Middle East, go to some refinery in Asia, then come back through a long supply chain, and withstand all the risks associated with it.

I'm not kidding myself; we're not going to fly a JSF on hydrogen, but if we can look at our energy supply chains in a different way and reduce some of that vulnerability, then we should do it. We can also apply it here. The only way to store hydro and solar at scale is pumped hydro; so wind and solar scales, pumped hydro. That's going to take ages to get to. We now need to look in Australia at producing regional or sub-regional networks, or measures using these types of energy integrators to amplify and make more resilient what's there. It's about integration, resilience, economics, energy security, and scalability.

Will the thinking about design emerge from within the industry? I can tell you that my view is, 'no'. Where the opportunity is, if Defence can argue on the basis of national security, then an integrated approach to capabilities or fifth-gen, if you want to use that term, could be applied to the energy market, which will benefit us significantly.

The bottom line is that a fifth-gen force, which is what we're building, can run on a third- and fourth-generation energy system, but at a cost and it's a premium. Our energy security is fragile and we can't let that continue. I think a fifth-gen force needs a fifth-gen energy system, and that's not just a military approach; it's national. Where a defensive use of energy is involved, it needs to transform. We must have an energy strategy and policy. If we don't, we're going to run around doing really nice innovative bits—we applaud Jericho for doing this) innovation—but I've got to tell you, what does the concept and the vector achieve, it's being led somewhere, there's a framework, but we don't have that nationally. Defence has to be a part of a national energy system design process because it's a part of the national security. We have to lead, not just follow.

If a retired pensioner like me can stir up a Senate inquiry and raise these issues, imagine what defence leadership can do if it stands up and says, "We've got a national security problem. We've got to model it with concern about military capability. If we think it can be applied to this, let us be a part of the discussion." Otherwise, this magnificent aeroplane in all its glory will be about as useful as that. It won't look anywhere as good at an air show.

Here's the bottom line. National security depends on energy security. We have to lead, not just follow, and I'm calling on Defence leadership to actually do that. It's our responsibility. That's why as a retired pensioner I'm doing this. I think it's important for our people to do.

A Changing Climate

Rear Admiral Neil Morisetti, CB (Retd)

Chief of Air Force, distinguished guests, ladies and gentlemen, good morning and thank you for inviting me to this conference and giving me the opportunity to speak about climate change. A sailor, a Brit sailor, talking about climate change at an Australian air power conference. It doesn't get more disruptive than that. It's also, in fact, I'm certain; it's a first. I think it's a positive first.

As you can see from the title, I've been asked to talk about what the changing climate means to the security community, including defence. I'm another pensioner. It's another set of pensioner's views. Views that I've gained in the last 10 years as I've engaged in these issues, initially in the roles you heard described. I'm more recently trying to bring the academic community and policy makers together to get some answers.

As most of you know, the climate's changing. There's nothing new there. It's always been changing. The challenge is, today, the pace and the nature of that change. It has become more unpredictable and it's faster. We could spend all day discussing why it's changing and I'm very happy to do that in the Q&A, or in the bar tonight. For this session, though, we need to accept the views of 97% of the climate scientists. The only explicable reason for the pace of change, and the nature of that change, relates to human influence and greenhouse gas emissions. The changes manifest themselves in many ways. While the dominant effect is increased temperatures either in the atmosphere or in the oceans, we're also seeing increasing extreme weather events: droughts, heatwaves, storm surges. They're happening in most parts of the world. But the principle focus today is on a band north and south of the equator, because this region of the Asia-Pacific region is probably the most vulnerable.

Whereas many of you have already felt those direct effects, it's not the physical changes that we need to think about today; it's the impact of those changes: the impact of reduced crop fields resulting from storm surges, droughts, flooding, or rising temperatures. A one-degree centigrade overnight temperature rise takes 10% off rice yields. These impacts are many but I give five examples: rising prices, increasing acidification of the seas that risks the oceans' fish stocks, the vanishing spring melt after glaciers have disappeared, rising sea levels causing salt water to enter the aquifers, and loss of farming land. All threaten our crucial natural resources, such as food, water, and land; and it's happening at a time when demand for them is increasing because of growing populations, and greater aspirations of a widening middle class. By 2030, we will expect 35% more demand for food and 40% for water and, despite reclamation, they don't make land anymore.

Many of you will recognise the countries and the regions where this is happening. They're the same ones that are suffering from other stresses: food shortages, health issues, demographic problems, water shortages, population issues. Those parts of the world where we've seen conflicts in the past and we'll see to the future, either intrastate or interstate, result from the governments not necessarily having the capacity and the resilience to look after their citizens. So, put crudely, the impact of a changing climate is like chucking a bucket of petrol on a smouldering fire; this is where you come in, but not as part-time pyromaniacs, because climate change is not just

an environmental issue. It impacts on our prosperity and our well-being. In other words: our national security.

At this point, I normally hear a couple groans in the Defence audience. I think that audience members think along the lines of, "Doesn't he know; we're busy; we're busy enough? We don't need something else to add into the equation. Or there's no security solution to climate change so why is he talking about it?" Well, let me explain why I think this is an issue for the security community, one that it needs be engaged in but, at the same time, we need to try and focus that engagement. It isn't because I think there's a security solution; there isn't. But there is greater insecurity if governments and society do not act. The issue is that the security community is the Government agent for ensuring the safety and well-being of the nation's citizens both today and in the future. The conditions I'm describing are threatening that security. They're clearly not the only threat; I note that we've heard more about that this morning already. Today's geographical, geopolitical environment is complex and challenging. As you're aware, we face a mix of traditional, often state-based threats and Euro transnational trans-boundary ones, frequently involving non-state actors.

The expectations of my generation that, at the end of the Cold War, there would be a peace dividend haven't come to pass. Many of those traditional state threats that we thought would disappear are still here or are re-emerging. And here I include activity that emanates from Eastern Europe or the very east of Europe, and the tension in the South China Sea, and the Korean peninsula. I also include tensions as new powers grow and find themselves with conflicting interests in parts of the world, such as, the Indian Ocean. And you'd expect me to say this, but piracy never went away.

At the same time, the non-traditional threats to stability and our well-being are many. We've talked about the cyber world today, and we've talked about terrorism, or violent extremist organisations. But to that list I think we need to add the impact of a changing climate, whether extreme weather events manifest themselves with an increased frequency or occur as long-term trends. That's not to say that climate change directly causes conflict. The consensus is that it's very unlikely. Rather, we need to consider the second- and third-order consequences. Climate change multiplies the threat. What do people do when they lose their livelihood, their home, or access to affordable supplies or those resources that I was talking about? Families need to be fed and housed, people need an income. However, different communities will react in different ways depending on their circumstances and resilience.

However, faced with these challenges, particularly competing for resources, it's likely that there's going to be an increased movement of people. Again, people are always moving. The issue today is the scale and the unpredictability of that movement. The vast majority of people who move only do so within their own country, whether they are nomadic herdsmen or merely moving from rural to urban areas. The UNDP in 2015 talked about 75% of the movement of populations that year have been of that nature. Others who move to the next country may or may not be welcome there. In the context of climate change, the issue that's always cited is the fence between India and Bangladesh to stop the movement of Bangladeshi people. And of those moving, 8% will go further afield, as we saw in Europe in 2015. But there's also another group of vulnerable people: the trapped populations, those who can't go anywhere, are particularly vulnerable, and are thus encouraged to support or join violent extremist organisations.

We have two examples of how climate change has been contributing to conflict or instability even though either was initially perceived by academics and experts as unlikely. Now they agree about these examples: the Arab Spring occurred when the wheat harvest failed in Russia in 2010 so that it stopped exporting a lot of its wheat. This failure was accompanied by heavy, very wet weather in Canada, which resulted in a rise in the price of wheat. When wheat prices increase, bread prices follow. This was one of the reasons for the riots in the markets in Tunisia.

Before the seven-year Syrian conflict, discussed by a previous speaker, began was a drought that lasted nearly a decade, which is extreme for that region. As a result, crops failed, farmers left the country and moved to the cities and the towns. This movement pressured towns and cities that didn't have the capacity to look after citizens before the new arrivals and thus exacerbated existing historical tensions, some of which are religious. It is now recognised that climate change contributed to the conflict and instability in both Tunisia and Syria. For a future perspective, I don't think we need to look very far, at the environmental troubles in the Sahel region in Africa and particularly the Lake Chad crisis. The UN Security Council issued a statement in January this year acknowledging the impact of the changing climate and its pressure on resources being faced by organisations like Boko Haram, and the potential of increased instability. I think Southeast Asia is another one needing consideration.

In these instances, it's the impact of a changing climate on the threat to natural resources that contribute to instability. Now, if I were giving this lecture in the UK or northern Europe or perhaps here, people would say, "Fine, okay, I accept all that: what's it got to do with me? We're okay." Well, the reality is, in part, that I'm talking about your backyard but, also, because we live in a globalised world. In other words, the impact of local events have global consequences. The world or one of its regions being unstable has implications for all of us and they may manifest themselves in various ways.

One of these ways is that volatility arises from the prices of vital raw materials. Look at the impact of energy in 2011 with the Libyan conflict being part of the Arab Spring and yet Libya had produced 2 per cent of the world's oil. Oil went off tap so that the price went up by 20 dollars a barrel. Two financial quarters at a 20-dollar-a-barrel increase equates to one half a per cent of global GDP.

In the same year, we saw a disruption to the world due to 'just enough just in time' supply chains. The floods in Thailand meant that microchips couldn't be exported, but were needed in cars, computers, and other mechanisms. In the UK, Honda wanted to launch a new car but the workforce changed to a three-day working week. And when you're in Orange County, California, Poland, or other parts of world, laptops are scarce. The countries most affected by the impact of a changing climate are the emerging countries and their markets, where my country is certainly looking to trade in the future. It is very hard to trade with countries where there's instability and/or conflict.

I've talked about the spread of radicalisation and I talked about the movement of people. Without a stable world, we cannot have a strong economic growth. Without a strong economy, we cannot afford the security we need. Geopolitical stability is not an end-state; it's a prerequisite. So what actions does the security community need to take? And I deliberately use the term security community rather than Defence or the military because security involves a community in its widest sense, applying to foreign policy, as well as Defence and military. Security involves international development aid, home affairs, and the respective agencies.

Each agency may have its own areas of responsibility or specific areas of interest but, as with any other most 21st century challenges, addressing the threat requires a comprehensive, collective and coordinated response. There's a need to acknowledge that not only is a changing climate a risk to our national security but, it needs to be treated as a mainstream risk, not a niche one. Climate change needs to be considered at the same level as other threats. Now, many countries achieve the first bit. They recognised it as a threat. But, there aren't many that are looking at it as a mainstream threat. As well, any analysis that takes place over this needs to establish what it means for our respective countries: how the risk can manifest itself and in what timeframe. And to do that, you have to talk some people you don't normally talk to.

We traditionally talk to certain experts about conflict risk and a lot of the talk relates to state-on-state issues or terrorist organisations. But, to develop the knowledge and, from that, establish an early warning system, it's imperative to talk to long-range weather forecasters, agrarian experts, and experts in the movement of populations. And if you're not sure who they are, I can assure you they are not very good at talking to the security community. A relationship is thus going to have to be developed. You are going to need to think through exactly what the exam question is: explain how you want that information presented and when. If not, there'll be a three-tonne truck outside Russell and an academic will tell you the answer's in there somewhere in the middle, but you have to communicate the exact data you want.

That analysis of the threat of climate change needs to be fed into a review of all other threats because only then can you understand how those threats relate and influence each other to prioritise action. If you don't do that, I would suggest you have reviewed and analysed your threats incompletely and weakly. If you feed such findings into your national security strategy, the result will be inconsistent and poor. Now, the output might make uncomfortable reading for some, particularly our political masters. There's nothing new there. And the same applies when you use the analysis. As I said, it needs to inform the national security strategy and subsequently, the national risk registers. That may not be straightforward because some will say, "There's too much uncertainty associated with the impacts of a changing climate. We can't use that information."

Quite frankly, that's rubbish! We never have 100% certainty for any threat. This is no different. In fact, in many ways, we probably know more about what's happening in a changing climate than about some of the more traditional threats. Others will say it's tomorrow's problem; it's outside the horizons of the risk registers. The visual evidence, I would say, disagrees. Anyway, you need to act today to reduce the risk tomorrow. And that probably presents a challenge when you're working with governments because this is a strategic risk that needs long-term planning even though most of society, including politicians, sees short-term horizons. You've got to convince them of the need for this.

In other words, all of this goes to speaking truth unto power. And the information gained in that analysis I mentioned can be useful, not just for national security strategy, but other strategies: economic, energy, health, transport, for example. Only then will you see the benefits from improved air quality for better health, less spending on health care, and, in the process, a reduced risk to national security. That's the security piece.

What about the military specifically? Well, clearly, you've got to address the wolf nearest the sleigh, the most pressing threat. But, I would argue that you also need to use the analysis to fuel those lower level operating environment strategies, the implications for likely missions and tasks. Now, in this region, military aid to the civil power in disaster response in mainland Australia, or

humanitarian assistance disaster relief in the region, are clearly high priorities; and in HADR, I wouldn't always assume this is going to be done in a benign environment. There's also the need for increased offshore tapestry, and monitoring of your surveillance of your EEZ. Importantly, as part of conflict prevention in a vulnerable region, to work with coalition and other partners means building capacity and resilience in those countries, which are fragile. Have they got the right kit to operate in this world in the future? Do they have the resilience?

John Blackburn saw the energy strategy. Have you got an energy strategy that determines how you're going to use energy and what nature of energy you are going to use in defence? Are your people at the right level of readiness and have they had the right training? And have you got interoperability, not just with the many different actors you're going to work with, but also with your partners. If you're a jet pilot and you' go up to a tanker to get a supply of fuel and you find he's only offering a 50/50 bio-mix when you take normally the aviation, it's not really going to be the best of days. None of that is different from dealing with any of the risk we face. This is why I talk about the need to be mainstream. What I do acknowledge, because climate change is unpredictable, and the fact is that people come to you as the first responders, is that you have to work very hard to be ready for all this. And, of course, you still need to maintain the ability to do high-intensity conflict resolution that nobody else can do. So, that's the theory.

What about the practice? Among the security communities in the world. I think there's been quite a lot of progress in the last ten years. I think the first time I came to Australia in 2010 to talk about these issues, the response wasn't very positive. One of your more robust senators let me know in no uncertain terms that he couldn't understand why the British government was spending any money on this or using my time. DOD cancelled all my meetings. I'd appeared on *Lateline* the night before to talk about the issues. If I look at the submission that went into the Senate Committee inquiry on the impact of a changing climate on Australia's security last year, there's been a lot of progress. Things have come a long way, including the Vice-Chief's appointment of a Defence Climate and Security Adviser and the fact that we're talking about these issues at this conference. But, as elsewhere, I think there's more that needs to be done. I suggest that we have a long way to go before there's universal understanding of what I'm talking about. It has not been instinctive to include climate change or resource scarcity or resource imbalance now security's thinking. Some of these issues lie outside the security domain with wider society, particularly our elected representatives, but that doesn't excuse the security community for inaction.

They need to acknowledge the complexity and the uncertainty of the operating environment. It's something you thrive on in your operations, but there's a hesitancy as soon as you get back into barracks or HQs. You've got to think about this on the policy side: that new operating environments will be reflected in our thinking analysis. We've got to avoid the temptation to reverse engineer; the military are very good at reverse engineering, whether it's a midshipman doing his astro-navigation in his cabin after failing to get up with the morning stars, it's the fault of the equipment capability team or whatever the scenario: it's either a tank, a fast jet, or a frigate.

And the same happens with some of the analysis of the threats. We know what kit we've got, we know what doctrine we've got, we know what training comprises so we'll reverse engineer it. We need to avoid that. There's a need to draw on your experience with other threats to develop effective early warning mechanisms, indicators, and warnings to know such things as when the price of wheat is going up, the price of white rice is going up, or populations are moving. We need

to build new relationships to allow that development of mechanisms to happen. Perhaps by using think tanks like ASPI or Lowy.

Now, all of that requires an investment of time. There's a need to share knowledge with other government departments and beyond; to work with partner nations, whether it's a traditional five-eyes community or broader. I can't reinforce John Blackburn's point about the need for an energy strategy enough. There's a need to get the language right. When I took over as the Government's Climate Energy Security Envoy in the Ministry of Defence, talking about soggy targets, and greenhouse gas emissions targets, the Ministry of Defence was fighting two operations at the time. I was under pressure and under about the cosh on resources: we had to change the language of things like operational capability, risk and cost.

But, above all, this concerns leadership, not just the truth unto power piece, but senior leadership demonstrating commitment. I've no doubt that voices like Chris Barrie and the commitment of Angus Campbell, and that we're talking about this today are going some way towards broadening our understanding. But more senior voices are required with a coherent and relevant narrative, because only then will all the activities described in those 15 pages of that submission last August become a plan or a strategy. While such a plan needs to be sufficiently robust to be adopted where required, it needs, more importantly, to withstand the results of administrations changing or people moving on.

Thank you very much.

From the Non-Proliferation Treaty to the Ban Treaty

Professor Ramesh Thakur

Air Marshall Davies, ladies and gentlemen, good afternoon. I'm going to speak to you as a professor, although I will join the pensioners in two weeks' time, and as a former UN official. Looking at the title, I have a sneaking suspicion that I've been invited to speak to you as a disruptive influence.

As we've heard from just about all the speakers, world order is at a crossroads, not least because the post–1945, US-constructed and policed liberal international order is under stress. Part of that is the global nuclear order. To link it to the address from the admiral we just heard, we face only two threats in the world today: one is climate change; the other is the bomb, except the bomb can kill us a lot sooner and a lot faster. What I find interesting is that those who reject the science of climate change are derided as denialists, except of course in Canberra, where they're known as the government. Those who reject the reality of nuclear threats are praised as realists. That's only half facetious, and I want to take you through that.

In terms of the broad theme of the conference, every historical era faces its own set of challenges. Where the prevailing geopolitical equations converge with and are in harmony with the prevailing normative architecture, you will have, by and large, stability. One of the reasons, particularly in the global nuclear order, we are experiencing stress is divergence between the geopolitical equation on the one hand and the normative architecture on the other. Today, effectively, the global nuclear order is bifurcated between global treaties: the NPT, the 1968 Nuclear Non-proliferation Treaty; and the Ban Treaty, the Treaty for the Prohibition of Nuclear Weapons, adopted at the United Nations last year by 122 countries. Today, we have two global treaties for governing global nuclear order and setting nuclear policy directions.

I want to make sure you understand that I speak to you as an Australian of Indian origin, not as an Indian living in Australia. That's an important distinction in identity because when the CTBT, the Comprehensive Test Ban Treaty, was being negotiated, I got it from both groups. To the Australians, I was Indian. "You duplicitous, deceit-prone Indians, what do you think you're doing being a naysayer to a global treaty again?" The Indians said, "What do you Australians think you're doing with us? This is a matter of national security."

What happened, of course, was the proposed treaty was blocked by India in the Conference of Disarmament, and Australia, with US encouragement and support, took it from there to the United Nations General Assembly, and had it endorsed by the General Assembly. Then we all said to the Indians, "This is now a global norm, and forget about all other treaties. Forget about the fact that you were protesting against it. You are now bound by this norm." Well, guess what? We objected to the Ban Treaty being taken to the UN, didn't take part in the conference, but that global norm now has been articulated by the General Assembly. It's just a useful reminder that we need to be careful of actions today because the precedent might come back to bite us in a decade or two decades hence.

That's a very quick pictorial representation of where we stand with nuclear weapons today. It will be familiar to you. The main point of showing this, for me, is to emphasise how more than 90% of the world's stockpile of just under 15,000 nuclear warheads is actually held by Russia and the

United States, 7,000 and 6,800 respectively. If you add the other three nuclear weapons states recognised by the NPT as such, that's China, Britain, and France, between them they own 98% of the world's stockpile. That's important because, as we go through it, you will understand it depends upon whether you identify the weapons themselves as a problem or who has them as a problem, so it's worth remembering that.

In terms of shifting from the NPT to the Nuclear Weapons Prohibition Treaty, let's call it the Ban Treaty. To go back to what I was saying about at a certain level of abstraction, it's the governance arrangements for meeting the existing challenges of the day that decide whether you have stability or whether you are disrupted. Remember my point about the distinction between the normative architecture and the geopolitical equations. The NPT reflects the geopolitical dominance of the two superpowers of the time, who embedded their normative preferences into the treaty and thus caused the resulting imbalance of obligations between non-proliferation and disarmament.

Now, there are two problems today; the five nuclear weapons states are also the five permanent members, the P5, but the geopolitical reality in the outside world has gone in one direction, whereas the Security Council permanent membership is frozen in time in 1945. That increases tremendously the transaction costs of enforcement of Security Council decisions because it doesn't reflect the geopolitical balance of power anymore.

Secondly, the normative balance of power is now being asserted by the majority in the General Assembly, not the major powers. This widening disconnect between the normative balance of power and the geopolitical balance of power is a major cause of disruption, and that's across the board, and this does not excluding nuclear weapons. Bear that in mind as an explanation; as a broad structural explanation.

The NPT had a three-part bargain. Facilitate the peaceful applications of nuclear energy, including the transfer of technology and for national assistance if required, but institute safeguards to guard against the risk of diversion of peaceful materials to military purposes, in particular the bomb. This non-proliferation set of obligations was rigorous. It was immediate. It was legally binding. It was verifiable, and it was enforceable. None of these five objectives applies to the disarmament obligation in article six of the NPT, which I'll read out shortly, but the article six obligation nonetheless is there. That was the price. We had to recognise that you can't do it immediately, but you who have the bomb, and we give you the right to maintain it, and in return you promise to engage in good-faith negotiations to bring détente.

Over time, that imbalance was institutionalised by the five nuclear weapons states into a permanent position through the doctrine of deterrence. They paid lip service to disarmament, but it was only lip service. "We'll get around to it someday, sometime in the future. Meanwhile, the world is too insecure. Let's not talk about that, and let's make sure we don't make it even more insecure by curbing proliferation ambitions." This meant effectively that there was a double interpretation of the NPT by the nuclear weapons states.

Firstly, they used it to legitimise their own ongoing possession of nuclear weapons, so what was meant as a temporary legal permission to hang on to the bomb was transformed into the language of entitlements, legal rights, enduring legitimacy to keep it indefinitely. The second interpretation of the NPT was, "This is our principal management tool to enforce the non-proliferation obligations on everyone else." Since the five nuclear weapons states were the P5, that's the enforcement mechanism that was used. Effectively, the belief in, and the requirements of, nuclear deterrence trumped the language of disarmament, and the calls for disarmament were

repeated at five-yearly review conferences of the NPT through the UN system. National security takes precedence over international security.

In the Ban Treaty, you get a reversal of that relationship between deterrence and disarmament. The majority of the world's countries have said, "No, the disarmament now will take priority over deterrence, international security will take precedence over national security, and humanitarian concerns will override national security concerns." What does it ban? It bans the possession. It bans the testing. It bans stationing, which has implications for all NATO allies. It bans the use of nuclear weapons, and it bans the threat of use of nuclear weapons. For deterrence, of course, you need not just possession, but you need doctrines for use, and the threat of use. Otherwise, deterrence breaks down. You need to be able to threaten retaliation. For that, you need the infrastructure, possession, and delivery capabilities, and resiliency, to pick up a phrase from the last two presentations, and you need survivability. If the threat of use is prohibited, as it is in the Ban Treaty, it fatally undermines the doctrine of deterrence. It is simply not compatible.

These are the various elements that are banned. In terms of what the agenda will be, the next stage will be for the treaty to enter into force. It was opened for signature in September; 50 countries signed on the same day. As of now, 57 countries have signed. Five have ratified. It will enter into force 90 days after 50 countries have ratified. Given that 122 voted in favour, I think the general expectation is it will enter into force sooner rather than later. Meantime, we are into the five-yearly NPT review cycle. The next review conference will be in 2020. That will mark 50 years, five zero, since the NPT entered into force. As part of that, we have preparatory committee meetings, the second one to be held next month, and we'll have a third next year, and we may or may not have a fourth. It depends on whether we feel the need to. Meantime, there's also the UN High-Level Conference on Disarmament. That's going to be convened starting in May. Again, the two parallel tracks, reflecting these two treaties, although the High-Level Conference is not exactly under the Ban Treaty, but similar states who voted for one have voted for the other.

Why, then, this drive for the new Ban Treaty, which the nuclear weapons states insist is a threat to the NPT? Firstly, because of mounting global frustration at the failure to implement the Article 6 obligation to eliminate nuclear weapons. Fifty years after the NPT was negotiated, most countries have simply stopped believing the promise of, "Someday, we'll get around to it." Fifty years is a fairly long time. It's a fairly long rope, if you like. If you look at the agreed outcome document and action agenda from the last successful review conference—which was the 2010 one—the 2015 collapsed. We couldn't get an agreed outcome. This is a study that my centre did, and it is actually the best study, even if I may say so, in the world. If you switch to Arabic for a moment and go right to left, you'll see the peaceful users' implementation record is very good.

Nuclear non-proliferation is imprecise, but when you come to disarmament, the non-fulfilment becomes much more important than fulfilment. Remember, only the possessor countries can implement disarmament. Bear that in mind, also.

Of course, at the NPT review conference, all the state parties take part. Therefore, it reflects the most common level agreement. Even that level cannot be met on the disarmament side, in particular. If you take a more exacting standard, which is a set of recommendations by the International Commission on Nuclear Non-proliferation and Disarmament—co-chaired by our own Gareth Evans and his counterpart, Yoriko Kawaguchi, the former Japanese foreign minister—and measure progress against their recommendations, which were all made by people who had held high-level, executive decision-making positions, so this was not ICAN, let's put it that way. It

was not a bunch of activists. These were people who had had serious positions. It's much worse in terms of what is needed and what is actually being done.

Meanwhile, of course, of the five original countries that had the bomb, the number has expanded. We now have nine. Nuclear weapons have spread to other countries in more volatile, conflict-prone regions with much weaker command and control systems. So, while there are far fewer warheads today, the prospects of a nuclear war, if not by design then by accident, rogue launch, or system malfunction, have grown. This is a different way of slicing that earlier diagram. There's two or three points of interest in this one. Firstly, you notice how the numbers—global stockpiles—kept increasing even after the NPT has entered into force. It's difficult to see how that is held to be compliant with NPT, Article 6. Second, the numbers have fallen quite dramatically. The nuclear powers, particularly Russia, and the United States, make the point that they may not have been acting under the NPT, but the 75% to 80% reduction in numbers since the Cold War peak is proof of good-faith intentions to try and meet the obligations to get rid of weapons eventually, and reduce numbers quite significantly. The third feature in this, again, is how the other countries disappear. You cannot really see the lines because these two countries dominate.

Meanwhile, arms control efforts stalled, going in reverse. As of the start of last year, forget about this year, even the ABM Treaty; of course, the Americans pulled out. We allege that the Russians have been violating their INF commitments and obligations. New arms control agreements? There doesn't seem any prospect that New START will be extended beyond 2021, I think it is when it runs out and, of course, no agreements exists between other countries, either. Nuclear risks, in the meantime, climb in geopolitical tensions, volatility in Europe, volatility in the Middle East, and problems between India and Pakistan. Last year also was a tense military standoff between India and China, and the Korean Peninsula: this continues to be in the news. A general perception exists that risks were multiplying and intensifying. Meanwhile, the humanitarian movement sprang up, pointing out that the humanitarian consequences of any nuclear weapons would be catastrophic.

So, the general conclusion that, in terms of advancing the agenda, as opposed to where we have got to, the NPT perhaps is no longer fit for purpose. Many real accomplishments; many real achievements; we don't want to undermine that, but if you want to move the agenda forward, non-proliferation has been applied to every country other than those who actually have the bomb. Security issues have taken over the nuclear security summit.

Peaceful use and interest has declined quite dramatically, particularly after the Fukushima accident. With disarmament, nothing is happening. So, the normative capacity is exhausted. Rather than that, it was never there. In other words, you have two things intersecting, one, a receding global nuclear arms control tide, and the other being elevated, or perceptions of elevated, nuclear threat levels. Then along came Kim Jong-un and Donald Trump, who you can, I think, call the godfathers of the Ban Treaty in terms of how they affect people's perceptions of risks. This is a public opinion poll of just Americans. The figures would be significantly higher in terms of concern, if you did a global public opinion survey.

Incidentally, just out of curiosity, how many people in this audience are confident that President Trump would know what you were talking about if you used the words NPT? I don't see any hand coming up. Okay. You might remember that.

The famous Doomsday Clock. Of course, if you take it literally, you can rubbish it very easily. They have ranged between whatever it is, 17 minutes in 1991 at the end of the Cold War, to two

minutes, the closest it's been. That was 1953 and now again today. Clearly, for all these years, we haven't had a nuclear war, but that's less important than the fact that it's a metaphor. It is an eminent group of scientists and others who make the judgement, and the judgement is that we are in one of the most dangerous periods the world has experienced, as dangerous as it was at the start of the hydrogen bomb era in 1953. That judgement is what is important, not the literal two minutes to midnight there. That gives you, as I said, the changes in the clock.

The other motivating factor behind the Ban Treaty is a belief in the symbiotic link between non-proliferation and disarmament as both a logical truth and an empirical truth. If nuclear weapons did not exist, they could not proliferate. Because they do exist, they will proliferate. In other words, the very existence of nuclear weapons is a sufficient guarantee of their proliferation. Conversely, nuclear disarmament is a necessary condition of nuclear non-proliferation. So, our choice boils down to if we actually want non-proliferation, and if we want to protect and preserve the gains of that, then we have to prepare actively for disarmament. Or if we fail on disarmament, we must be prepared for a proliferation cascade and ultimately nuclear weapons use again, someday, somewhere, by someone.

This was expressed in the language of security by our own Canberra Commission in the 1990s. "As long as any country has nuclear weapons, others will want them. As long as nuclear weapons exist, they will be used again someday, if not by design, then inadvertently, through accident, rogue launch, or system error. Any use of nuclear weapons could be catastrophic for the whole world."

The Ban Treaty updated this terminology to 'humanity' includes three propositions: "No country individually, nor the international system collectively, has the capacity to cope with the humanitarian impacts of a nuclear weapon"; " It is in the interests of the very survival of humanity that nuclear weapons are never used again under any circumstances". I put under any circumstances in colour because that's the phrase that caused us the biggest problem in Australia, because you have to be able to contemplate its use under some circumstances, otherwise deterrence is not possible. Then the third one: "The only guarantee of non-use is the total, irreversible, and verifiable elimination of nuclear weapons." In other words, the collective interest of the international community in disarmament overrides the individual interest of the possessor states in national security that puts the world's very survival at risk.

What the majority of the world is demanding is that the very possibility of nuclear war must be eliminated by de-legitimizing and eliminating the possession of nuclear weapons and the doctrines of nuclear deterrence today. The collective moral revulsion of the international community is embedded in this treaty as a normative treaty. That is its primary intended impact. They're trying to shape or reshape the global normative context, the prevailing cluster of laws, international humanitarian human rights norms, principles, practises, and discourse, that shape how we think about and how we act in relation to nuclear weapons, so that particularly as the number of ratifying countries crosses 100, there will be a deepening crisis of legitimacy.

Having said that, let's remember there are certain terms that are shared between the NPT and the Ban Treaty, non-proliferation, no testing, even non-use. All sides want to avoid having to use nuclear weapons, avoid a nuclear war, but where we part company is in the threat of use, and therefore in deterrence, and therefore also, from the other side, in the importance of near-term, practical actions to launch disarmament. There is also a worry about the softening boundary between conventional and nuclear weapons.

In terms of the problem, the NPT itself and much more forcefully and strongly, the Ban Treaty, identifies the bomb itself as a problem, but for many countries, including the USA—including us in *de facto* terms—the problem is not the bomb but who has it. That's the applied reinterpretation of the NPT. There should be only one article six there, not six sixes! It calls for each of the parties to undertake effective measures, at an early date, for nuclear arms control and disarmament. This was strengthened by the World Court's Advisory Opinion in 1996 with three relevant important points, that any use of nuclear weapons would generally be contrary to international law, in particular, humanitarian law, that they could not pronounce definitively that the use of nuclear weapons would be legal even if the very survival of a state was under threat, and that states, because of that early-date promise, had the obligation not just to pursue, but to bring to a conclusion, efforts at nuclear disarmament.

The problem with deterrence ... there are several, and I'll just speed through them so I can finish on time. First, the historical record is very ambiguous on the utility of deterrence. The peace in Europe, was it a result of the threat of nuclear weapons? Was it the democratisation of Western Europe? Was it the integration of Europe? Certainly, there is no evidence that any side contemplated the act of aggression but was deterred from doing so by the knowledge that the other side had nuclear weapons, not in Europe nor anywhere else. We do have contrary examples. Argentina invaded the Falkland Islands. No one doubted that the U.K. had nuclear weapons. The USA, the Soviet Union as it was, have suffered defeats on the battlefield, and accepted defeat on the battlefield, rather than escalate to nuclear weapons.

There is marginal and questionable value in deterrence. It has limited utility. It's not that it doesn't have any utility, but in the context of the modern world and the threats we face, they are marginal and questionable, but the risks, and threats, and dangers are much more substantial. That, of course, is the changing balance argument that Kissinger, and Shultz, and Perry, and Nunn used to call for efforts to abolish nuclear weapons after the end of the Cold War.

Of course, if you accept that deterrence works, then it's an equally dangerous proposition. If we really believe that deterrence is important and useful and works, why are we not encouraging Iran to get nuclear weapons, so that we will have peace in the Middle East? Why should only one country have them? If deterrence works and underpins stability, why do we censure and sanction Pakistan and India? The more violent and conflict-prone the region, the more we should be facilitating and calling for countries in the region to get the bomb, so that then we can have guaranteed peace. Now, Bilahari is one of the few people who accepts the logic of that, but most of us are horrified at the thought, and I think with good reason, because the mathematical probability of an unintended nuclear war grows exponentially with each additional entrant into the exclusive nuclear club. That's why we try to do away with it.

So, conclusions. The collective revulsion of the international community against the bomb found a double expression, originally in the NPT, in both non-proliferation and disarmament obligations, and now in the Ban Treaty, which focuses just on the disarmament side. It reaffirms non-proliferation, but it extends that. As I said earlier, the temporary exemption for the nuclear weapons states was converted. It implied a conditional acceptance of deterrence, but with changing perceptions of risks, we now want to reemphasize and elevate disarmament over deterrence, because the latter is held to be unacceptable. Therefore, deterrence itself becomes a problem, and disarmament is a solution.

I think the Ban Treaty proponents accept that they can't get rid of nuclear weapons because they don't have them, but they also point out, by the way, that, to date, not a single warhead has been eliminated under the NPT. Only the possessor states can cap, then reduce, and, in the longer term, eliminate under a verifiable, enforceable nuclear weapons convention, after all the technical requirements for verification have been sorted out. What the non-possessor states can do, and what they have tried to do through the Ban Treaty is to stigmatise, and to take away the legitimising prop, to de-legitimize the possession of nuclear weapons and the accompanying doctrines of deterrence based on the threat of use.

The Nuclear Posture Review, and I'll finish with that, makes only one reference to the Ban Treaty, and that is to say that it injects disarmament into a non-proliferation regime. In other words, the Nuclear Posture Review of the United States, issued last month, pretends that article six of the NPT doesn't exist. To the majority of the world's states, and all 122 states that voted for the Ban Treaty are members in good standing of the NPT, to the majority of them; the Ban Treaty represents the completion of the NPT agenda. That tension between the two is going to be the most important issue in nuclear policy over the next two to three years. The two treaties have somehow to be harmonised, otherwise that disruption is going to magnify and amplify.

Thank you very much.

The Future of Security in Space

Mr Todd Harrison

All right! Well, good afternoon everyone. I am mindful of being the first speaker after lunch—that I've got to make sure to keep your attention! Also, mindful that my biological clock is telling me it's 10:30 at night right now, so bear with me. And I want to thank you Air Marshal Davies, Air Commodore Edgeley, Auntie Tina and Uncle Harry for the opportunity to speak here at this forum and to share this stage with so many other distinguished speakers today. And I'm excited to talk about this timely and important topic of the future of security in space.

Now to understand the future of security in space we first need to understand a bit of our past, how we got to where we are today. For almost as long as humans have been able to place objects into earth orbit, space has been a contested domain. It's easy to forget that the United States tested the first anti-satellite weapon in 1959. That was just two years after the launch of Sputnik. And throughout the Cold War, both the United States and the Soviet Union developed and tested a variety of anti-satellite weapons. Now thankfully none of these were used in anger, but the threat was ever-present. So sometimes I'm taken aback when I hear people say that what's different is that space is now a contested domain, because it's always been contested.

Now what has changed in space that's causing people to become so concerned? Well you've heard about the three Cs – congested, competitive and contested – and I'm hopeful that when you leave here today you'll also remember the four Ds – diverse, disruptive, disordered and dangerous. Now I would argue that the first two – diverse and disruptive – are positive developments but the last two are a bit concerning.

Space has become more diverse because more countries are launching satellites than ever before. You know, during the Cold War, it was mostly the United States and the Soviet Union. Over 90% of the launches from 1957 to 1991 were from either the USA or the Soviets. But today, there's a wide variety of nations launching and operating satellites. It's become much more diverse and we see a lot more commercial forms that are getting into the space business. Also, during the Cold War, satellites that were on orbit were primarily government and primarily military. But today, the majority of satellites going up are commercial.

Space has also become more disruptive because many of these new commercial space firms are bringing all sorts of new ideas and new applications for space, things like robotic on-orbit servicing and geostationary orbit and on-orbit mining and manufacturing. It's an exciting time and it may fundamentally change the way we use space and operate in space, both commercially and militarily.

But at the same time, these forces are making space more disordered than ever before. Our laws, regulations and treaties weren't designed for many of these new space missions and many of our nations are struggling to keep up. A good example of the disorder I'm talking about here occurred just recently with the controversy a small space start-up company in the US created when it was prevented by the US Federal Communications Commission from launching a set of four experimental satellites; but it went ahead, and it launched them anyway on an Indian rocket.

And as space has become more diverse, disruptive and disordered, it has also become more dangerous. And I say this for two reasons; I'll go into them in a bit more detail. First, the way we use space systems has changed.

Throughout the Cold War, US and National Security Space Systems were protected by the cloak of nuclear deterrence because these systems were primarily used to support nuclear forces. We had an understanding with the Soviets that we would not interfere with either country's national technical means because, doing so, would have been perceived as a prelude to a nuclear attack.

But today our National Security Space Systems are used across the full spectrum of conflict, from counterterrorism operations to high-end combat against a near-peer adversary, all the way up to nuclear deterrence. And I should note that only at an Air Power conference can I get away with putting a slide up here that depicts the full spectrum of conflict using only airborne platforms. So please don't tell any land power advocates that I'm doing this.

But the United States, Australia and our allies in Europe and the Asia-Pacific region have integrated advanced space systems into military operations in increasingly sophisticated ways. Space systems give our militaries global reach, power and influence, and to be sure, potential adversaries have taken notice of this. Our dependence on space makes these systems a natural target for adversaries to exploit. They are developing counter-space systems designed to thwart our advantages in space.

And as you can see, they aren't doing it secretly either. I'm particularly amused with the Russian A-60 airborne laser platform because—note the little blow-up here on the slide—you can see the insignia they put on the side of the plane. So just in case you thought that, you know, maybe it's not used for counter-space missions, no, they made it abundantly clear for us. They've got a picture of a falcon there with a lightening bolt going up and it looks like, you know, a space telescope, something like the Hubble Space Telescope, I don't know. And the lightning bolt is going right into the aperture of that system. So, they're making it very plain, very clear, that they are building systems to target our space systems and to negate some of the advantage that we gain because of them.

Also, as you can see, it's not just the kinetic ASAT weapons. There is the Chinese DN-3 direct descent ASAT missile you see on the lower right-hand side. But it's also all sorts of other non-kinetic means of attack, including things like these truck-mounted GPS and SATCOM jammers that Russia has fielded, and reports indicate that they've provided them to North Korea. And more recently, we've seen Russian jamming equipment show up in places like Syria and the Ukraine. These things are being used all the time.

And the intent here is to leave our forces blind and deaf in the event of a conflict. Space is simultaneously a powerful enabler and a serious vulnerability. Put simply, the United States, Australia and other allied nations are increasingly dependent on space across the full spectrum of conflict, but our space systems are not adequately protected across the full spectrum of threats.

Conflict that begins or extends into space, particularly if it becomes kinetic, will not end well for anyone. Our primary focus should therefore be on deterring conflict in space. And I believe there are three main areas where we can do more to improve our deterrence posture in space. So first of all, we need a clear understanding and articulation of the thresholds for escalation in space, not just our own thresholds but those of our allies, our partners and our adversaries, and an understanding how all these other actors perceive our thresholds.

Now back in in 2016, my think tank, CSIS, partnered with another think tank in DC called the Secure World Foundation and together we conducted a space crisis simulation to explore some of these topics. And one of our findings from this exercise was that escalation thresholds for conflicts in space can be ambiguous, particularly at the lower end of the spectrum of conflict.

Now, as in other domains, thresholds are context dependent. The way an attack is perceived depends on the context in which it occurs. And each side can have different views of their own thresholds and their perceptions, or misperceptions, of the other side's thresholds. What's difference about the space domain is that we don't have much history to draw upon, or widely accepted norms of behaviour. You know in the maritime domain, if someone fires shots across the bow of your ship, you understand what that means. You understand that it's a warning. And there are rules of the road. There are ways that you operate in shipping lanes.

Now I've heard it said before that speed limits don't stop people from speeding; they just allow you to identify who the speeders are. Similarly, norms of behaviour in space will not stop the bad actors but it will allow the good actors to quickly identify rogue behaviour.

Another complicating factor is that adversaries can use forms of attack against our space systems that are sometimes difficult to detect, attribute and deter. Some kinds of attack such as jamming are temporary in nature while other methods of attack, such as using a laser to blind the satellite sensors, may not be readily visible. So, these attacks can happen and no one else may even realise that anything has happened. Moreover, if you're the operator of a satellite that's being dazzled or blinded, do you really want to acknowledge what just happened and give your adversary that battle damage assessment, to know if what they were intending to do was actually working or not?

Now, many methods of non-kinetic attack against space systems, including cyber attacks against ground stations, can be difficult to attribute in a timely manner. It's nearly impossible to deter an attack if you can't attribute its source or know with confidence that the effects being experienced are malicious. Improvements in our ability to detect and attribute the full range of threats to our space systems, not only enhances deterrence, it also provides an asymmetric advantage and it gives us a powerful tool to control escalation on our own terms.

But if escalation thresholds are left ambiguous, it can invite grey zone aggression in space. Now we're already seeing grey zone aggression in other domains today, where adversaries are probing at the seams trying to find ways to create problems for us or advance their own ambitions, but without triggering direct conflict. The same thing can happen in space. We need to be prepared for that.

The second area where we should be focussing more effort is enhancing and augmenting space capabilities with our allies and commercial partners. We are all in this together. It is a joint international force in space; we depend on one another.

As I mentioned before, we're in the midst of a renaissance of commercial space and many commercial firms are making advances to do things that used to be the exclusive domain of government. That makes a lot of people uncomfortable, particularly in our intelligence communities. The surface of the earth and the space environment are becoming more transparent, whether we like it or not.

This is not something we can stop. Now, on balance, I believe this is a positive development for those of us who believe in a rules-based global order because it makes it more difficult for rogue

actors to operate in secrecy. They know we can see what they're doing. I think that's a positive thing.

But the challenge here for our militaries is to stay attuned to the advances in commercial space – and it is commercial space that are driving many of these capabilities that make earth and space more transparent – to stay attuned to these advances and to keep pace with the speed at which innovation is occurring.

Now in the US Military, we have a system called the Planning, Programming and Budgeting and Execution System (PPBE). If you are familiar with or if you've worked with the US Government, that's the system that we use internally within DOD to develop our annual budget request and then, once it goes to congress, there are the authorisation and appropriation processes that they use to provide funding and oversight. These processes are simply too slow, even when they work as intended, as often they don't.

This year is a great example. We are almost halfway through our fiscal year and we still do not have appropriations passed by congress. But even when they work as intended, it takes about two years from the time you have an idea for a new program or a new initiative to when you have money that you can put on a contract to start work on that idea. Any of you who work in the acquisition environment know that when you're putting money on a contract, that's just the very beginning. That's just when you're starting work. And it takes us two years just to get to that starting point.

In that time, the commercial space industry will have already progressed to a new generation of technology, maybe two generations, not to mention how long it then takes us once we start a program to go all the way through the acquisition process and ultimately field a new capability: a new weapon system of some kind.

That's one of the reasons that we are launching, we are continuing to launch, wideband global SATCOM, satellites: our wideband systems that provide about three gigabits of data throughput per satellite. That program … I remember when it started back in the early 2000s. We're still building and launching those satellites today 'cause that's how our acquisition process works. The commercial satellite communications industry has gone through multiple cycles of development and technology. And now, VITASAT, one of the commercial companies, is launching satellites where they're using various types of technology to achieve 300 gigabits per second of data throughput per satellite, literally a factor of 100 by which they are improving their data throughput.

Now in addition to all these things, the window of opportunity for some things, like hosting a military payload on a commercial satellite, may last only a few months. If it takes us two years just to get the funding to go forward with an initiative, the window of opportunity will have closed. Innovation is not just about having great ideas and new technologies. It's also about being prepared to take advantage of opportunities when they materialise.

Now a third and final area I believe needs more attention is the problem of communicating thresholds and capabilities. Communication is a critical part of deterrents and our ability to manage escalation in a crisis. We must be mindful that, as space is becoming more transparent, some of the capabilities and operations that we used to be able to keep secret in the past may not be secret any longer.

And I know that's hard for many folks who work in our space operations community to come to grips with. But we can't keep pretending that people can't see things we know they can see. Even with commercial technology, they can see what we're doing.

Secrecy invites suspicion among our allies and partners and does little to deter our adversaries. Put simply, an adversary cannot be deterred by something it does not know exists. While certain aspects of our National Security Space Systems must remain secret to be effective, too often the United States and its allies default to over-classification.

It was an encouraging first step when DOD declassified the existence of the Geosynchronous Space Situational Awareness Program (GSSAP) back in 2014. I believe that this disclosure enhances our security and helps deter aggression in space because the whole world is now on notice that we're watching what others are doing in geosynchronous orbit. We can see you.

I would like to see us go a step further to name and shame bad actors in space, those who conduct irresponsible, aggressive or hostile activities, and back it up with hard data. I'd love to have a picture one day to put on a slide up here that shows you some of these objects that we're tracking in space. You know, something that Russia launches, doesn't declare it, it gets catalogued as a piece of debris. A few weeks, few months go by and then we see the piece of debris manoeuvring. Kind of funny that debris can manoeuvre like that! I'd like to see a picture of that on the front of *The New York Times*. I think that would be appropriate.

The over-classification of information also inhibits our ability to work with international partners and commercial firms, both of which can play an important role in improving the resilience of our space systems. Classification issues can make it difficult to discuss escalation thresholds with other nations, even some of our closest treaty allies, like Australia. Now lowering classification levels where appropriate would ease the integration of more allies and partners into our space operations. We build up so many different levels and so many different firewalls within our space operations that sometimes, even within the United States, we have problems with one organisation sharing information with another organisation and we're all supposed to be on the same team.

Similarly, over-classification makes it difficult to work with many commercial firms, especially those that are new to doing business with the government and may not have any cleared personnel within their organisations. As someone who's worked at a small space start-up before, I can tell you that that is a big barrier to entry and a disincentive to doing work with the government.

Also, sometimes the licencing process gets hung up for licencing purely commercial space missions because someone, somewhere in our interagency community will flag something and say, "Ah ha, that's a security issue." And then they can't even talk to the company about what it is and why they're flagging it. And you know, it could be that it's something that's very easy to clear up.

To improve communication of thresholds is to be more explicit with commercial satellite service providers about how attacks on their systems will be treated. The new US National Security Strategy that was released back in December of 2017 says that the United States will "consider extending national security protections to our private sector partners as needed".

Now, that's a step in the right direction but more clarity is needed. What kind of protection will be provided, financial or otherwise, and under what conditions will these protections be triggered?

One of the things that's been discussed that I think the US and other countries need to look at is: do we need to provide some sort of an indemnification program for commercial space companies when they do business with the government, because in the event of a conflict, they very well may be targeted? And looking at it from a business perspective, that's a risk they're not going to be able to insure. Insurance companies don't like to underwrite acts of war. So, we need to think about this in advance because when you get into a crisis and businesses are being put at risk, capital is being put at risk, you don't want to be scrambling at that time to figure out how we're going to reassure our commercial partners who are an important part of our space architecture.

The US Military already depends on commercial operators for satellite communications, imagery and many other capabilities. An adversary may seek to attack these commercial systems simply as a way of signalling intent or resolve, believing that their actions are below the threshold for military conflict. I think that would be a big miscalculation on their part, but without clarity of how such attacks would be treated, commercial space operators may not be willing to accept the risk of doing business with the military in the event of a crisis. We need to think about this carefully and ensure that doesn't happen.

So, in conclusion, much remains to be done to improve our deterrence posture in space for the wide range of threats we face today. I believe these efforts should focus on the three areas I've outlined here: clarifying escalation thresholds in space; enhancing and augmenting space capabilities and the speed at which we innovate; and improving how we communicate thresholds and capabilities to others.

If you would like to learn more about the thoughts that I've shared here and learn more about the space crisis simulation that I mentioned, you can download a copy of our latest report, *Escalation and Deterrence in the Second Space Age*, at our website here. And in the appendix you can find the methodology and all the scenarios that we used for the space crisis simulation. So, you can look those over and feel free to use them in your own work.

And, of course, if you have any questions, I'd be happy to address them later in the conference or at the Speakers' Corner or the lobby after this event, and I thank you all for all your time and attention to this important topic. Thank you.

Uninhabited Aerial Systems

Dr Thomas X Hammes

Good afternoon, it's good to be back in Australia. Air Marshal Davies and the team, I'd like to thank you very much for inviting me to this and giving me the opportunity to speak.

I think maybe the staff pushed past disruptive when they invited a marine infantryman who studies history, to talk about technology for the Air Force. We may have gone right past disruption and irrationality. We'll see if I can do better than that.

Now, one of the things … Americans don't know much about Australia, so I thought it'd be a good idea to show you one of the views we have. I don't think this is what your tourism industry wants, but that's the view. I'm a little concerned that by the end of this talk, the pilots in the audience will think this is a pretty good idea.

Now, a disclaimer: I am still working for the US Government, but nothing that I say is; it's all my opinion. DoD does not necessarily agree with me, and nor does the National Defence University. So, the topic I was given was Uninhabited Aerial Systems: Disruption or Prescription? I would say a little differently. They're both autonomous, will be unmanned, they will be autonomous, and they are inevitable. And my fundamental thesis is that within two decades, they will dominate the air domain. And we have to think about how we're going to make that transition, and they're going to dominate because of superior range, vastly superior numbers, lower cost, and the fact they will not need fixed bases, like our current family of manned aircraft do.

So, what are the things that are going to make this happen? This is in the short-term … again, the next 10 to 15 years, all of these things are here. Now, some of them exist now, and I'll talk you through them in turn, and why this will change the dynamics between manned and unmanned aircraft.

The first is the fact of small warheads. Now, you see that little plastic cylinder about the size of the explosive tech's hand? That is an explosively formed projectile. It has 30 grams of explosives. For the Americans in the room, that's 0.07 pounds. And it has a tiny little copper penetrator in a plastic tube. So, for about 70 grams, I can devise a weapon that will punch through a half-inch of steel. Obviously enough to destroy an aircraft on the ground, to destroy most wheeled vehicles by going into the engine compartment, getting it a mobility kill. Now, what's going to make this really interesting, is nano-energetics, which is the US Navy's polite way of saying explosives. Already, in the unclassified realm, they show as having 10 times the power of TNT for the same weight and mass. So, as you begin to experiment with this, you begin to look at the thought of "well, maybe, a Tomahawk land attack missile with a 1000-pound warhead really comes out equivalent more to an eight to ten-thousand-pound warhead, if you change the explosive load". And, what does that mean for delivery systems and potential?

The next thing is 3D printing, and this gives you capability plus volume. If you look at this picture here, the gentleman there is a researcher at the University of Virginia, and the Marine Corps asked him if he would build a small drone force, 3D-printed drone, that could hunt autonomously. It took him about a year, but what they developed is this drone you see here. He 3D printed the body, and it snaps together. The little electric motor, he bought online. There are two batteries he bought online, and one of the grad students had to give up his cell phone.

Now, this has a 50-kilometre range, autonomous; he only flew it out 25, and 25 back, because the kid wanted his cell phone back. Total cost: $800. This is an autonomous system which can hunt out to 50 kilometres. To put it in comparison, the Javelin anti-tank system, which hunts out to two kilometres, costs $195,000 for the round; that does not include the launcher.

Now, the bottom picture is of 3D printers. Since this was printed in 2014, when it took him a little over 26 hours to 27 hours to print, and a couple of hours to assemble, printer speeds have increased between 100 and 200 times with carbon 3D printing. That is a fact today. He's pushing it and he thinks he can get it to 1,000 times faster. So, the one printer that printed one of those in a day can now print 100 to 200. So, if you look at what UPS … and they're getting into the printing business, because they think printing is going to gut shipping pretty badly … UPS is putting up a plant today, that has 100 printers in it. If you had carbon 3D printers, that's 10,000 autonomous drones a day out of a single plant. Of course, if you reach the 1,000 printers, they plan to put in that plant, that's 100,000 drones a day. That's the kind of numbers we may have to deal with.

Is it possible to launch that many? Well, obviously if you've got that many, it's nice, but if you can't get them out, it's really irrelevant. But what we've seen … in the corner there, in the tubes there at the top, is the US Navy's LOCUST system, and that launches a larger drone like the one you saw, and these are totally coordinating drones, so they're somewhat larger, somewhat more complex. But what this illustrates, is that that container, which kind of looks like a 20-foot container, can fire about 30 drones. In the lower corner, you'll see the Chinese Harpy system. That's an 18-round launcher. The Harpy is a fully autonomous system. It picks out and can fly 600 miles, deliver 50 pounds of warhead, and it hunts in both IR visual and electromagnetic spectrums. It was initially designed as an anti-missile system, to take out anti-air systems. It goes after radars, but they've changed it into hunting in other systems.

So, you can mass launch them. Now, the next thing that's going to happen is AI, and this is not complex AI. This is AI that does task-specific things, like fly to a certain grid, look for this collection of targets; this is a priority if you find one, suicide into it. Now, the DX-3 is a Canadian system that's designed for exploring the high north for exploitation of materials and minerals. It has a range of 900 miles. It costs about $200,000. That sounds expensive. It's about the same as operating an F-35 for three hours. The one in the lower corner is the Flexrotor. It has an operating time of 45 hours, multispectral imagery, and a range of 2,000 miles. Lower left corner is the Turn. This is a Navy experimental. It's a much bigger platform; it's a 30-foot wingspan on that. Vertical take-off and landing off any platform at sea; delivers 500 pounds, 900 miles. In the upper corner is the Kratos QX-222. Kratos has been making drones for the United States for a lot of years, and they finally said, "Why don't we apply this?" They've flown a successful version UTAP-22 as part of a swarm, with a Harrier controlling three of these down range. This was planned to be an autonomous system that will deliver 500 pounds, two small-diameter bombs, a distance of 1,500 miles. It has stealth configuration, but not stealth coatings. So, it comes in pretty cheap. They say if you will buy 100, they'll sell them to you for $2M a copy. Let's say it's a normal DoD project, and the price goes up 50%, then they're still only $3M a copy. That is cheap enough to send on a one-way trip of 3,000 miles, at which point it kicks out whatever missiles or bombs it's carrying, and then they hunt. But again, this is task-specific AI. I'm not asking you to do hard things; I'm asking you to do specific things.

Now, what the heck? How could you use a weapon that goes out 3,000 miles? Well, you've got to see what you're doing, and this is cheap space. In the upper corner there, is the Rocket Lab

CEO. This is the guy that has created the new space power of New Zealand. They launched this bird, they got it up, and it actually worked. They had a little bit of a problem, but they planned to do it quarterly launches, and then down to monthly launches. And what they launched is the CubeSat; you see there in the lower picture? It's four inches on a side, and you think that's not very impressive, but over the years, they figured out a way to marry several of these together, and they can give you imagery down to two metre resolution. A slightly larger version called a KegSat, because it's about the size of dorm room keg … and that's where it was designed … will give you resolution down to one third of a metre.

Lower corner there is of course the Indian launch that put 104 satellites up in one launch, 88 of those satellites belong to a company called Planet in the United States. Their business model is for selling an image of anywhere on the planet, taken every 24 hours, with interpretation. Bottom line is, they will know where your bases are. They will know where your ships are. Within four years, this company plans to do that every six hours, and it has a business model that's attracting the money to do it.

So, now you've got this problem of cheap drones, plus cheap cruise missiles … because 3D printing advanced manufacturing will also reduce the price of cruise missiles … and you can start to think differently, which the Russians are doing. This is their family of weapons they sell in 20-foot containers, for the specific reason it's hard to pre-empt 20-foot containers because there's so many of them. Look out in any aerial imagery of any city or base area, and you'll see dozens of these things out there. They have the entire Kalibr series of missiles. Now, admittedly, it didn't have a great record flying out of the Caspian Sea into Syria. They had a failure rate of 10-15%, but if you're launching enough of them it doesn't really matter, and if you have complete surprise launch, your time from detection to launch is less than ten minutes. You won't know this is a missile system until the lid starts to come up. Their land attack version can go 1,500 miles, so your air bases simply aren't safe. They can be either hauled around by a truck, or like in the lower left corner, it can be done by one of these ships, or if you think very differently, China has 200,000 oceangoing fishing vessels. Almost any of them can handle a 20-foot container. Many of them have 20-foot containers. So, this is a threat. This is the convergence of technology that brings together massive numbers of cheap autonomous weapons.

Now, one of the things we're counting on to protect ourselves against this, of course, is directed energy weapons, laser and microwave, specifically. Now, the good news is that laser and microwaves both provide an advantage to land-based systems … defensive systems … because they can plug into a power grid that allows them to have a great deal more power generation, a lot more shots. If you have to take your laser airborne or out to sea, you've got a power limitation. We're working to overcome that, and we may be able to get there.

The other huge advantage of a land-based laser, of course, is concealment. It's very hard to see systems in the background clutter of a city. And if they're a mobile system, like many of them are, and the US Army is developing mobile systems, you can literally put them in a parking garage. You can put them in a bus garage; you can hide them underground, until minutes before you need them, and then you roll them out, establish them, and shoot. Of course, the key weaknesses of lasers are smoke, haze, and there's been some unclassified writing on possible reflective coating.

I don't know, you'd have to go deep into classified, I think, to find out about that. But smoke and haze, we do know has an affect; certain weather effects, and we're working to overcome those,

but it's really tough to base the idea that you will survive on a fair-weather system. That should concern you.

Microwave weapons, back in the Cold War, we used Faraday cages, which are simply a metal cages around your electronics to route the power pulse around it. It was to defeat the EMP pulse that comes out when a nuclear blast is set off. Well, as long as you're 3D printing the electronics on a drone, and we are doing that today, why not print a Faraday cage around it? It doesn't absolutely protect it from electromagnetic weapons, but it does increase the number you need and the ranges they have to operate at. And, of course, if you use ground avoidance, and we have ground avoidance already in cheap drones, then you can pick a route that minimises line of sight kind of defence. If you look at something like the airbase at Bagram, and you study it through Google Maps, you will see that the closest Afghan village, where Afghans live today, is 1000 metres from where we park the C-17s and the rotating 747s and other civilian birds that rotate our troops. It would seem to be a fairly easy problem for a minor drone to get out there, and, even if all you bring is a bag of gas and drop it on the wing and ignite it, I guarantee the Airforce is going to think twice about putting more C-17s there. They're simply too valuable an asset to risk that way.

So, where does that mean we are? Well, there's a historical pattern to this, and the problem is that a system will get replaced over a period of time; it doesn't happen instantly. And, normally the problem is, as new technology is developed, or a new concept is developed and somebody figures out a way to integrate this with the old system in an operational concept, that makes it an assistant; as that technology improves, you improve the operational concept, the training, the education, and you begin to use this as a partner, and then finally, it's a replacement. Now, a perfect example of that is the carrier aircraft. As you look at aircraft first coming into use, the Navy looks at them and says, "You know, not very good, but hey, they can look over the horizon, they can be an assistant that the battleship needs to see over the horizon". So, they start to do that. As the aircraft gets better and more powerful, they move to an aircraft carrier, and one of the reasons, of course, if you catapult it off a battleship, you've got to stop and pick up the pilots. They're kind of whiny about that. And, so you've got to go back and get them. That's bad for a battleship. So, you have them land on a carrier. Well, then, as the carrier aircraft improves, and you develop fighters, dive bombers, and torpedo bombers, you find it becomes a full partner. In 1936, the US Navy ran an experiment of a surprise carrier raid on Pearl Harbour and sunk our battleships in the game. The umpires disallowed it. Then, the Japanese ran a similar simulation a few years later, and it was not disallowed.

So, by 1942, the carrier has replaced the battleship, and so there's this transition from assistant to partner to replacement. And this goes back through a number of things. You think about the pikeman versus the armoured knight. If the armoured knight can get close enough, he could easily kill the pikeman. The thing to remember is the new system rarely has better capability than the old system. The advantage that it has is range.

So, this requires aggressive, honest experimentation, and by honest, you've really got to keep people from resetting a clock. Like I said, the US decided "we'll just disallow sinking the battleships, and that'll solve it". The Japanese did the same thing before Pearl Harbour, when their experiment showed that the US surprised their carriers and sunk three of four.

So, they reset the game, re-ran it, and then, of course, it won the way it was supposed to, which is their battleships caught our carriers and sunk them. Then, we ran the real battle, and we sunk four of their carriers. So, we've got to avoid that.

Inertia and unions are your other big problems. Unions in the US, and I think a great example of that is that we built this X-47 drone that is flown off carriers. It has an enormous capability and range, but, in the fight over what it should do, the pilots' union in the United States have relegated it purely to refuelling because nobody wants to do that job. So, rather than looking at how it could take over the deep attack mission, for which we don't have a suitable aircraft, or other mission, they were relegated; and this is a part of inertia in which militaries are inherently conservative, for good reason, because you have enormous risk when you introduce something new, but there's a huge amount of inertia that comes with that.

So, where are we in the air domain, in this assistant/partner/replacement? Well, if you look all the way at the bottom at assistant, in electromagnetic warfare, we're starting to put up some drones that have EW systems on them. Same thing with ASW; we're starting to fly drones off of … or have been flying drones a long time off … the old DASH helicopter, which didn't work very well, but we've improved it. And then communications relay, in partner … in Deep Strike, the Tomahawk missile is very much a full partner. A lot of times it's just to open a path for the fighter aircraft to go downtown. Naval anti-surface, the same thing … missiles are beginning to replace aircraft, and anti-airwarfare … we're beginning, like I said, the UTAP experiment with the Harrier and the range, they found that actually works. Because the UTAP doesn't have to have a lot of brains, it just has to get the missile to the right place to release it, so it can pick up and go after the target, and provide close air support. And, we're already a full replacement … in persistent surveillance in a low-threat environment drones have completely taken over from manned aircraft. There is some still use of P3s, but, if you've got a drone, it's just frankly cheaper.

And then high-risk strike; ever since the First Gulf War, we have been sending cruise missiles downrange, to places where we don't want to take the risk of losing a pilot, because you get them in an awful situation like we had in Lebanon, where we had to negotiate for the return of our pilots.

So, the immediate issue is range obsolescence, and this pattern, if you look at the armoured knight versus either the pike formation, when the Swiss pikemen beat the French armoured knights, or the crossbows and longbows which the French took three times to figure out what was happening to them … pike formation versus musket formation, again, it was not that the pikes were less effective; it was that the muskets could kill them before they could get close enough to use the pike. Same with battleship versus carriers. And the key things to remember, is it's still superior. The battleship today could deliver more firepower in less time, than a carrier. It is also much, much physically tougher than a carrier; much harder to sink a battleship than a carrier. But it's totally irrelevant, because it can't get close enough to the carrier to make a difference. And there's a market cost advantage. When we first started sending aircraft after battleships, the F6F, the frontline fighter of the US Navy in 1945, cost $35,000. So, you could buy lots and lots of them. This was the small, smart and many of the era. And they could throw against the battleships with the market advantage.

So, what does that mean for us today? Well, this is the problem. This is a range chart, in nautical miles, of the various drone ballistic missile and cruise missile systems that are flying today against the F-35. The fundamental problem is that, even with conformal tanks, like on the F-16 and F-18, you don't get a massive increase in range. But we do know that drones are increasing rapidly … like I said, a few years ago, we were getting 100 miles out of a drone; today they're getting 2,000 miles out of a drone. And relatively cheap drones. So, this is going to be a problem. The

other thing is, one of the objections to AI is the possibility to jam, and this is why you've got to go fully autonomous, non-GPS dependent. Non-GPS dependent goes back to the old TLAM in the 1990s. Initially it was inertial nav, plus visual … there was no external signal. You launched it; it went silent and went in and hunted its target. That is now much cheaper, because think about how much computer power cost in 1990 as opposed to today, and imagery capability as opposed to today. The other big reason this is happening fast is Amazon wants it. Amazon has a requirement out for a drone that will lift 20 pounds, 100 miles, GPS independent, and hardened against radiation, because they want to be able to fly it in their airfields. They don't want to get hit by a radar and shut down and lose their package. It also must be cheap enough that, if they lose the thing, they don't carry that much. That is going to make it commercially available. A lot of this stuff comes from commercial systems, and that's where the great advances will be, both in range and capability, and ability to hunt.

So, the fundamental problem is how do I get the F-35 close enough to the fight that I'm not destroyed on the ground? Because frankly, if I'm an enemy planner, I have no intention of fighting the F-35 in the air. From everything I've read and the pilots I've talked to, it's going to be a great system. We've got bugs to work out, we'll throw enough money at it, we will work those bugs out. So, why bother to hunt in the air, when I can hunt it on the ground? The Centre for New American Security did a study they call, First Strike … and if you look it up, you've got to get the two-author version; both Schugart and Gonzalez … because they released it; there was such a problem that they pulled it back and released it with only one author's name, and dumbed it down. But the first version looked at a surprise Chinese strike using missiles, cruise missiles, and drones, against US Forces in Japan. Using 20% of their SRBM (short-range ballistic missile force), 30% of their medium-range ballistic missile force, and between 30 and 80% of their cruise missiles, because we don't really know what the count on those is, they could hit every US headquarters, every US ship in port, crater every runway and taxiway long enough to take off from, and kill 200 US aircraft on the ground. That's the opening 30 minutes of our war. And the fundamental problem we have: there's nowhere to back those aircraft up to, which are within range of China. And these are not hugely expensive systems. Again, the Harpy, with 600 miles, can get to Okinawa from the China coast. The other big problem is that these are all vertical launch systems, so you don't have the advantage of knocking out their airfields. The idea that you're going to roll them back, as part of a campaign, is a little 'iffy' because they're on trucks, and we have not demonstrated the ability to actively hunt mobile systems. And particularly in a cluttered environment, when they break cover, the time from breaking cover to launch is about 10 minutes. That would require an enormous number of orbits over China all the time, to put a warhead on a forehead in ten minutes.

The other thing is trade-offs. Remember, operating costs; the F-35 costs $140M to buy, and $65,000 per operating hour. A loitering TLAM, and I use this … this is a very old system, but it's usable just because it gives you an idea. We paid $1.1M a number of years ago—with the advantage of mass manufacturing we think it would reduce the cost 40% to $600k—but $1.1M was a very limited run.

We never buy as many TLAMs as we should and, of course, the QX-222 is offered for $2M, so your trade-off is: you can have one F-35 or 230 TLAMs, or 70 QX-222s. And using only operating cost … now, when I say operating cost, that's just the way the US government charges it … that doesn't include aircrew training; it doesn't include the maintenance crew training; it doesn't include the people that operate the airfield; it doesn't include air traffic control; it doesn't include

golf courses or O clubs. So, by not operating the F-35, I can buy 15 more TLAMs, and that's an F-35 squadron of only ten, and flying a minimum number of 15 hours per aircraft per month, or five more QX-222s. So, in essence, every month you don't have the fighters, that you have these, your combat power can increase for the same amount of money.

So, where are we in the conventional air domain? Well, frankly, what I would do … again, if I were the enemy … I would attack your fourth and fifth generation aircraft on the ground, and your key enablers, and the Chinese have made it very clear that they're working hard to take out AEW&Cs and tankers in the air. And we do this, when we have a Red Team … I was talking to some guys the other night … the Red Teams work very hard at getting a tanker in the AEW&Cs, because they know that's a huge advantage. But suppose I can do it with cruise missiles? Launching out of Guam doesn't do you any good, if I can hit Guam, and they now can hit Guam. So, you're launching where? Out of Hawaii, or Alaska? How many tankers does it take to get you there? How long can you sustain yourself there? I can also strike logistics and C2 nodes. While cyber is not something you normally think about using drones against, remember, every element of cyber resides in the real world somewhere. It's on a server; it's passed through a node; it comes through a cable; there's a downlink antenna. All of these are susceptible to strike by cheap drones. So, I can also use it as a cyber weapon.

Evolved cruise missiles and drones are going to take over most manned aircraft missions; again, within two decades. There will still be some that we will need for special purpose missions, but we've got to start thinking in those terms. Because the fundamental question is: is the manned fighter range obsolete, and a question I always ask US airmen who are wanting to spend billions of dollars on the B-21, the new long-range bomber: do we really think anybody's going to let us fly those bombers out of Missouri, and not go after Missouri? If you take one of those, or a box of those cruise missiles and put it on a merchant ship, and put it in the Gulf of Mexico, you can range all our bomber bases, and Google Earth will let you know where they are, if you don't want to buy it from anybody else.

So, my conclusion is autonomy is inevitable. The key thing, and this is the good news slide … there is some good news in this brief, even for pilots … the good news is, you can lead the transition. Let's face it – all of this is happening fastest in the air domain, because of the physics. Air is simpler; things are more subject to rational rules in the air domain than they are on ground or underwater. So, you can lead this transition, because you're the first people being forced to; and you have two goals. First, to seize the advantage in each stage, and we're already doing that. It's kind of in our DNA. When you look at the way we've married cruise missiles with strike fighters, and we're using types of drones that are allowing us to get the strike fighters in, things like that … we're seizing the advantage in the early stage of making assistants and partners. Now, we've got to start working through the process of how do we make them the replacements? And, we've got to rethink operational concepts. We've got to experiment ruthlessly in free play, multi-role … some lives, some virtual, mixed together, and then you've also got to have tabletop games, where you just explore the logic of it. And really be ruthless. Make sure bases are not off limits.

Very often, the way you can justify the continued existence of the fighter, is that the base is off-limits. Or, if you've ever played a US Navy wargame, every game I've ever been in, we sink the carrier and it never seems to make it to the brief. Because if you're so short-legged, like the F-35 coming off the carrier, then your problem is how do I justify a $13B carrier?

And then become an aerospace force. I mean, if New Zealand can become an air power, you guys have already got it in your plan, but I think there's a real possibility and this is a natural place for the Air Force to lead. Lastly, would be study help. Others have succeeded. Millett & Murray's wonderful book on innovation in interwar period examines six nations and the progress they made between World War I and World War II, and why some of the innovations succeeded and some of them failed, and there's some interesting characteristics there, and you can examine your organisations.

And finally, perhaps the key thing aviators have to do is maintain air mindedness. I'm very concerned that if ground and naval forces get the idea that "hey, we can strike far enough with these missiles that we don't need air forces", that you lose that idea of thinking of air as a fighting domain, and we've got to maintain that. So, that's the good news. We're going to need you guys air-minded.

Okay, and I'll be at the speakers' corner, and for the fighter pilots, I guess, the phrase is fight's on. Thank you very much.

Imperatives Opportunities and Challenges in the Digital Age

Mr Mark Ablong

Thank you very much everybody. And it's a great pleasure to be here to talk to the Air Power Conference.

I was actually asked very quickly to talk a little bit about the sorts of things that keep us awake at night. The things that really cause us to think deeply about the nature of what we're trying to achieve and I thought I'd start that by just reminding you all. I'm sure you've all had a chance to read the 2016 Defence White Paper. What it did was establish an alignment between strategy, capability and resources that is fundamental to the way in which Australia and Defence maintains our military capability edge and prepares for the high-tech conflicts of our future.

I want to talk about each one of those elements. Strategy, then capability, then resources.

Over the last couple of weeks, both the Minister for Defence and the Secretary of the Department have commented that changes are occurring in our strategic environment at a rate quite a bit faster than was anticipated in the 2016 Defence White Paper. Most significantly, we have seen North Korea make faster progress with its ballistic missile capabilities and its nuclear capabilities than was predicted. And we've seen Kim and the North Korea regime show a willingness to endure harsher sanctions than perhaps the world had expected. But that's not the only significant change that we have been seeing over the last couple of years. The threshold for the use of chemical and biological weapons has changed, as we've seen recently in Syria and the United Kingdom. These weapons have been employed as both tools of intimidation, tools of assassination and tools of coercion. And that is something that we haven't seen in our environment for quite some time.

We've seen the emergence of hybrid and political warfare; new tools to try and shake the behaviours of states towards the interests of others. And we're seeing social media and information operations take on some grand strategic functions, as you would have seen with what has gone on in terms of the allegations of Russian interference in the US elections. All these sorts of big strategic changes are causing us to ask some fundamental questions about, at what point do the pace of change and the sorts of change that we've been seeing over the last little while overtake those fundamental strategic judgments we made in the 2016 Defence White Paper. And perhaps more importantly, is there something in all of this that is changing the nature of war quite fundamentally? I'll just leave that one and come back to it.

Secondly, I'd like to talk very quickly about capability. The White Paper and the great investment program that was released alongside it provided a significant increase in Australia's hard power, that is, the ADF's military capabilities and enabling systems to deliver a more capable, a more potent and a more agile future force. Sitting alongside those hard power investments that the government made, was a substantial new investment in soft power—our use of the ADF and the defence capability in international engagement. And this White Paper, for the first time, funded and prioritised as a core business for Defence, the idea of expanded capacity building using ADF resources, particularly in the South Pacific and Southeast Asia.

These two investments in both hard power and soft power are quite fundamental to delivering on the White Paper. But again, we start to ask ourselves some fundamental questions. And in this one, talking about capability, I particularly like to talk about the sorts of technologies you've

heard about today that are changing some of the nature of our regional superiority. They are hypersonic weapons, advanced materials, autonomous systems and artificial intelligence, quantum computing, biotechnology, and augmented reality. All of these things which we've been hearing about over a number of these conferences for perhaps a decade, are now starting to reap some real returns in terms of their ability in the military environment.

And the fundamental question you've got to ask yourself is, at what point are the very exquisite and very expensive capabilities, which we are acquiring in the White Paper, overtaken in terms of their military comparative advantage by some of those new technologies and new capabilities. This is the fundamental question. And it's one of the reasons why the White Paper talked in the section on the future submarines by saying, the technologies around ASW, the technologies around AI, about senses and systems, are moving at such a pace that by the mid-2020s to late 2020s, we are going to have to conduct another review to determine whether the submarine technology that we are constructing in the future submarine project still provides us with the relative advantage that we're looking for, or whether we need to change the configuration to make them more suitable for the future environment. That's a big investment we're making: the $50B we're spending on the future submarine. You have to ask yourself that fundamental question on a regular basis. And it's certainly the case that we do that.

Finally, I'd like to talk a little bit about the resourcing that was in the White Paper. The 2016 Defence White Paper was the first white paper to be fully costed, with external cost assurance of all the capabilities in it. The Government agreed to fund the White Paper by increasing the Defence budget to 2% of GDP by 2020/21, which resulted in about $195B of additional investment over the 10-year period. As you all know though, technology inflation is impacting upon the cost of military capability. And as our economies return to growth and as new technologies start to emerge, both costs are going to grow. We're probably going to see additional costs incurred by higher labour costs, both for military personnel, civilian personnel and contractors. We are likely to see higher costs in doing business and higher costs in sustaining the force over the long term.

In the light of the resource challenges we are likely to see coming forward, the key question we need to ask ourselves is whether we can continue to afford the leading edge, highly sophisticated, exquisite military capabilities, or whether we need to start thinking differently about the nature of our force structure. Those sorts of questions, the fundamental questions about at what point is our strategy overtaken by either new technology or new methodologies of war, the question about whether our capabilities continue to provide us with the best investment in our military capability advantage and whether or not we can be appropriately resourced to deal with all of that, are the things that the senior leadership is talking about and considering on a day-by-day basis.

I don't want to leave you with the impression that we're all doomed or that it's a particularly dark and bleak outlook.

On the contrary, on a regular basis, and the White Paper talks about this too, on a six-monthly basis, the senior leadership sits down with the Minister for Defence to re-examine, based on a formal strategic assessment of our intelligence system, our strategies, our capabilities and resources, and realigns that link between strategy, capability and resources. These six monthly reviews are an important part of ensuring that we can maintain the ADF that we need.

Since the release of the 2016 Defence White Paper, we've conducted a number of these reviews and I'm pleased to tell you that, to date, we have concurred with the plans laid out in the White

Paper. The capabilities we're seeking to acquire and the resources we need are still aligned. But there is a fundamental question about how long that is going to continue to be the case. And at what point we will need to start thinking about a realignment of those three elements of strategy, capability and resources.

Thank you.

Major General Kathryn Toohey, AM, CSC

Good afternoon. I wish to acknowledge the traditional custodians of the land on which we are meeting this afternoon, the Ngunnawal people, and pay my respect to their leaders, both past and present. I want to start by thanking the Chief of Air Force, Air Marshal Davies, and the Air Power Centre, for the invitation to address you today. The Chief of Army, Lieutenant General Campbell has asked me to pass on his apologies; he's currently travelling overseas. The title of my presentation this afternoon is "The Army in the post-Digital Age". An alternative title for my presentation might be, "The Rise of the Combat Geek".

I'm guessing looking around the theatre today, a sea of blue, that there might be a few closet geeks amongst you. I'm guessing that there are even more out of the closet geeks amongst you. But now, back to the official title, "The Army in the post-Digital Age". "Post-digital?" I hear you ask. I'm deliberately setting a stretched target for our conceptual thinking about the imperatives, opportunities and challenges, which confront defence leadership right now, and in the decades ahead. Notwithstanding the frantic catch-up the Army is embarked upon to achieve the essential reality of a networked, digital force by design, supporting the better distribution of information that MINDEF spoke about this morning.

We are kidding ourselves if we think this is our ultimate destination. Consider the work being done today by people such as our Australian of the year, Michelle Simmons, on quantum computing. It may well be a few years, or it might be many decades before the outcomes we seek in this area are realised. Either way, when it arrives, the change will be transformational for the way we think about warfare. Which takes me to the bit about geeks. Whoever stated, "The geek shall inherit the Earth," was probably quite right. In the high-tech world of our most likely future, there is no doubt we will still need some muscle bound, crack shot, adventurous, courageous, men and women to do the difficult things that no one else wants to, or can, do.

This is what the Australian Army solider has always done, and will always do in the future. War has been, and will remain a fundamentally human endeavour. But maybe in a post-digital world, we might be able to significantly enhance the effect, and reach, and scale of our combat soldiers through the application of technology. Given the challenges associated with a small force defending the largest island continent in the world, this is a very attractive proposition. Don't get me wrong, this isn't happening tomorrow, although the technology is maturing. Our adoption of it will take years, if not decades. I think that the requirement for dirty, dangerous, and demanding tasks of combat soldiers will not ever go away.

But as we seek to protect, empower, and support our soldiers to achieve their mission, the manner in which these dirty, dangerous, and demanding tasks are executed, will change profoundly. In the future, I believe robotic autonomy, artificial intelligence, and other fantastic scientific and

engineering advances, will provide alternative ways to do many of the hazardous, difficult, and repetitive things our combat soldiers do today. In some circumstances, possibly better. In those tasks, where technology alone cannot do that task, and there will be quite a few, our combat soldiers will be increasingly aided and enhanced by those same technologies. This will, I think, require a different set of thinking skills for our future combat soldiers.

More interestingly perhaps, these technologies may well allow service-minded patriotic geeks to serve in our Army and perform well in many previously aligned combat tasks. Your physical conditioning, how many push-ups you can do, or how much weight you can carry on your back, may become increasingly irrelevant in the age of robotics, and physical augmentation. If robots, artificial intelligence, and quantum computing technologies figure large in the ADF, as they must if these technologies develop and proliferate, our workforce much change to where the application of Australian humans to the conduct of warfare will bring the benefit. These might be in previously unknown roles.

The combat robot psychologist, mission-coding specialist, operational data miner—they may well be future trade titles. On the battlefield in the future, the urgent shouts for, "Medic," and, "Gunner," may instead become shouts for, "Geek, quick! We need you." This brings me to the imperatives, opportunities and challenges for defence leadership coming out of the rise of the combat geeks. The Deputy Chief of Army, Major General Rick Burr, has a favoured phrase. "Leadership makes the difference. It is the glue that holds it all together." Leaders empower, and create capability, by bringing people and technology together. As leaders, geeks, or otherwise, we exist to make a difference.

In the post-digital age, this will likely include recognising the tempo and rate of change in technology, understanding that change, the possible applications of the technology for our purposes, and training and configuring our workforce to deal with new technology. And perhaps, recognising that our future young workforce may be better adapted than we, the leaders, are. Are we prepared to be listeners? To be managed upward by the digital and quantum natives of our emerging ADF. In particular, we will have to recognise, understand, manage, and lead the cultural workforce impacts of the rise of the geeks. Soldiers who might be able to remember 28 computer passwords, but not the name of their commanding officer, and have more friends on Facebook than in real life; Isaac Asomov, being regarded as more useful than Clausewitz at Staff College; and 'World of Warcraft' games rather than rugby games during garrison sport afternoons!

On a serious note, the rise of the geeks will require a profoundly different way of thinking about the relationship between our people, the capabilities we offer them, and the manner in which we prosecute warfare. It will require deep thought about how we treat the legal, moral, and ethical risks that the increasing application of autonomy and AI will bring to the operational space. The challenge for Army in all of this, and for the young military professionals who will join our increasingly high-tech force over the next few years, is identifying, then using, the shifts in human technological interaction to enhance Army's mission effects.

This of course, must happen without dilution of the vital, moral, social, and cognitive aspects our people bring to the fight. The partnership with the joint force, the whole of government, industry, and wider Australian society, and the understanding we develop together about the possibilities, and the challenges, is going to be vitally important. In conclusion, the post-digital age will be defined by continuity and change. The need for joint effects over multiple domains,

will be the continuity. Change will be the possibilities enabled by new technology. The exponential development of new technology, and its application to warfare is inevitable, and assured.

The success of the Australian Army's leadership, and that of the broader Australian defence force, in leveraging the opportunities afforded by technology, is neither inevitable nor assured. Leadership is the key. It will be the glue that holds the force together in the face of massive technological changes coming to our capabilities, and our people. We must work harder to listen, and understand the impacts that are coming, and comprehend the true impact of the rise of the combat geeks. Technical dystopia, or war fighting nirvana? Where we end up will be a result of our success, or otherwise, in embracing the change which is coming.

As we ponder that, I will leave you with a thought offered by Bill Gates. "Be nice to geeks, chances are, you'll end up working for one."

Thank you very much.

Vice Admiral Tim Barrett, AO, CSC, RAN

Good afternoon all. Look, I was told I had the last gig of the day. It's been a long day, if not for you, certainly for me. Many decisions have been made and so I am going to keep my presentation fairly short.

I am going to start with a video. I'll give you a sense then of where Navy is affected by a transition into the digital age. But I'm going to present it in a way that I hope is vastly different from what you have seen today. I was told "You need to do a Ted-type talk", so I bought a clipboard. I'm going to wander around like this and I'm just going to give you my sense of where the world should be.

If you don't like what I've said, I don't mind, because half of what we should be doing here is challenging our own thoughts and our own views of how the world will look. So, we'll just start with a quick video. Thanks.

Look, that's got nothing to do with what I'm going to talk about today. I've just had this ongoing passion to be able to come to an Air Power Conference and show you something about Navy.

So, let's just talk about the digital age. What I've been asked to talk about, and I'll do it briefly, are Imperatives, Opportunities and Challenges. So, let me just set some context. It might be hard to believe, but it's only about 10 years ago that Navy stopped teaching Morse code and semaphore. Think about it. What I used to enjoy was, at sea, you'd be alongside another ship doing not air-to-air replenishment but alongside replenishment. Two ships probably about 100 feet apart; there'd be a couple of sailors in complete silence looking at each other across the two ships and they'd just be waving their arms like this. And then, all of a sudden, they'd start laughing as if the world had come to an end, telling jokes, but it was only at the punchline that you realised what they were doing. Where I'm going here is the ships were doing about 18 knots, 20 knots if they had a need for speed, but big data, big data these days; the amount of information that we need to share across our fleet, the bandwidth we need to do it, it actually now travels, not at 20 knots, but it travels at, well think about it, about 624 million knots. I mean, that is the speed of light.

The information warfare side though is not the only bit that affects us when we consider where the digital future will lie. We have a tendency only to capture it around our management of

information warfare. And I'm sure that that's where you've talked, or you have talked about today, but I want to go a little bit further. I want to go left of the fight but talk about applications of significance when we talk about the digital world, but where it will enhance the fight.

So, I'm going to talk about a couple of things that are important for Navy right at the moment. The first one, let me say, is, you might not have heard, but we're about to recapitalise the Navy. And I'll say that again. We're about to recapitalise our Navy.

Government will spend about $150B over the next 30 years in doing just that. It's a significant amount of money, clearly. But there's an aspect of this that is important where I think that an understanding of the broad-spectrum issues of what the digital age is all about is just as important. And when I normally speak to people, I don't always concentrate on the warfighting end; I like to talk about this continuum.

And some of you might have heard me say it before. It starts at one end, the high end, with deterrence, which is what we do. Face it, as a Defence Force; our aim is to demonstrate that we have a capacity and a will to be able to demonstrate deterrence so that our adversary will think twice about trying to hit us.

Next step down is lethality, because deterrence cannot be achieved unless you can demonstrate that you have a lethal force and that you're willing to use it.

The next step down is availability, because, quite frankly, I can own the best fleet of conventional submarines, but if they're all alongside the wharf and can't get away I've not offered deterrence. And how do you determine availability? Well, you talk about sustainability. And below that is affordability, 'cause, at the end of the day, the

Service Chiefs, including yours, myself, Chief of Army, we sit around in a group at the investment committee and we have to decide where our priorities are against what is a finite set of money.

So, along that spectrum, that continuum, and I use it all the time because there are elements of all of us, not just the fighting force, not just those who support the fighting force but industry. But also, other parts of the community offer those who will be educated enough to be able to work the systems that we are using: it's those financiers who support what industry needs to be able to generate, that is, the things that we have to have in place for industry to meet sustainability, availability, etc.

So, let me just use one example. As I said, ship building. You may have hidden under a rock after the last couple of years, but we're about to create a ship-building industry in Australia. But we won't just be establishing something that churns out ships as we did during the First, sorry the Second World War, where we produced almost close to 60 ships in a short period of time. And they were almost prefabricated, and they just rolled out.

What we are developing is not just nine new Frigates, 12 new submarines, 12 new offshore patrol vessels; we're designing an environment in which we can develop the future Frigate beyond the future Frigate. We're developing the environment in which, according to the threat, we can adapt how we build those ships. There's probably some controversy here, but I will say I don't expect the Night Frigate to look exactly like the first Frigate that we built. And the significance here of what I'm saying in terms of the digital world is that we are going to build a—an environment, a facility that is built entirely from, … in Europe they call it Shipyard 4.0—a digital yard. It is the ability to understand your design intent, move that into design, move that into production, but

also at a moment's notice to be able to redesign, reconfigure and develop configuration control throughout your fleet.

So, we're taking the view that moving into the digital age starts fundamentally with the equipment that we're going to be using. It's all about being able to be adaptive against the need.

The next point I'll say, it's all about asset management. And again, from a digital age, we seek to apply those relevant practices, those relevant arrangements. And I always use an example – and I'll use it again in this audience given the aviation background. I always say that there's an aircraft usually flying between Sydney and London. It used to go via Singapore or via Bangkok, QF1, let's call it that. And, while it is airborne one of the engines goes, starts operating at a higher temperature.

Now, before probably anyone in the crew has noticed, there's someone back probably in Mascot who's already identified that the engine's going hot; they've already checked the other engines on that same platform to see if it's an issue across all of them; they've configured or considered the environment; they've looked at the technical means by which that engine was last maintained; they've looked at crew performance to see whether the it has done anything to make that engine run hot. And all this is being done so that, by the time it arrives in London, there's a solution to that problem. Why? Because that aircraft has to turn around and fly back straight away, because it's all about bums on seats, it's all about profit; it's all about availability. It's all about asset management.

Now, we don't do that in our surface ships. We build them somewhere, we sign a sustainment contract years later, we consider about 15 different agencies that all have a role to play in how we sustain it, and we wonder why we can't get our act together and deliver availability to the level we need when we need it.

Well, the opportunities that abound now, in terms of the digital revolution and the fact that we will be building through our new shipyards a regime in which we can understand emphatically how the ship operates, will allow us to do true asset management. And that improves availability which, together with lethality, offers a better deterrence to government.

The third issue: we often look at artificial intelligence, AI, In Australia. If you ask most people what AI means, if you're from a rural area, you'll talk about improving cattle herds and things like that. Artificial insemination, for those who didn't understand. But AI, in terms of – again, most people if they get the point that it's artificial intelligence, will think automatically about applications such as robotics or UAVs etc. There's another point to it where, you look at how you apply AI to schematics or to scheduling, and we are doing that at the moment; we've done it recently with the helicopter aircrew training system which is established in Nowra which will train both Navy and Army pilots and aircrew. We've used AI to determine the scheduling methods and all the arrangements we need to make it faster and more effective and more efficient to produce pilots of the right quality, aircrew of the right quality.

It's not just around the normal applications on the battlefield; it's all those other applications where we must need to move into the digital age.

And the last one, at the high end involves things like cooperative engagement. The Navy signed a contract, or sorry, signed an agreement last year that we will move to a specific way that Combat Management Systems will be placed in our ships for the next 30 years. We have set ourselves on a path where we will engage through EGIS to be able to provide cooperative engagement.

All of this entails using the digital age to transform how we do our business, but it's not just around the platform. It's about the environment. It's about creating a digital environment. It's about demonstrating that with these things you can be adaptive in your processes and you can match what is required across the threat horizon that we see emerging over the next couple of years.

In some cases, in Air Force, you would say "Well that's all about air worthiness." We'd say the same in Navy about our air platforms.

But, for us, it's also about sea worthiness. It's about assurance. It's about when CJOPS says to me, "The expectation that you deliver me the ship with the crew", I can demonstrate that it will do as he requires, and it will be done in accordance with the preparedness directive that CDF expects.

So, they're the kind of imperatives. It goes beyond just saying "What is the business end of the war fighting?" It's throughout that continuum that we need to consider all aspects of where digital design, where we move, where we transform, our business practices.

In the next bit, I look at the opportunities. And I've already spoken to them briefly. It is about joint design; it is about the future force and the amphibious demonstration that you saw in that video, so I will refer to the video. It wasn't entirely just there for my own benefit; that demonstration of where we are going to connect, if we are going to bring Army and Navy and Air Force—there were air traffic controllers on board that LHD that you saw—it's a matter of being able to show how each of those can be done. And it's the transformation through the digital age and it's the information we pass which is the glue that allows us to do that. It is not just about the platform, it's about the package. It's about the ability to adapt and mould and bring a task group together because you've set the environment in which we can all work together.

You should be confident that Chief of Air Force, Chief of Army and I meet on a regular basis and not just in the IC but when we are discussing with CDF the way in which we can produce what will be his future force. We do consider it together. We consider it as a joint design process. And I think of some applications straight away, be it theatre ASW, be it our ability to look at joint strike, which is not just a Navy or an Air Force matter, it is an ADF practice, or if we look at integrated air defence.

So I think I've talked about the opportunities, I've also talked about why we should be doing this. The challenge is, well, the very things that I've said offer us the imperatives are also the things that offer the challenge. And I know that CJOPS spoke to some extent around cyber forces that will allow us to be able to manage ourselves; well, for me, it is about asymmetric warfare and I use the example of when I talked about configuration control in a ship that we will design in one of our new yards so that I can provide assurance to CDF and CJOPS that it's ready to go when we need it. But the same thing that you hear that can and has happened in situations with air forces around the world, change one or two numbers in the NSN and you can completely change your assurance around the configuration control of your platform. You can completely undermine the assurance that you need for air worthiness or, in our case, sea worthiness.

They're the things that still hit us. So, at a ship level that is, configuration control and configuration management; and at an operational level, it might well be that you just corrupt the data, the nav data, and heaven forbid, we might walk into someone else's territorial waters. Yeah, someone understands that.

Tactically, you could start changing the control systems on board. And that is, you might not have any ability to affect the fact that your steering system which is controlled through some digital medium will be driven by someone else to take you into someone else's territorial waters. The cyber issue is important to us.

The second point is disruptive technologies. We've talked about some of the things that might change. It is the impact of robotics; it is the impact of UAVs. And some of those things, and again CJOPS mentioned them briefly, what it brings with it is a view about we're now introducing asymmetric warfare; we're introducing, in some cases, non-combatants, and we also have to consider the legal and moral aspects of where the ROE might be applied. Again, it is a challenge.

The third one for us is personnel capabilities. We're a nation of about 25 million people. Someone told me at some stage that there are nations in this region that recruit per annum more than every position or seat we have in an education institution teaching anything about IT or computer science in Australia. I'm not saying that they're recruiting all of ours; I'm saying in sheer numbers from within their own organisation, their own nation, they are able to do that on an annual basis. We have a capacity issue in Australia about our ability to keep up.

And the last one is that we live in a liberal democracy. The security challenge is here already. It's about our own R&D, it's about the fact that we have advantages in some areas. I would say our research in, say, acoustic signatures, certainly in hypersonics and some other areas, can be lost. It can be lost far too easily if the measures or the understanding of what we need is not embedded in the very institutions that are doing this work.

So, they're just a couple of challenges. I know there are plenty of others, but they're the ones that keep me worried at night.

So overall what am I saying? I said I wouldn't talk for long; I've spoken for longer than I said I would. We are already in the digital age. Get used to it. It is all about emersion, full emersion in the full spectrum of what I've said, from deterrence all the way through to affordability. It's not just about the high-end information warfare side; it's about our tactical and operational use of information and of digital transformation throughout the entire spectrum of how we operate. It's about the creation of a digital environment and thinking how we work within it. It's about adaptive technology, it's about our ability to take advantage of the speed with which this is upon us, but also, it's about the understanding that we need to secure the basis on which we say it.

It's an uncertain future. And I'll end by just saying one of my favourite writers, Martin van Creveld, once said that "No success is possible or even conceivable which is not grounded in an ability to tolerate uncertainty. We must cope with it and we have to live with it."

Ladies and gentlemen, thanks very much.

Vice Admiral David Johnston, AM, RAN

Now, because I know all Navy Vice Admirals look the same, for those of you, you'll recognise the Chief of Navy. He's the scruffy bloke with the beard that will appear shortly behind me.

Challenges, opportunities and imperatives. Chief of Air Force, thank you for the opportunity of having this chance to provide your Air Force brains trust the view and the imperatives from an

operational commander's perspective of that which we might need. Not only from air power, but from the ADF. The challenge that I have is, 10 minutes is all I've got to be able to provide that perspective to you.

I want to preface my comments with just a couple of sliding or starting view points. For the international members of the audience, my role in the Australian Defence Force, and perhaps it might inform a few of our own, is that I am the Joint Force Commander, that is, the employer of the force. I'm responsible for taking the great capabilities that the Service Chiefs, Chief of Joint Capabilities, provide and employing them on the task. What probably a few of you are less familiar with, is I'm also the joint trainer. I've got the great delight of taking the capabilities that are prepared by the services, bringing them together in the Joint Training Force—which is why Talisman Sabre is a JOC-led activity, amongst others—and then, of course, certifying the Joint Force, and taking it and employing it.

I've got that role across the ADF to look at the capabilities. I'm the zero to five year guy, would be how I would describe it. You've got General Tui, Chief of Air Force, and others who naturally have the role, who are looking out much further. My time horizon stops at about the five-year mark. That's about as far as I can judge the risks that we may have for the Joint Force and its operations.

I look closer. When I look closer, some of you might know this, I've been in and out of Joint Operations Command for a while. One of the differences in my responsibilities or the way I execute now to when I did as the J3 back in 2010, is the capabilities the ADF provides to me. General Evans was my boss back then, and the options I could put up to him as the J3 were almost substantively different to that which I can offer the CDF as the current chief, because of the types of capabilities that have entered the ADF, and those which will come to us over the next few years. I've got that part of me that's an historical perspective of what's changing in our operation environment.

Second preface I'd offer you, and you're about to have somebody who is much more articulate and will describe this better than I can, when Peter Jennings comes up, is the environment in which we work. The way I would describe it is, in my career, I do not recall a period where the geographic spread of security issues, nor the diversity of state to non-state actors that we are collectively dealing with, was as complex as it is now. All of that underpins, perhaps from here to the five-year mark, what we might be dealing with.

So let me start then with a few observations of my perspective on the characteristics of the operation environment which we are in. And these are only a few, I don't pretend it is all of them, but it is those that, at the moment, provide the priorities for me, the way that we look at the Force employment.

Speed of response is the key. Now, we've been used to an expectation that we can respond quickly under a number of different scenarios. And, disaster relief would be the most common one. We're doing it in Papua New Guinea at the moment, we're doing it in Darwin and cleaning up debris from the tropical cyclone that moved through there on the weekend. We thought we might be doing it in Victoria after the fires that have swept down through the south. But we are used, as an ADF, to being required to respond in low-end capabilities at short notice. We're now having to do it more frequently using different capabilities. When we responded to the rise of ISIL in the Philippines and the circumstances in Malawi in the middle of last year—that was an immediate turnaround for a P3 that was doing a maritime ISR task to an overland ISR role, over the top of that city.

In combat operations in 2014, we got about four weeks' notice from a government decision to employ combat air power over Iraq, for the commencement of our first operation in Saudi. So, speed of response now is an absolute factor that we have to deal with, and it has some consequences that I'll come to. Task diversity is now also common with us. If I picked a C130 operations during the early part, again, of mid-14, in Iraq, we re-roled from conducting humanitarian airdrops over Sinjar mountain that was very much needed, at short notice, to moving equipment in and around various European countries to provide to the Iraqi security forces. And then into more traditional air mobility tasks, to support our own forces on the ground.

One platform, multiple roles, and not much time between them. As both, I think, General Tui and Chief of Joint Capabilities indicated, the nature of what we have learnt over the last couple of decades of operations I fear can also mislead us. We have enjoyed, generally, an uninterrupted electro-magnetic spectrum. We haven't had to worry about air superiority. Sea control, when we've needed to move equipment around to various areas of operation, has been inherently available to us. We've got used to working in that environment, and I am very uncertain that that is the environment that our future operations, cyber, or otherwise, will be performed in.

A couple of final ones. Public visibility of what we do is very different now to how it was 50 years ago. You will see almost as instantaneously as I do what's occurring in Syria. I refer to what's occurring through Afrin at the moment and what was happening in Mosul during the fight there this year. The prevalence of social media on the ground, journalists in that environment, their ability to push information back into the global community, has a consequence to the way that we work. Two final ones about our environment: legal complexity—one of the wonderful things about having new equipment is that you've got to find a whole series, or we do find a whole series, of legal boundaries—and policy matters, that have either a significant impact on our ability to employ them, or take significant time to resolve so that we can employ them in the manner that we would seek to.

I'll return what we need to do about that. And, as Air Vice-Marshall MacDonald has said, cyber is everything to us. We do deploy cyber protection teams. We do conduct cyber operations. It does change the way we need to think about what others may do to us and the opportunities that also present themselves to us. That's the environment. Where do we find our competitive advantage in that environment?

At the very top of my list are two factors. One is absolutely fundamental to a small to medium size ADF, which is what we are, and that is an integrated force. We aren't big enough, like some of the larger militaries that we work with who can duplicate capabilities between their navy, army, air force, or marines. That is not us. The only way we are able to bring the full suite of capabilities together as an ADF, is to integrate the force, not just the services, but all of the enablers that are key to us. So an integrated approach is where we find our competitive edge. We are better at it than most, but we are not yet good enough at it, because there is more that we can achieve. When I talk about integrated, I am not just talking about military or defence capabilities. I also refer to our partners: law enforcement, immigration, those that sit in our national security bubble, but who, in the past, have not necessarily been the key, or at the forefront, of what we understand may be integrated.

It's not hard for me to envisage a scenario where I've got to get information off a JSF, into the hands of somebody who has an unclassified clearance, because they are the person who might need to use it. We've got to find a way of working with our partners and taking some of that information, some of the systems and capabilities, and handing it to others at a very different level to us.

The second of the two, and I said integrated is one, that is the absolute stand out for me, and I see it wherever I visit our people on operations—and we are sometimes trite about, and underestimate, just how powerful the effect of this is—but it is the quality of our people. We find ourselves not always with the technological edge; I think, increasingly, we're at least on par with many, regarding what we are able to operate with, but our people are remarkable. It is the one stand-out feature wherever I go. The way they operate with others, their ability to assimilate a culture, partner with people, ride across the spectrum that we're working with. Our people are remarkable. That should be a lesson in what we might need to do.

Finally, the consequences. How do we take the environment, how do we take the areas of competitive edge, and what do I expect of you and Air Force, and across the other services? The first point for me would be that we need to be ready to work with what we have and ensure that what we have brings the capabilities, the policies, the legal framework for us to employ it to achieve the mission the government gives us. We've got to, in the US parlance, the fight-tonight issue is a real one for us. When I describe a complex world environment that requires us to respond at short notice, we, the ADF, have got to be ready to take what we have and employ it at short notice across the spectrum of operations we could find ourselves in.

That's not just then about making sure our people are trained, certified and able to operate, it means all the supporting structures need to be at that same level of readiness with us. And there is the second part of my focus; intelligence databases, targeting systems, practises and policies, logistics, health, and all the fundamental enablers that come with us wherever we go. We don't move unless the movers can get us there, air mobility is in place, we can't operate in the environment unless the sofas, the protectors and immunities, and the policies that enable us to exploit the capabilities, are in place.

What I ask of you, is that when you think about the capabilities; you cannot look at it through a stove pipe of what your particular equipment set, or your functional element may bring. You need to look at it in the full environment in which we may need to employ it. And address those second and third order consequences that are key to us.

Finally, our people. That is where, I said, the edge absolutely lies for us. The training of that force, the way we prepare it, from our induction training at recruit, all the way through to the force preparation that we do prior to deployment; that full spectrum is what brings us to a capability edge that we can take our people and get them to do the remarkable things that they have.

That part of the future is bright. I leave you with the one comment: keep your perspective broad, the environment is demanding, the capabilities sets are with us, all of us need to think the second- and third-order elements that bring true capability to a battlefield.

Thank you.

Disruption and Resilience in the ADF

Air Vice-Marshal Warren McDonald, AM, CSC

Disruption can be caused by the smallest of things. All disruption needs is a way in. In the hands of an enemy, it's always looking for an opportunity. To demonstrate my point, I'll show a very short video clip. Viewer discretion is strongly advised as some of you will find this very disturbing. Video, please.

You may have noticed a resemblance. Yes, they are my children, and yes, as I stand here, I did tell my son at a very young age never to get into a survival situation with his sister, because he'll be used as a food source.

Chief of the Royal Australian Air Force, visiting Service Chiefs, distinguished guests, ladies and gentlemen; disruption and resilience are two words that we, in the military, should be familiar with. We should always be aware that they are also inextricably linked. Generally speaking, those who have been disrupted are resilient, and those who wish to disrupt had best be resilient. Using this link between disruption and resilience, have we as airmen paused and thought, "How resilient is modern airpower?"

For decades, airpower in most conflicts since World War II has largely had its own way over the battlefield. Over the 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 on the battlefields of Iraq and Afghanistan aided in 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 airmen, must remember our weakness, which is that we pursue technology without always thinking deeply as to its consequences and its vulnerabilities. Today, more than ever, we need to balance out the risks and the advantages. For example, the largely unopposed use of airpower in the Middle East saw the fielding of unmanned aerial systems without encrypted links. While the Taliban had little capacity to intercept these links, we forgot that others on the periphery did. They gained a bird's-eye view of our tactics and procedures, and in some cases, full platform ownership.

My opening question on the resilience of modern airpower would lead the listener to think that I'm 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. My comments are centred on the ADF personnel in this room. You might be surprised to learn that, for an Air Force officer, the outcome that I seek today is not to buy yet another piece of equipment at the other services' expense, but that I call to arms our service personnel to awaken to the threat, adopt the right attitude, stand your ground and remain vigilant against a clever and elusive enemy, and take up the fight and protect your nation.

While these words may 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 airpower in an age of disruption.

You are well aware of the rapid proliferation of asymmetric cyber capabilities, which, owing 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 subject to intrusion and deliberate targeting. So, too, have many high-profile Australian businesses. Likewise, there is an excess of open source data on operations in the Ukraine, all of which are instructive. Such operations are well within non-aligned nations' capabilities today, as they are with other powers whose interests are harmful to ours and who are rapidly developing capabilities and doctrine to exploit us. In 2017, we saw a 15% increase over 2016 on cyber incidents. Of the 47,000 events that occurred in 2017, 671 were considered serious enough that I sent the Australian Signals Directorate for an operational response.

All of what I've just said, mixed in with Hollywood movies and the media, would lead you to think that the only way to defend us against these risks is to have a sophisticated response and impervious networks, but let us not forget context. While it is true we must have sophisticated responses and strong systems, leaving it to advanced training and systems architecture largely overlooks perhaps a more traditional way to improve our security. What is that, you may ask? Simply, we can do it by changing our attitude.

Why would you say that's important? Because we are making it too goddamned easy for the enemy. Exploitation and disruption are not that difficult to achieve, particularly when the electronic environment is so pervasive. The in that an adversary uses is generally along the seams that we, perhaps—through the blind pursuit of social acceptance, technological advances, convenience, and commercial gain—have made available. Now, when you add the human element, which was the 'in' that led to the compromise of the Enigma machine, then you can see perhaps that a more traditional approach to improve resilience may just 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 matter. Stripped of all technical jargon, we should remember that cyber operations involve age-old elements of war, sabotage, subversion, espionage. While funding efforts to improve network resilience makes perfect sense, we have the awkward propensity to overlook one of the biggest threats: ourselves. Humans need context to shape their reactions and their responses, but when context is difficult to grasp and difficult to see, or, when it is so pervasive it is normalised, then we can lose focus.

This is equally true in other areas where things have been normalised. Many of you in this room, whilst in the Middle East, would have witnessed the widespread use of mobile phones and open landlines to communicate aircraft movements and other important events. How will we fare when the stakes get a little higher? Are we capable of changing disruptive habits that we, over the past 15 years, have learned? Additionally, many do not think twice about posting information on social media sites, all of which can be used by an adversary.

The integration of technology into our lives has been so rapid and so pervasive. Technology and its convenience is like a drug. We resist at first, then we quickly succumb to it, and then we forever forget the risks. 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.

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 freely available, then you open yourself to disruption and you cut the throat of resilience. We must remind ourselves that cyber and information warfare are a threat. When they are done well, their

existence is almost imperceptible. Importantly, we must remember that we are enmeshed in a conflict with absolutely no end date. Cyber and information warfare is not something that's going to happen. It's happening now, and it will always happen.

We set the scene well when we enter a conflict zone: for pre-deployment training, ID awareness, and weapons training, we generally have an end date. All of this provides context. It frames our responses, and it gets us into the right mindset. I estimate that we spend about 60,000 hours a year undertaking weapons training, not to be a better shot, because it's never helped me, but to make sure we don't shoot ourselves, or worse, somebody else on the team. The context now for our sailors, soldiers, and airmen is that deployed or otherwise, they must have the right security mindset every single day, because there are no physical borders to information and cyber warfare.

To make security improvements to a scale that I think we should accommodate requires no additional funding or personnel. It only requires the adoption of a warrior's mindset. For a warrior would not stick a dongle they found in a car park into one of our networks. The naïve would. A warrior would not put their password on a sticky note. The weak would. A warrior would not enable the Wi-Fi on a sensitive network. A moron would.

Only last year, the number of security breaches detected by our red cyber teams on Talisman Sabre were simply unacceptable. Very early in this exercise, locations of named individuals and 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 to have your head in the fight, because you think that your life is so interesting that everyone else on social media should participate. It's like flipping the safety off your rifle and pointing it directly at the head of your best friend.

So, what is the real problem here? Does it come back to the human psyche, that we have trouble understanding the intangible, something like cyberspace, which we can neither see nor touch? To elaborate this very point, I will talk about a recent example of a tangible security incident. Most of you would be aware of the recent loss of a filing cabinet in Canberra. This story gained considerable media traction. On this incident, we and the general public quickly grasped the issue. We quickly understood the security ramifications. There were images. There was a filing cabinet. Data was visible. How very, very primal. However, at the same time, there were actors seeking to access data on our government and public systems that would dwarf that found in that filing cabinet. Over the same period, I wondered, how many people had left their desks with their computers unlocked? How diligent were our systems administrators at sanitising our networks and understanding the authorities of those who were on it? 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 be a great benefit to the majority. The same can be said for alcohol. Is it that we enjoy the benefits of connectivity, both publicly and in the military, but that we subconsciously place convenience ahead of security?

We must be honest with ourselves and have a discussion on convenience over security, because the only difference between unclassified and top secret is inconvenience. If we have a mindset of convenience over security, then we must be cognisant of how far we interconnect our systems. The greater you interconnect, the greater is your exposure to risk and the risk of disruption. You provide seams, you provide 'ins'. Also, the more you interconnect; the more you should invest in resilience. To do otherwise ignores that the enemy is awake and that the enemy is hunting.

This is a challenge for every domain. Inconvenient? Absolutely! But to go down the path of full connectivity without thought disarms us as warriors. "Everyone has a plan until they get punched in the face," as Mike Tyson said. It's in the recovery. 'Fight hurt' is the United States Marine Corps catchcry. I think we'd do well to adopt it.

The final part of resilience is raising awareness of risk without creating alarm. For example, loose lips sink ships. 'How very World War II. How very traditional. How very effective!' Wishing these problems away is not a solution, and the ADF bears a special responsibility in this domain. So, what are we doing about it? Defence is undertaking cyber certification for existing platforms and networks before they can be used in operations. This will take a considerable amount of effort, but it is a sign that we're awake, and we acknowledge the need to prepare our forces to operate in all war-fighting domains, including cyberspace. Additionally, debate has begun in Defence on how far we pursue connectivity. This should equally apply to the public space.

In 2017, the Joint Cyber Unit was stood up. This year, Defence SIGINT and Cyber Command came into being. Additionally, we continue to strengthen our key relationships with government agencies so that we can cauterise the seams and the 'ins'. Also, with the assistance of the United States Cyber Command, a succession of accelerated defensive cyber courses are underway. Also, we are strengthening our cyber and information warfare awareness campaigns, so we'll come fishing for you.

People are the key to all forms of warfare, and resilient people are at the heart of it. By raising the awareness of the threat, we will know when resilience ceases to be a technical one and becomes a human one. In the end, resilience is largely about attitude. It's about being a warrior at home and when you're deployed. To achieve the best level of resilience, and that must be our collective goal in this room, we must first wake up and realise that we are in a fight that has no end date, and that those things, both cyber and information warfare, are a threat, and they will do you harm.

And so, to a Cold War adage that I learned, "Remember, while you sleep, your enemy studies your weaknesses."

Thank you.

Thriving or Just Surviving: Australia's Tough Choices in a Risky Strategic Age

Mr Peter Jennings

Ladies and gentlemen, good afternoon. I realise I'm the one thing between you and a drink and a snack, and, for that, I'd like to thank Air Marshal Leo Davies for his invitation to speak, but speak last. I hope I can say some entertaining and useful things for you today. My topic is to ask if Australia is up to the challenge of overcoming a risky strategic outlook. We've had a day of challenges, and now it's fallen to me to attempt to answer the question "Is our system going to make it possible for us to not simply survive, but thrive, in this international environment?"

My starting point here is to begin with possibly a slightly embarrassing story. This, gentlemen, is how many Australians really think of themselves in terms of our national qualities: confident, extroverted, adaptive, good with animals. You think this is a risky strategic age? That's a risky strategic age, ladies and gentlemen. But let me tell you, our self-perceptions can be inaccurate. Crocodile Dundee was, for example, what many Americans thought all Australians were like in 1986 when the movie came out, and when, at the age of 23, I went to the Massachusetts Institute of Technology in Boston as a Fulbright Fellow. They loved Crocodile Dundee, and they so badly wanted me to be Crocodile Dundee. Was I Crocodile Dundee, ladies and gentlemen? This was me in 1989. That's what I looked like. I can tell you; I was quite a disappointment to my American hosts. Although I do point out to you the rather fetching narrow-grain leather tie that I'm wearing. Sadly I don't have that in my collection any longer.

My point, and there is a point, Leo, is that we don't always live up to our national self-image. In fact, there's a long history of Australians doubting our ability to steer our own affairs. Some of you of a particular age might remember Donald Horne's book, which was published in 1964, The Lucky Country. The real takeaway line from Horne's book was this one: "Australia is a lucky country run mainly by second-rate people who share its luck." His critique was really about a type of Australia that we all know, a complacent, short-sighted, very unstrategic Australia, and Horne's book was one of a regular series, almost one or two every decade, which argue exactly that point.

But it can be countered by also more positive views about our capacity to deliver good strategic direction, and, if you want an example of that, I'd refer you to this book by Ian McLean, written or published five or so years ago, "Why Australia Prospered", which looks at of how it is that we've been able to run such a successful economy, not simply for a period of years, but really over the life of the country. It says, "Australia attained the highest incomes in the world in the middle of the 19th century, and remarkably they have retained that pretty much right up until the present age, a standard of living that is not appreciably exceeded elsewhere. Few economies," he says, "have been able to achieve that over such a long period of time." The reality is that we have actually achieved quite a great deal in our short history. Is this good luck or good management? A bit of both, according to Ian McLean.

What I want to go to next is to talk about what are the threats that we face that are impediments to our ability to thrive in this increasingly challenging international strategic environment, and I broadly identify four things about our national system: four things about the way we do politics that could be seen to be threats to Australia thriving.

This is the first one, what I've called the Canberra consensus. I've been a resident of our national capital for 32 years. I love the place, but a strong case can be made that Canberra's isolation from the wider business community and from the mass of Australia's population has disconnected government from the realities of Australian life. It's very much a one-company town, and, of course, that company is the Australian Public Service, which for a very long time was comprised of people who looked mostly like me, living and talking mostly with other officials, all with similar backgrounds and life experiences. So, a clear risk to thriving is the blandness and the sameness of the policy advice that goes to government.

I think the second threat to thriving is arguably that Australians can be a complacent people. "How complacent?" I hear you ask. The framers of the constitution made voting compulsory, in case we couldn't be bothered to go to vote at election time. Our national day is celebrated every year, but we're most enthusiastic about it when we can turn it into a long weekend. We're most passionate about celebrating our range of extensive military defeats. For some years, the Lowy Institute, my competitors you might say at ASPI, have been tracking Australian opinion on a range of mostly international issues and also on Australian attitudes to democracy, and the results remain largely unchanged since the question was first asked in 2012.

About 60% of Australians say democracy is preferable to any other kind of government. 60%! 36%, in fact, say that, either in some circumstances a non-democratic government might be preferable, or they say, for someone like me, it doesn't matter what kind of government we have. 36%! That figure actually goes up if you ask 18 to 29-year-olds. Of them, 48% do not agree that democracy is the most preferable system of government. Perhaps it's the case that long periods of economic growth have made us too relaxed and comfortable and too unwilling to believe that we face a more risky future.

The next threat is our political system. We're not badly governed I have to say, but there are some out-of-date aspects to our political system that need fixing. Three-year terms, a 36-month cycle for our federal government is simply too short for a strategically minded government. We have overworked and sleep-deprived politicians. Believe it or not, our federal electorates are two to three times the size, in terms of the numbers of their electors, of electorates in the UK and in Canada. We have about 100,000 voters per electorate in Australia compared to about 30,000 voters per electorate in the UK. The result of that is exhausted members of Parliament unable to focus on national issues.

I have no expectation of ever being able to win this argument with anyone anywhere, but our system would actually be better if we had more members of Parliament with fewer electors per electorate. Our Senate voting system supports too many micro-parties getting into the Senate, creating a near permanent block on government from the House of Representatives. These are structural impediments to our political system, which really do need to be changed if we're going to improve the quality of our strategic thinking. The fourth impediment is just generally the absence of strategy. Mostly Government and the Public Service have stopped doing strategy, by which I mean long-term and complex planning. Defence is actually about the last place in town that tries to take strategy seriously. Instead, what we have mostly is policy designed around managing as much risk as possible out of the equation.

Okay, so they're my four horsemen of the policy apocalypse, and what I want to talk about now is the things that we're doing well. If that depresses you and Julia, I want to suggest five areas of public policy experience, where I think Australian governments and their advisors in the Public Service

and Defence have done pretty well in recent years. The first one happened just last weekend, which was the holding of the first ASEAN summit in Sydney with the Australia government. It's actually no small thing to have nine out of 10 of the ASEAN Heads of Government in Australia at the one time, because here we have the leaders of 600 million people effectively that form our geographic front yard.

If Australia was going to play a role on regional security, a leadership role, this is the area on which we need to put some more priority. A second thing I think we've done pretty well over the years has been regional stabilisation. Operations like the one in Timor-Leste starting in '99 was really the beginning of the modern Australia Defence Force and also of the way in which contemporary Australian governments think about how to use the military. So, the role that we played then in designing, forming, and then leading a stabilisation force was new to a country which, at that stage, was more used to being a component of a bigger coalition operation. What I'd have to say is there's no going back to that older style now. The region and our allies expect Australia to take a stronger steering role in regional security. I would say though that, while we've been good at stabilisation, we've been poor at working out how to hand the reins of power back to the political masters of some of our neighbouring countries, and we've been even worse at promoting conflict prevention.

The third success is Air Force modernisation, and no, Leo, didn't ask me to put this slide into my presentation. It's not just because I'm talking to this audience. The Air Force is now effectively the go-to force that Government thinks of first when it thinks about providing an Australian element to an international military operation. Air Force has the most developed modernisation program and has the most developed thinking about how to fight with these modern capabilities, so there's a golden moment I think, a golden moment for Air Force to lead the ADF and Defence thinking on the demands of joint and integrated fifth generation forces.

I can't quite believe I'm going to say this to this audience, but Marc Ablong has left, so let's just keep it between us. We're pretty good at policy development actually. Defence does a good job. If anything, it's a bit too ritualistic and the organisation is way too disposed to worship at the altar of completed policy documents like Defence white papers. But there's no doubt that these are useful bits of strategic policy thinking in an otherwise desert-like Public Service. The desperate need is to work out an acceptable way of quickly questioning and modernising policy when it needs it, instead of doing what we do, which is doggedly defending the out of date.

Here's my fifth one, one that you may have spent a little bit of time looking at in recent months. The government, I think, deserves a real Bravo Zulu for delivering such a comprehensive modernization of Australia's legislation relating to espionage and foreign interference, which was introduced into the Parliament last year. When he did so, Malcolm Turnbull said that the laws had been based on the Australian Security Intelligence Organisation making significant investigative breakthroughs and delivering a series of very grave warnings to Government about foreign interference. It's fair to say that our system as a whole has not, or had not, grasped the nature and the magnitude of the threat. But I think the new legislation places Australia at the international forefront of attempts to counter foreign political interference.

Okay, so these are some things that we've done well, and we've spent the day talking about the range of challenges that we face in international security, so I'm not going to, you'll be relieved to hear, go into the challenges in great detail. But let me highlight four which I think are unusually important from an Australian perspective. They are some challenges that we have to deal with

as we move into the future. The first one is obviously China-US relations. This sets the broadest context for how Australia and other countries need to think about their strategic interests going forward. The key question for Australia is: What, if anything, can we do to shape US and Chinese behaviour in ways that better suit our interest? Frankly, it's going to require a more advanced approach to policymaking than we're used to.

The second thing has been referred to by a couple of my predecessors, and that's the speed of change that we have to deal with. I like to make the point that, in the 24 months it took Australia to write its 2016 Defence White Paper, China effectively staged a military takeover of the South China Sea. We're simply not well-geared to responding to the pace of strategic change that's needed to handle all the things rolling through the Asia-Pacific region. Look at our acquisition programme, which is more focused on the Defence Force we'll have in the 2040s. I frankly doubt that the current international order will survive to that decade, not at least without there being a major challenge to the system happening much sooner.

The next threats are hybrid, and the image there, if you're not familiar, is the Russian Buk anti-aircraft missile launcher moving into the eastern Ukraine in 2014, just before the shoot down of the Malaysian aircraft. The range of threats that we face are becoming more hybrid, and they're covering more grey areas short of outright conflict and impacting on the domestic spheres of our country. I fear that traditional Defence thinking doesn't address the span of risks we face in this emerging environment, so I'd ask the question of all of you: Can there be such a thing as hybrid warfare for good? Can we legally and ethically turn any of these strategies against our opponents or is a hybrid strategic approach only ever going to be something that's turned against us?

The fourth challenge is, of course, technological change. This is going to be the focus of much of the conference tomorrow, so I'm not going to dwell on it, save only to note that I think we're on the threshold of some astonishing changes to Defence capabilities as a result of artificial intelligence. The challenge for us is how we gear our thinking quickly to these new technologies rather than continuing to polish the current and planned order of battle.

Okay, so I've been through the challenges. I've been through the things that might slow us down that make policy difficult to do because of the nature of our political systems. If we take the Government at its word, that it wants to take on a stronger leadership role regionally and internationally, I think it's worth focusing on the costs of leadership, the demands of leadership, and whether or not, as a country, we're actually up to those demands. Four points to make about the demands of leadership. Great photo, if you look at that; all the recent Prime Ministers with the exception of Whitlam.

The first demand is that leadership costs. We've always wanted to have international leadership on the cheap. I guess the important question to ask here is: can we really provide strategic leadership in the region while we're spending a fraction just under 2% of gross national product on defence? Frankly, I found it slightly embarrassing to hear Malcolm Turnbull in Washington DC a couple of weeks ago celebrating, as a demonstration of our ability to be a regional and global leader, that Australia was nearing that 2% of spending on defence, when of course the United States in 2016 was spending 3.26% of gross national product on defence. My own view is that, in time, strategic reality will turn that 2% figure into the floor rather than the ceiling of what our defence spending aspirations should be. Of course, if you look at that chart, you see how our defence spending has spiked, but usually only after a conflict has forced us into a more uncomfortable reality.

The second demand of leadership is that it requires leaders to make decisions, and often governments are reluctant to make decisions because they close off options, and the consequences of decisions can be uncertain, like for example our hesitancy to conduct meaningful freedom of navigation operations in the South China Sea. At the very least, I think we should publicly do one of those now. But frankly the challenge is to be thinking beyond what is already a lost competition. My question would be: What will we collectively do when China closes the airspace over the South China Sea for a military exercise? That's surely going to happen this year or next. That will be the moment when some new regional leadership is required.

The next challenge of leadership is that it raises expectations. I've already made the point that we've become the victims of our own successes by conducting successful military operations over the last 15 or so to 20 years. So, if anything, our allies and our friends have higher expectations of us than we have of ourselves.

Finally, on leadership, individuals matter. Political leadership is a function of personality and capability. Some leaders have the ability to really lead or they acquire that ability. Others don't. In the words of Vladimir Ilyich Lenin, what's to be done? What are the things we need to do if we're going to improve our chances of thriving in the challenging strategic environment that we all know is bearing down on all of us? I've got six suggestions that I want to leave with you as being things that I think, from a national perspective, are changes that we should make to how we make and do policy, which would improve our ability to thrive in this new strategic environment.

It may come as a surprise to you to know that, in fact, Cabinet doesn't tend to make many strategic decisions. What Cabinet meetings do is that they tend to be very transactional and make week-by-week decisions, often in a quite reactive way. They're a sort of a clearinghouse of new policy ideas. The reality is that governments don't spend that much time thinking about strategy, but Cabinet needs to be our strategic engine room. During the middle part of his time as Prime Minister, John Howard actually held what he called 'special-strategy' Cabinet meetings twice a year, and they dealt with a 10 to 15-year outlook on the national economy and national security for the country. They were a great test of the long-term value of those day-by-day, week-by-week policy decisions. I'm not aware of the Australia Cabinet holding a strategy meeting like that for the last 15 years. So, more strategy for Cabinet, says the Head of the Australia Strategic Policy Institute.

Secondly, fewer political staffers. I've been one of these people. I've spent about seven years of my life over three separate jobs as a political staffer, so I have a sense of what these jobs demand and what's actually helpful to politicians, and I'm here to tell you we have a significant overcapacity in political staffers in Parliament House right at this moment doing damage to how government does policy by applying a model of risk aversion to every decision that has to be made. Offices that were comprised of fewer but more experienced political advisors would enable ministers to develop better relations with their departments.

Electoral reform: I think there's now a desperate need for Australia to move to fixed four-year terms in order to give our governments the chance to be more strategic and to spend less time campaigning or recovering from political campaigns. I think we need to change the Senate voting system so that it returns fewer micro-party candidates who are just there to block policy and to rent-seek, to sell their votes for preferential spending in their electorates. As I've said, we need more members of Parliament, which I would trade off against fewer senators.

This one might surprise you: university reform. What that list shows you is world rankings for Australia's universities in 2017, and frankly I think it's something of a national indictment of our university system that the best we can deliver is the AU at 20th in the world and then a long tail of underperforming universities. Our universities are failing us. They've become degree factories too obsessed with making money from foreign students, and they've lost sight of the core purposes of universities, which is to fearlessly pursue learning. It's time to review the purpose and funding base of our universities, and this, ladies and gentlemen, is the long-term solution to the skills shortage that most employers, including the Australia Defence Force, worry about.

Public Service skills. We've deskilled the Public Service to the point that many people no longer know how to do strategy or complicated policy. We need to promote people with the eye to encouraging imaginative leadership, whereas right now, the APS promotes mostly on the basis of people's ability to manage problems away from senior leaders. You've all heard the phrase "safe pair of hands." That's what that means. It's about managing problems away, not thinking creatively and imaginatively. The problem simply is that such a managing approach doesn't create any basis for making imaginative policy decisions.

We need to promote policy competition. My friend Michael Pezzulo and I don't agree on everything, I have to say, but he is a person who understands the value of competition for ideas within the policy context. That's why he engages with the think-tank community. Competition not consensus is the thing that promotes better policy outcomes. There's got to be more active interaction with groups outside the Public Service, not entities that are pursuing single-issue sectional interests, but rather individuals and groups willing to push the policy boundaries.

My final recommendation is what I've called 'red teaming' in Defence. We need a questioning environment where people have permission to think unconventionally and to question policy settings. I do see some of that happening in Defence with the current focus on innovation. That's very welcome indeed. But I would like to challenge Air Force to see how far they're prepared to go in thinking like this. So, Leo, next time there's an Air Power Conference, I encourage you to back the idea of an Air Power fringe festival. I think you should give your young officers, airmen and airwomen, the chance to think dramatically unconventional thoughts, and then be prepared to fund the best ideas.

Overall, these recommendations are designed to create a more stable political system, better able to make policy changes. Secondly, they're to improve the quality of skills that policymakers bring to their professions, and thirdly to encourage more of that sense of challenge and contestability in policy development. This is the best foundation that I can think of to help Australia deal with the deeper and darker strategic challenges that we face. Ladies and gentlemen, that concludes my presentation, and I think it's probably time for us all to go and have a drink and to talk further on these matters.

Thank you.

The AI Revolution

Professor Genevieve Bell

So, listen, it's my absolute pleasure to be here. It's a little bit daunting; I'd have to say. I realised when I walked into the building, I'd obviously dressed not quite the right way. I'm just going to blame Silicon Valley on that, and what I wanted to do for the next half an hour, having stolen someone's watch because I'm trying to give them up, is talk to you a little bit about where I think the future is going. I know this is an event dedicated to talking about disruption. I realise that disruption can get talked about in a lot of different ways. It can be a scary thing; it can be a thing that needs to be managed; it can be a thing that you sometimes hope you're just going to get to the other side of intact. I want to suggest it's also a different set of opportunities, and some ways we might want to think about how we husband and shepherd our resources and where we might want to place our bets.

I framed this talk around the notion of AI because I know that's a conversation we're all having. I want to be really clear here about a couple of things though. One is that AI as a label, the notion of 'Artificial Intelligence' – there are as many definitions as there are technologists in that field, and also cultural anthropologists. The thing about AI is that, really, it is in fact a constellation of technologies that run from data through machine learning and sensing and algorithms to include, I would actually argue, both ethics and the data that fuels that whole cycle. And artificial intelligent technologies are with us now and functioning, but they are the beginning of a much longer transformation that we need to be paying attention to. So, every time I say "AI", imagine that is shorthand for something much more complicated. And I want to think here about what all that technology is going to mean for human beings, our systems, our institutions, our organisations, and our countries?

So, there's lots of ways to locate all those remarks and to think about them. You heard my formal biography. Here are the other things you need to know about me. Not only am I a cultural anthropologist by training – I did my PhD at Stanford in the late 1990s. My work was in Native American Studies and Feminist Theory. You can imagine how someone like me would end up in a tech company. It was an obvious training, right there. And the reality is, like many Australians in the late 1990's knocking around the rest of the world, I met a man in a bar, in Palo Alto in 1998, and he changed my life by offering me a job, which was excellent. And I've spent the last 18 years at Intel prosecuting a particular agenda about how you put people into the business by which we make technology. The notion being that most innovation has, up until now, been driven by the notion of what was technically possible. Not always about what people wanted, what they cared about, what they were passionate about, what frustrated them. And my job at Intel was to bring all those things together.

But I come to anthropology through a sort of sideways route. I'm actually the child of an anthropologist – true. I grew up on my mum's field sites in Indonesia and in Central and Northern Australia in the 1970's and 1980's. I spent most of my childhood living on Aboriginal settlements in a time when those settlements were still new and I was lucky enough to spend that childhood speaking Warlpiri, not wearing shoes, killing things – and, I hasten to add, eating them, just in case you were concerned there – and it was the most remarkable childhood you can imagine, and it left me with a very particular way of thinking, both about the world and my role in it. My

mum was really clear that one of the things you should do, coming out of a childhood in Central Australia and looking at how Australia contended with its original people, was that we all had an obligation to make the world different to the world we found.

So, I'm in some ways part of, I think sometimes, the last generation of Australians who were raised on an idea of service, that you should remake the world into a place that you want to inhabit, with all your energy and all your capacities.

So, that's taken me all over the world. It recently brought me home to Australia. The Vice Chancellor at the Australian National University told me it was time to come home, and he told it to me in no uncertain terms, and then he offered me an interesting job, which was to think about how we might manage these emerging systems.

So, how would you frame all of that, right? You know, what's an anthropologist doing talking about technology? Why do I care about these things? Why should you care about them? Well, partly you should care about them because of this chart. The World Economic Forum published this graph about two years ago. In it, they attempted to, in some ways, stabilise the last 250 years, and give it a clear cadence and a clear kind of structure. And what they said was we have had four waves of industrialisation.

The first one we all know about; that's the original one. It involved a steam engine. It was basically when stuff got mechanised. We know this as the dark satanic mills, lots of big machines, transformations in production. And that happened between the late 1700s and the middle of the 1800s.

The second wave of the Industrial Revolution here is pegged to the production, really, of electricity and mass-market production. Think of this as the factory line. So, this is really the late 1880s into the 1920s and 30s.

The third wave of industrialisation comes with computers. So, think of this as basically World War II onward.

And then what the World Economic Forum said, two years ago, was that we are now entering the beginning of that fourth wave. And that fourth wave will be, according to them, characterised by cyber-physical systems.

Now, there are a couple of things you can say about this chart. It makes all that look very tidy. Like, that looks clean and simple and straightforward. And the reality was, if you were anywhere in the world as that was happening, it was not that tidy and clean and straightforward. There were massive social upheavals. There were dramatic transformations in political systems, in what got made by whom and how it was circulated, consumed, or rejected. We created entire new academic disciplines to contend with these things, and new forms of public policy and new forms of regulation. Frankly, most of you know wars were fought on the basis of who had access to these technologies, and those technologies changed the ways wars looked and felt.

It's been a complicated thing. It's also the case that each one of those new revolutions didn't wipe out the previous one. Computers needed electricity. Production lines needed machinery. Each one of these waves has been cumulative. This fourth one, however, is interesting because, like each one of the others, it represents a slight break in what the technology can do, and where we sit with it.

That first wave, around mechanisation, was about machinery that did more than our bodies could do. It was about machines that could move faster, push harder, and lift more. It let us basically make human labour happen at scale.

That second wave was about making it happen at scale, and at speed. And where it wasn't just about the human body pushing that machinery, but with that machinery now using electricity to drive faster and faster. That third wave took both of those pieces; the notion of being able to mechanise a process, in this case, computation, and move it further forward. But each one of those in some ways relied on things we already knew how to do, and in some ways on augmenting our bodies. This last one isn't quite so simple, and it represents a very different break from the last one, and that's where I want to kind of leave the rest of my remarks here.

First thing you need to know about that third wave of industrialisation. So, the thing the World Economic Forum says is about computers and digitisation. So, first computers that we would recognise as such, were built in the late 1940s; 1946, to be precise. ENIAC was experimented with, and basically went live in Philadelphia. It was huge. It probably took up an area the size of this entire space here. When you turned it on, it required so much electricity that the power in Philadelphia flickered, and households all over Philly went "Oh, they'll be computing again at the base". So, computing was actually a thing you could see, even if you weren't in the building. In Australia, we had our own version of this, a computer named originally Cicero, and then CSIRAC. It operated at the University of Melbourne, effectively in the 40s, 50s and 60s. It also required an enormous amount of electricity, about 35 kilowatts, for effectively one kilobit. So, basically, yeah, it would take I think about four million of them to be your cell phone. And by the way, it also took up this whole stage. So, it wasn't terribly effective.

But the thing about these computers was that what they did was subtly different than what had happened up until then. So, until 1946, when you said the word "computer", what everyone imagined you meant was a human being who did maths. A computer was a person who did calculations. In fact, usually computers were women who did calculations, who sat in rooms and tabulated large bodies of numbers. But a consequence of World War II was that there was an inordinate amount of machinery that needed increasingly complicated calculations, and in increasingly short amounts of time. So, the American Navy had a room full of women who did calculations to help aim, basically, guns off boats at things, and it became really clear that was inefficient. And so, the US Navy started to experiment with building faster ways of doing calculations to brute force their way through numbers. So, those first electronic computers were just smart calculators. But by the 1950s, those smart calculators become something else because they get programmed. So, it's no longer a matter of basically punching the numbers in. You could now abstract the numbers onto punch cards, and later to tape and even later to programs. And those programs told those computers what to do.

You should recognise this. This is, in fact, command and control, and this is what we talk about when we talk about computing from 1946 to now. It operated inside a command and control architecture. Effectively software told computers what to do. And they did it, and that's all they could do. That was it, right? And that is still true for most of the computing that will be allegedly turned off in your backpacks wherever you are sitting now, in that it mostly still operates this way.

But starting about 10 years ago, computing started to feel and look and operate a little bit differently. Something called the Internet of things turned up and computing suddenly got smaller scale, and everywhere, and started to collect data in real time. And that was interesting.

What was much more interesting was when data collected in real time could drive those individual little pieces of technology to do work, without an explicit program. So, we move from talking about command and control, to talking about artificial intelligence; first by talking about algorithms, and then new forms of learning.

Now, I'm willing to bet most of you in the room have heard about these things, and you know a little bit about them. What's important to remember here, is that we have spent an enormous amount of energy in the last three to five years, talking about AI. It's not the first time. 'Artificial Intelligence', as a phrase, was invented in 1956. It was really popular in 1956, and 1957, and 1958, and then not so popular for quite some time. Because it turned out it was really hard. It required all this computing that people didn't have. Computers didn't do what they were supposed to. The guys who were working on it found that they got funded to do other things, and artificial intelligence kind of died a few times on the vine until we get to now, when it looks pretty sexy and interesting. But my contention and my argument would in some ways be that artificial intelligence is no more or less than the steam engine to this next Industrial Revolution. It's not the end game. It's just the power. It's the thing that will make things possible, but like steam engines, it only gets interesting when you know what it's going to do.

So, when Newcomen built the first steam engine, way back in the 1700s, he was very pleased with himself. It was a lot of work. There were a lot of people who had theorised steam engines. No one had made them successfully. He made one; it was kind of cool. And he showed a lot of his mates, this steam engine, and they went "That's really kind of nifty", and a lot of people went around going "Ooh, steam engine's kind of cool". This is a crass rendering of the 1700s, but you know, not inaccurate. And for a while people went "Yeah, what are you going to do with that?" And eventually he worked out that what you could do with that, was pull water out of increasingly deep mines. So, the first steam engine stood next to a mine. It was huge. It required an enormous amount of wood to make the steam that would create the power to pull the water out of the mines. It was a big piece of equipment.

And for a long time, that's all steam engines did. They sat next to mines and pulled water out of holes. And then someone went "If you can do that, what else could you do?" And imagining how to put that steam engine on a train meant thinking completely differently about a whole lot of things. You had to think differently about weight. You had to think differently about the relationship between the heat source and the water and the steam. You had to think about how you were going to carry the fuel where you were going to find the water, because it came out of the mines. It wasn't going to come into the train in quite the same way. And the entire build of steam engines was transformed at the moment they had to be on a train.

And then they were on boats. There is a glorious experiment in America where they tried to put them on an airplane. It went every bit as badly as you would expect. There was fire and things exploding and no one ever tried it again, and that was probably for the best. Because what it made clear was that certain sorts of machinery require certain kinds of infrastructure. And when the steam engine went into the train, you suddenly didn't just have the men who made steam engines in the conversation. You had the guys who thought about actually building trains, and laying train track, and having to think about camber and grade and safety and selling tickets, and even as far as inventing daylight savings time and standard time, so that the trains would run on time, are all the consequences of moving the steam engine from sitting next to a mine to putting it into something that had to move.

So, if that's true about artificial intelligence, where would that leave us? If we imagine that what is happening here, is we are going from a moment where computing was all command and control. We wrote software; the computer did its job. Artificial intelligence makes it possible, that bundle of technologies, for computing not to need a pre-written piece of software to do its job. It can now look at a body of data and determine what its job perhaps should be. It can decide, based on previous activities, what you might want to do next. These are forms of building algorithms, right? You know, whether they are prompted by humans or, in this case, the data, drives the decision-making in the machine. You are now talking about the possibility of computational objects that aren't waiting for us to program them. Or that aren't acting on a program that was written years ago, for how to respond to a certain circumstance.

So, what would computing look like, if it doesn't sit inside a command and control architecture? What would be the principal questions and the things you would most need to manage and worry about? And there are three critical questions that surface, almost instantly, and they have implications for all of us, no matter where we sit in this ecosystem, because they're all things we're going to need to contend with.

The first one is okay, well, how are we going to manage these systems? What is that going to look like? What would be the ways you would manage it? You manage it through questions, right? The first question, the first problem we have, is if these systems are no longer command and control, are they autonomous? And if so, what do we mean by that word? We've spent, what, the last five years, certainly the last three, hearing an enormous amount about autonomous vehicles. Guess what? Every time you hear that word, underneath of it, is a different instantiation of the architecture.

How Google is making autonomous vehicles is completely different to how Volvo is. What Tesla is doing with their autonomous vehicle mode is completely different to what General Motors is doing. They all say autonomous, loosely, but that's basically like saying that your BMW is exactly like your Commodore. And, if any of you care about cars, you know that's not true. They are engineered differently. They are built to different standards. They have different implementations, and different ideas about what a car should do. They have some things in common like wheels and doors. But the rest of it can feel radically different.

The same is true with how those autonomous vehicles are functioning. Currently, Tesla, where every one of those vehicles is networked, in basically a hive mind. At the end of every cycle, those vehicles upload all the things they've encountered to a central repository, and that knowledge is, when it's considered relevant, pushed back out to everyone else in the system. They are a learning organism, basically. They are individual, but not autonomous in the classic sense. They ladder up to something more.

In other instantiations, we know that each one of those vehicles is separately architected and running on its own model, where it isn't sharing data. We know some pieces that are being built in the autonomous vehicle space, where those vehicles are communicating with each other in real time about the road situation around them. So that they are, in fact, an ***ad hoc*** network gathering data in real time.

So, one of the challenges here is when we talk about autonomy and, being autonomous, we aren't actually clear about what we are saying. And the problem in English at least—and not, I know, the native tongue for everyone in this room—but in English, autonomy is a slippery semantic term. Because when I say autonomous, there's a whole set of things in your head that immediately pop

up. Something is autonomous, it has a self. It might be self-determining. It has consciousness. It has awareness. Somewhere in the deep … possibly not so deep, if you're of my age … recesses of your brain, I say autonomous and you think Cyberdyne Systems went live and killed us all.

You possibly think the Terminator. You may think Frankenstein, if you were literary. But we know that when things come to life and get conscious, nothing good comes of it. And autonomy and consciousness get co-branded in our psyches, in ways that aren't always helpful. Because it turns out you could be autonomous, without necessarily having a fully developed human consciousness. But every time we go from talking about an autonomous vehicle to a self-driving vehicle, we've already made this interesting semantic move where the car suddenly got a self, basically, because the self-driving piece has knocked the human out of the loop.

Complicated, right? But what does it mean to talk about autonomy? How would we implement it? So, if we want to talk just in the most basic terms, about autonomous vehicles, or autonomous systems. Pick any robot and, to build that, there are radical things you have to do to your environment. If we wanted to have a fleet of autonomous trucks, for instance, ploughing the road from Adelaide to Alice Springs. That seems like a good idea, right? That is a long stretch of road. We know it is dangerous. We know there are challenges. So, for those of you not from Australia, that would be basically from the bottom of the middle to the halfway up. It's about 2000 kilometres, give or take.

Okay, so now we say autonomous trucks. Problem number one is that, although the word autonomous suggests those trucks are contained, they actually need a network. So, if you want to run autonomous vehicles on that road, you need to have a robust telecommunications network with low latency. Those of us who are Australians in the room already know the problem right there. So, you'd need a robust telecommunications network with low latency. You could get some of it done with satellite, but satellite's not good for real-time communication of hazards or other kinds of things, and the latency, that is, the amount of time it takes to bounce the signal backwards and forwards, is wrong.

There's also a cable lying next to the Stuart Highway. You could crack it up, pull it up, and, you know, be fine. Though there's some costing involved there. So, problem number one is you'd need a robust telecommunications network. Without that, what you would find would be a fleet of autonomous trucks parked at the Pimba Roadhouse. Which is a nice roadhouse, but it's probably not where you want to park your fleet.

Your second problem is that for autonomous vehicles to work well, you need to have a clear and well-marked infrastructure for them to operate on. They need to know the road is a road. If you grew up around anywhere in Australia, you know that there are parts of Australia where the road is a memory of a road at best. And frequently, a dim memory. That's good; we know that that thing over there that looks like it could be a road, might be a road, and we'll probably be fine on it. Trucks, not so much. They're not happy about that. So, now we have two classes of problems. The vehicle can be autonomous, but you need to have an infrastructure so there needs to be a world beyond the autonomous, to make autonomy possible. You need to have a network. You need to have a road structure. Oh, and by the way, you need to have an agreed-to set of rules. And the challenge here is the vehicles can agree to the rules, but human beings are terrible at this. My colleagues at Amazon have one of the largest fulfilment warehouses in the world which has a shared floorspace with humans and robotic objects that do shelving and pull things on and off the shelves. The robots have yellow lines between which they run around inside the factory. The

humans are told explicitly to never cross the lines. The humans are not like all of you humans. They routinely cross the lines, because they just don't think the lines apply to them or they think they can get across them more quickly than the robot. This means we have an enormous amount of time with the robots and the humans not intersecting well.

As far as anything we know about what happened yesterday in Arizona, with the crash of the Uber vehicle and a pedestrian who was killed, one of the things that seems to be clear from the first wave of data that's available there, is that the human acted in a way that was outside the rules. The vehicle was taught the rules. The human didn't obey the rules, and now we have an interesting conflict.

So, when we think about what it means to make machinery autonomous, it's not just about the machinery and what autonomy might mean. It's about all the other pieces in the ecosystem that need to be functional too. It's about a network. It's about a clearly maintained and well-developed built environment. It's about a steady stream of data. It's also about a clear set of rules, and about who's participating in them and who isn't. And then there are all the interesting problems about how would you mark these objects as being autonomous, such that everyone else who is encountering them, knows how to behave accordingly?

If you've seen a Tesla on the road, and you've paid attention to it, you know it moves differently to other cars. It looks different: the way it proceeds, it has a very different flow on the roads. The early Prius, when it turned up, confused the hell out of Australian wildlife, because they could see the headlights and couldn't hear the car. And there were a lot of kangaroos, I'm sure, standing around going "I don't know what that is. Like, bad".

So, how are we going to mark these objects as autonomous, such that we know how to respond to them? You can't run around the entire world, much as I'm sure some of you in the room would like to, and paint yellow lines on everything. And just go "Humans here, everything else over here". It's not going to work, right? So, how are we going to manage that? And then last, but by no means least, how will we think about regulation in this space? Who will regulate these objects? How will that regulation proceed? How will these objects be able to talk about what decisions they are making, and what classes of decisions are being made? And how that will be unpacked.

There was an experiment last year from DeepMind in England, which is a machine learning and algorithm and AI company. They built a machine and they taught it to play Go, a Chinese strategy game. It took about a month for that first machine to learn it, and it was exposed to the rules to "Go masters". It played game after game after game after game, until it worked out basically the rule set, and it started winning consistently. DeepMind then did something really interesting. They effectively created an experiment where that first machine, taught by machines, taught a second machine to play Go, without humans. It took that machine about 36 hours to work out the rules, and to reliably beat human beings.

So, from a month to basically a day and a half; what was more interesting still, was that the second machine plays the game inside the rules, but with a set of strategies no one has ever seen before.

And here's the complicated piece, if you're a regulator—or frankly you are playing against it, in both the metaphoric and literal senses—that second machine can't tell you why it is doing what it is doing. It doesn't know how to explain its actions. So, it's autonomous, but it can't explain itself. How would you regulate that? How would you decide that you wanted a piece of technology that behaved that way, inside your ecosystem? Would you want something in a battle situation that

made decisions that looked good, but couldn't be explained? Would that sit inside the conventions by which many forms of encounters happen? We already know there are challenges in the financial markets of using tools that do this. What will it look like when it's everywhere else? So, it might be autonomous, but how do we think about unboxing it? Regulating it? Managing it? What will all that look like?

So, if those weren't disturbing enough problems, you have a second-order set of problems. So, first question is, if no longer command and control, is it autonomous, and if it is autonomous, what do we mean by that, and how will we build and manage that? The second set of questions are okay, so now you've got these autonomous systems, how much agency do they have? That is, how much can they act without checking back in? What is their control and limit mechanism? So, if you are the autonomous vehicle example again, does your autonomous vehicle get to go to the edge of the ACT, because it's federal, and then should stop at the border? You know, if you think about every airport that we police, that would be one mechanism. Is it allowed to go to the edge of Victoria, but not to South Australia, because you wouldn't want to go to South Australia?

Like, you know, what are the limits and how would you define those in advance? And by the way, how would you make those visible? How would you think about multiple objects negotiating with each other that have different models of world inside of them? How do we think about what it will be to be human, when certain classes of decisions are taken from us, and are now being enacted elsewhere? And by the way, how will you know what that looks like?

So, my colleagues at Google, who do some of the most interesting experiments in this space, and who are incredibly good about being very transparent about what they're up to there, did some work last year when they built a series of little tiny basically intelligent agents, so, little computational systems, and all they did was basically negotiate for cheap plane tickets. That was all their deal was, was get you a plane ticket. So, we'll get you a plane ticket. Easy enough. Now, they built three of them. One, they trained on chess, for how you do strategic negotiations. One, they trained again on Go, for a different kind of strategic negotiation. And the third one, they trained on a single person shooter called "Call of Duty". Now, I am willing to bet all of you in the room can work out which travelbot got the best price, when you needed to get it done by lunchtime. Call Of Duty, obviously.

The problem was, no one wanted to negotiate with that travelbot ever again. Because it was total scorched earth, right? It was really bad. So, now scale that up. Imagine that you have intelligent agents, cyberphysical systems, operating on your behalf, your institution's behalf, your branch of service's behalf, and they're negotiating with someone else.

How do you know what they were trained on? How do you know what they have decided the appropriate way to act is? How do you know what limits they have? If it's someone in your command, you know because you trained them, or they were trained by people you knew inside a system that you understand, that is clear and transparent and reviewed. What will it look like when these systems have a capacity to act? How will they signal that? How will that be transparent? How will we regulate it? Will it be contextual or absolute? You can only go to Adelaide in the winter. You can only go when the temperature is above this direction you can never go. And if it's conditional, where does that conditioning sit? Does it sit inside the object? Does it sit on the network? Does it sit in some third party regulatory space? How does that work across national boundaries? Because again, these cyberphysical objects are going to move, but by the way, like everything else that moves, they will be regulated. The same way there are pieces of

technology and medical systems and people and, in my childhood, books that we didn't let into this country. The same with these systems too. And, by the way, there'll be other parts of the world which aren't going to let these systems move into their regimes either.

So, how does all that get played out and all that get managed? So, if not command and control, and some degree of autonomy, what are the limits? Who sets them? How do they get reviewed? How do they become manifest and get managed? And what's it going to feel like for all of us, just incidentally, because that would seem to be an important part of this puzzle too. And, and, and, oh by the way, some of these systems are going to be talking to each other without us ever in the loop. So, what's that going to be like? And how does that get made visible and managed and at what speed?

And then last, but by no means least, how on earth do you talk about safety, security, reliability, risk, trust, privacy, manageability, ease of use, and explicability. A whole bundle of things. Now, I've spent 20 years, actually, 25 years, in Silicon Valley. One of the things that was always very clear to me in my time there, was that we treated security as an afterthought. We built the system, and then went "Ooh, shit, we should work out how to secure it". Or sometimes we built the system, and then waited 10 years and went "Oh. We should have done something about that", and bolted security on the end.

The reality here with these systems, is we're going to have to think about this from first principles all the way through. How do we imagine these systems will be secure? How will they be authenticated? How are we going to think about liability, trust, and risk? Of the first people who are putting stakes in the ground about this, their imaginations of this world are both interesting and different from one another and start to suggest this is going to be a contested landscape.

The German Government, last American summer, the North American summer, the northern hemisphere summer, July, last July, put out a set of standards that basically said "Here is what is going to need to happen in order for autonomous vehicles to operate on German roads". They had a tripartite version of what they thought should be risk. They said the car manufacturers will be responsible for the vehicle and liable for the vehicle's actions. However, the metric by which they would measure the safety improvement of the vehicles was not about diminishing danger to the drivers but diminishing danger to pedestrians. Because their argument was that these people exist inside a society, and the implications of these vehicles can't be about diminishing road toll to drivers. It has to be about diminishing road toll to everyone outside of the vehicle. That's already an interesting logic leap, right? That's very different to what we have seen, perhaps, in the United States.

Second the Germans decided that the local government, so, the state government, was on the hook for building clear road marked infrastructure. So, no memories of roads in Germany. Just roads. With clear signs, consistent signage, well maintained.

The third piece of the liability they said sat with the Federal Government, which is responsible for ensuring that there was an implementation of clear and well-complied with road rules for the whole country. Now, think about how is it that we are going to determine things like liability? You have a cyberphysical system, it was trained on one set of data. It is enacting a certain set of policies. Who's on the hook? Who's the scrutinising body? Who decides if it's safe or not and under what circumstances? How do we then think, in that alpha Go example, how are we going to scrutinise something that doesn't even have a capacity to explain itself? Unsurprisingly, the EU has a series of regulations in this space, one of which is about the right to explanation. It will be

a hard one to work through, right, of how will these systems explain themselves? And frankly, if you're a regulator, that is a thing you're going to be looking for. Can the system articulate what it is doing?

How we think through this whole subject is sometimes talked about as ethics. I think it is both simpler and more complicated than that. It is absolutely the case that we need to think about how we build systems that do not reproduce manifest social inequities, and do not create huge problems. Doing that requires thinking more crisply and cleanly about data, data providence, and the biases in data. But this isn't just about being moral and ethical. This is about creating systems that can be scrutinised, where the decisions that are being built into the systems can be clearly made and clearly articulated.

So, if not command and control, if instead, systems that have some degree of autonomy, systems that will need a degree of agency, systems that will need assurance, we are talking about a profoundly different world than the one that we have inhabited for the last 60 years. We're also talking about a world where computer scientists and engineers, much as I love them, are not going to get it done. This isn't just a matter of bolting ethics on to CS and hoping that we can be happy. This is about saying as was true with every previous wave of the Industrial Revolution: we had to build new ways of doing and being and thinking. We actually built new roles for human beings. The first wave of the Industrial Revolution gave us engineers. The second wave of the Industrial Revolution gave us business degrees and MBAs. The third wave gave us computer scientists. I don't know what this fourth wave will give us, but I know that's what I'm actively working on building here in Australia.

So, my current role, maybe, my current role here is to put all those pieces back together again, and say if computing, if this fourth wave, this cyberphysical system world, comes into existence, who is going to help us manage it? Who's going to help us build it? Who's going to help us regulate it? Who is going to make it work? This isn't about saying we need to get rid of computer science or engineering or business. This is about saying we need to build a new way of thinking.

And so, for better or worse, that's what I'm doing with the ANU. I'm setting about working out how we would answer these questions. How ANU will, in turn, build a new academic discipline and a new body of knowledge, and I hope one day the people that I train will be working in your institution. Which means I also need your help. So, if any of this sounded interesting to any of you, bearing in mind there are lot of you in the room, please track me down. I can't come to the speaker's corner, because I've got to rush back to campus, but if you suddenly thought "I want to help that woman build that applied science", I am not stupid enough to think I can do it on my own. So, track me down, help me. And with that, I'm going to say thank you.

Imperatives Opportunities and Challenges in the Digital Age: An Industry Perspective

Mr Mike Manazir

Thanks, Mark. Chief Davies, fellow Chiefs and general officers, ladies and gentlemen, it's my high honour to be invited to address the Air Power Conference. I have been back to Canberra twice before this to talk to Williams and so it's a great honour to be back. I'm humbled to be able to take the podium and present to you under the benevolent gaze of my newfound uncle and auntie in the original peoples, and they obviously have a sense of humour because they had me following Genevieve Bell. And so, I hope to give you a little bit of a discussion point today on a set of pedantic rules that we need to look forward to as we go forward in this digital age.

A 5th-generation war fight requires partnership between industry and defence and when I say 'defence' today, I mean roughly those people in the Government defence agencies, uniform and civilian, and 'industry' being people that look like me. We need a partnership going forward. So, the thesis today is that partnership has to get stronger. We have to fix our processes to be able to succeed in this 5th-generation fight.

I did transition from the United States Navy, but I'm not a pensioner. The quickest way to get to be a pensioner is to represent to you today that my presentation is official Boeing policy. It's not. These are my views as a three-decade tomcat fighter pilot. By the way, Genevieve talks about carbon-based, silicon-based. I'm carbon-based, probably closer to early man. Don't have any hair on my knuckles because they drag. So, I give you a fighter pilot perspective about going forward, but these are my personal views based on my experience. By the way, kids, that's not me and if you want to figure out who that is and what they did after that, them come over to the speakers' corner at morning tea and we can talk about fighter aviation.

This thing is exceeding my carbon-based stuff. So, Einstein said that, "If I have an hour to save the world, 59 minutes will be to define the problem." The problem is our current process takes too much. It takes too long and costs too much. But we continue to go back in there and expect a different result. I'm on Quixotic ventures all the time, tilting at windmills all the time, trying to fix this process. We've got to fix this process collectively. There's wide bipartisan agreement in the United States that our current process doesn't allow the United States military to respond quickly or defence industry to respond in the way we did in World War II. We must change the model. We can't just operate around the edges. We have to come up with a new process that we can collectively go forward in to take advantage of the innovation that's out there for the 5th-generation fight.

As we look at the environment that we're all going to operate in, there are four forces that drive change to go forward. That environment affects everybody. It affects competitors, it affects allies, it affects 'competi-mates'. The first one is a maritime system. If you stand any place in Australia and look in any direction of the compass, you will get to a maritime boundary. Same with the United States. Logistics pipelines, destinations, sources or that 95% of the worlds merchandise moves across the sea. In the decade 1992 to 2012, maritime commerce increased 300%. In the Indian Ocean, the centuries-old centre of trade, fourfold or 400%. And while ships are about the same speed as they were in the late 1800s, about 18 knots or so, look at all the material that moves

in the biggest ships we have. Twenty-five percent of the world's oil and one third of the natural gas go to the Indo-Pacific maritime region.

The maritime system, global maritime traffic, is critical to our survival. Talk about maritime commerce, the freedom of trade, open seas: points for conflict.

The information system is the second force: currently, 2.5 billion people are operating an information system. They each have about two mobile devices. Between now and 2025, 1.8 billion people will join that consuming industry with three mobile devices. We double the amount of information in the world every two days. Undersea cables carry 99% of the world's voice and data, and 95% of the United States' voice and data. Interestingly, if you tried to move that to the high terrain into space—we think about beyond-line-of-sight communications all the time—if you tried to move that almost 100% of translation of information up into space, you could only carry 7%. Undersea cables are critical. People are using the information system, and the technology they use and the rate of technological change, is our third force driving innovation..

There's a great book by Friedman called 'Thanks for Being Late' and it talks about the rate of change to the human. It's going too fast. I can't keep up. How do I think about this? So, depicted on the right-hand side upper part of that chart are three different ways to look at that. The number of patterns for technology has increased exponentially. US private manufacturing has increased in output exponentially as well, while jobs remain roughly flat. Robots are now into the manufacturing space. In 2011 alone, robots in manufacturing space increased by 170%; man-machine teams; you should think about that, talk about that. Genevieve talks about autonomy and AI and its assist with the human. Where the human is in that team is a more provocative way to move forward into the future. And then the Internet. Sixty-two thousand or so hosts in the Internet in 1995, now almost a billion.

So, if we were to take those first three forces and think of them as three currents in a river that we're paddling down in our kayak, then the fourth force in that Navy budget is your paddle. I would contend that that paddle right now is a stick. It can't paddle very much at all.

Rand and the Congressional Budget Office have projected that Western or allied defence budgets between now and 2025 are going to flatten or go down in real value by about 7%. So, our resources to go after this rate of technology change and the environments of the global maritime system in an increasingly faster information system are increasingly harder to get. So, I just draw a graph of the budget authority in the US. It already looks a little bit unpredictable. You throw an administration change on top of it, sequestration, Budget Act of 2011 for us, and then a continuing resolution. You heard a speaker yesterday talk about the fact that we don't have a budget in the United States yet, and so we don't have a stable or historic budget consistency to plan on.

Deputy Secretary of Defence Shanahan spelled it out in the West Conference about how industry can work more closely with defence. He talked about industry setting the standards. Governments should agree to that standard. There's a deeper discussion on standards and, if you take a long time to try to define a single standard, you're probably losing the innovation in standards to go forward. The American telecom companies, as they progressed from the 1980s up to now looking at 5G, have a standards committee that gets together and talks about standards, but they never set themselves on a standard. Industry can set those standards and we can get together. Industry is going to invest; DoD ought to guide that investment, talk about that investment, be very clear on how we integrate that investment, and then get together in a room to evolve those capabilities

that both industry and government come up with instead of holding them close and then saying, "Here, try this." Data, information, knowledge—get it in the environment.

And, as we talked about with that silly Einstein cartoon, it costs too much, and it takes too long. So, at the core of the American national defence strategy is the ability to succeed in this space.

On July 21, 2017, President Trump issued an Executive Order calling for an assessment and a strengthening of the military defence industrial base and assessing the supply chain resiliency of the United States. In order for the United States to react to a crisis, or to maintain readiness, requires a capability, capacity and resilience of our industrial base and supply chain. The Aerospace Industries Association based in the United States responded to that Executive Order. They created a working group involving four pillars of success. We talked about funding already and the fact that it needs to be balanced and stable and predictable in an acquisition policy that can take those resources and turn them into capability in a rapid manner, by capitalising on the leading edge of technology. A talented workforce with specialised skills. Entrepreneurial mindsets with no fear of failure. Inquisitive minds who say, "What if we put chocolate with peanut butter?" And then the stewardship of key capabilities. What you have here in the Commonwealth that is special. What do we have in the United States that is special? What does each country have that is their secret sauce? What does each industry company have listed here that's our secret sauce? Steward those capabilities, maintain the IP but bring the ability to put it together. So, we maintain that competitive edge between countries and business, yet we still share the information.

So, a wordy slide here. I built it this way with the 10 fundamental priorities for you because you have access to these slides. You can take these away. So, as you look at these ten priorities, we need to buy back our readiness capability with balanced funding, but any budget or programmer has to balance current readiness, zero to five years, with the modernisation of what we currently have for the future, so, say, three to five to ten years, but what does that future look like in 2028? That competition between buckets! If we only have enough money to put money into either one or two of those buckets, you diminish the other one. You have to have balanced funding to go to all three. How do we move to the future?

We also have to quit jumping to the next bright, shiny object. When I was in the Pentagon doing the N9 job as the Deputy CNO for warfighting systems, we just loved to have the next bright, shiny object. I wanted to get the next aeroplane, the thing that I can grab onto. John Blackburn yesterday talked about a simple labelling of generations and we did that with aircraft. So, when I was flying a Tomcat back in the '80s I learned how to fight a third-generation aeroplane or a fourth-generation aeroplane. An F5 was a third-generation aeroplane and an F16 was a fourth-generation aeroplane. It was a simple label and characteristic of that platform. As we move into a 5th-generation fight, it's a combination of various platforms and capabilities. It's a 5th-generation fight with F18s, F35s, Growlers, P8s and if you tried to label them as 4th or 5th, you're not doing service to the fight that you have.

And so, as we look at that long-term planning stability, we've got to reform the contracting process. I will tell you that it takes too long. Lowest price technically acceptable. Curtail that. Here, lowest price. Yeah, it works about right. Best value, we need to do that. Best value.

And then you synchronise defence and commercial aerospace trade policies. So, what's the commercial space producing that we can use in the military and vice versa? We talk about COTS, or commercial. That's changed now, I think. Commercial technology is taking off and we in the military have to grab a hold of the leading edge of that technology.

Our people need to be more invested and inquisitive and stand with specific skills, not only aerospace and mechanical engineering plus cognitive computing. In electromagnetic warfare, across the electromagnetic spectrum, creating machines that can look at a signal and say, "That's not in my library but I can put that together and figure out how to react to that." Genevieve talked about AI and all of that, machine-learning materials and then of course the data science that goes with that. We have a dearth of data scientists. We look at our networks. You've got to figure out the data requirements. Data rate latency. Do I need to just do a weapons data set across a link 16 or a data-link network, or do I need to move a whole picture under an advanced wave form from one battle management asset to another? Maybe an airborne battle management asset to one on the sea and I need to move that entire picture with latency, so it presents the same picture to decision-makers no matter where they are.

So, a nuclear power train, so I've got a graph, but I'm a fighter pilot so it's a very simple graph. If we match our programs by value and time, so Chipper's sitting in the offices over there at Defence Headquarters, team comes in to present to him, they want to spend money on a project. It's going to cost $25 million. "Okay, what do I get?" "You get this. This is our schedule. These are our assumptions." We look at a PowerPoint brief very expertly delivered by people we trust, and we say, "Okay. I trust that. Here's all $25 million. Go ahead, Mike. Let's present and, just to make sure we're on track, we'll do periodic reviews." So, we put all our money and resources, and this early man's got a laser, so watch out. Right there with the most risk and most uncertainty, we put all our resources right there. And then we get out here some place and we say, "Hey, it's not really on track. Maybe our capability is not ready." I'm saying, "Okay, you know, that stuff's risky. I mean, we just didn't see how this was going to work. And I need a little bit more money and I need a little bit more time. That IOC was going to happen in 2022. Well, now it's in 2024." In a different scenario, that same presentation comes in at that certain time, Chipper says, "Those four assumptions you have; have you tested those assumptions?" "No. That's part of the program. We need money to do that." "Okay, okay. Back up a little bit. Slow down there, cowboy. The first assumption: how much does it cost to test that first assumption?" "Oh, it's about $200,000." "Okay. How long do you need to test that first assumption?" "Oh, three weeks." "Okay. Here's $200,000 and three weeks. Go test that first assumption and come back and tell me that it works, and I'll give you the money for the second assumption," thereby creating value as we go so that our resources match the risk that we have going forward. We need to do that. We don't do that in the Pentagon. We don't do that in industry. We want to get all the money upfront, so we can show business in the future.

I have a backlog. In the military, that is anathema. In the commercial world, a backlog shows that you're going to be viable for a long time and the street loves that. It doesn't do us in the defence industry or do us in this competitive world, any good. So, we've got to figure out how to change the processes going forward and still have wins in the business world, wins in the defence world, and wins in the competitive world partnering together.

Here are my imperatives as I looked at this over the last several years. When we innovate prototype, experiment and demonstrate, we need actually to demonstrate to learn something. It goes to failure where we learn and then go from there. I got in a fight, a little bit of a fight with John Richardson, the Chief of Naval Operations, about failure. And I lost; he said, "We're not willing to fail." I would stand up in front of a group and I would say, "Elon Musk was willing to

fail. In September of last year, his rocket blew up at Wallops Island. In December, he launched another one." In Defence, can we do that? Can we respond that fast? To be willing to fail.

The Admiral's contention with me was that we have to have tolerance for failure. Okay, like my tolerance for pain is about right here. Is your tolerance for failure at your shoe soles or is it up here at your shoulders? I'm going to risk big things, but I know the risk, I know the rate of return.

The other piece is key for those war fighters that are out there; steely-eyed operators who are waiting for the new thing to show up to be able to do better. It is operational risk. But in the acquisition world and the engineering world, boy, we're going to make it perfect. "Oh, it's not ready to go yet." We don't do early adoption in the military. We don't give the new iPhone X to somebody and say, "Hey, how do you think this works? Come talk to me later. See how it works." And so, the war fighter waits while we manage risk down to nothing. We need to match the acquisition engineering risk with that operational risk.

System-to-systems approach, integration and operability, kill webs shortly. If you're coming to Williams tomorrow, we'll talk deeper about kill webs. Imagine kill chains, horizontal, now stitch them together so that any sense or any shooter, any affecter can complete that kill chain. You sort of mash it together, you've got a kill web. It's a systems approach. You need an independent kill chain, or I can take my F18 with a gun and shoot somebody all the way to completely interdependent, where that network is operating together and can't do its thing without being interdependent. Federated, integrated in and out, aggregating, disaggregating, information flow.

Modern simulation analysis to be able to replicate the real world. You're going to hear two great speakers this afternoon talking about live virtual constructive. The mistake you will make thinking that live virtual constructive is a new way to do simulators means you don't understand the nature of the high-end war fight. Think 'Ender's Game'. Immerse the operator in an environment such that it is every bit as real. All the models are physical models. They're connected. We had to create waveforms to take data all the way from unclassified to sensitive compartmentalised information off the aeroplanes that are airborne and put them into the site to be able to mould with the virtual simulation or emulation so that are all being shown the same constructive environment. Everybody's operating from the same sheet of music.

I'm going to optimise the government industry team. In this fight going forward, two things. First, we have to connect what we have already fielded. You're going to need to cross the main solution to do that. Your E7 is already engineered a certain way by Boeing. Your joint strike fighter is already engineered a certain way by Lockheed Martin. How do you get them to talk? You need to cross the main solution to do that. And it isn't as simple as, "Here, just take this radio that I have in my aeroplane and put it over there. Everybody has the same," but it is about software-defined radios and software-defined networks. Your Air 6500 is an outstanding example of a chance to create the best athlete as you go forward. You have companies in Australia that do parts of Air 6500 to create an integrated air and missile defence capability later. You must partner with the services. Who gets the prime system integrator? Can it be the Government? Probably not. We're trying that in the United States and we're not doing so well.

So, we have to partner with industry. So, who in the industry is the best prime system integrator and then who brings pieces of that together so that everybody has a piece of it? You can't just be king of the whole thing. How do you create the national capability in any of our countries to be able to put our key capabilities together? The engineering solutions to integrated fire control are

hard and you have to do them early now because you already have fielded systems. Your Royal Australian Air Force is recapitalised with the highest end systems in the free world today.

You have a wonderful opportunity to put them together and have the greatest 5th-generation information system in the world today. You don't have to wait for anybody. I've seen it myself. I've tried to create an integrated force in the United States Navy and it's hard and I'm telling you, you have a great opportunity right now. Go. Don't wait. Get your innovators to start putting it together. Put the best athletes out there and have these discussions at the national level, with Government and industry. Different name tags, different labels. L3, Lockheed Martin, Boeing, CAE, Northrop Grumman, RAAF. Tim Bartlett stood up here and talked about creating the Navy. Who's thinking about connecting the RAAF with the RAN, the E7 to the Air Warfare Destroyer, and taking a whole picture out of the E7 and sticking it on the Aegis Weapon System on the Warfare Destroyer? "No, sorry, can't be done." Lockheed Martin. Boeing, "I can't move that. That's not the waveform we have." You guys break it open. Best athlete.

But all this stuff requires a secret. So, if we were sitting here—by the way, for you who are going to sleep in my last slide—if we were sitting here today with a group and maybe all the junior officers that are in here, I'd just keep that question at the bottom and I'd wait until somebody answered it. Because I'm running out of time. I'm going to lead you through this. In 1942, carrier aviation moved from a battleship navy to a carrier aviation navy. Billy Mitchell demonstrated decades before that you could bomb and sink a ship. He started talking about aviation. He got court-marshalled! Court-marshalled for his beliefs! Our speaker last night at dinner talked about Douhet, the French aviation theorist, being put in jail for his thoughts on aviation. Incarcerated! He pushed through. The Admirals in World War II in the United States Navy, John Towers, Halsey became a qualified aviator. They pushed aviation. Hyman Rickover with the Nautilus, nuclear power, risked then a development that we would not take now. He created that system, created the rule set around it and pushed it against all odds himself. Aegis Weapons System, Wayne E. Meyer, force of personality. The F1-17, Kelly Johnson, using a lot of F-bombs, pushed back on big air force and said, "Get out of my way. I know what I'm doing." John Boyd, F-16. The only reason the F-16 is alive today is because John Boyd completely slaughtered any opponent in front of him.

So, what's in common here? A human champion. Somebody who is ready to stand up and say, "This is where we're going." Sometimes those champions are singles, like Hyman Rickover, Wayne E. Meyer, Kelly Johnson; and sometimes it's a team, and I think in this 5th-generation fight, represented by the integrated battle force of 2030 down there, there might be more than one champion, but you need a champion set of people. And it's my hope, and I thought this in uniform, that we don't have to go to war to be able to figure this out.

Ladies and gentlemen, it's been a real pleasure to be able to introduce some concepts to you today. Some of the rule sets were sort of, okay, it's a set of rules. Well, the concepts in the other speakers are more provocative, but I think you heard some common themes and I continue to hear common themes from yesterday today. So, I encourage you to continue to stitch them together and take the opportunities that are in front of you. Thank you very much.

The Cyber Battlespace: Are we Already in the Matrix

Mr Alastair MacGibbon

Well, thank you very much for that introduction and thank you for welcoming me here. As you'll see, the topic is fairly appropriate with swapping in and out of characters; I'm not Alistair McGiven!

For those of you who haven't come across the International Cyber Policy Centre yet, we're now a team of about 10 people working on the full spectrum of cybersecurity topics with a focus on Australia and our region.

Now, I didn't come up with the topic for my talk today but when it was suggested to me, the cyber battlespace 'are we already in the Matrix?' I immediately had to go with it. My degree was in philosophy and perhaps, unsurprisingly, you can imagine how difficult it was to land a job with that background. So, now that I actually have a job, how could I go past a movie whose central theme is Plato's 'Allegory of the Cave'? It might be delayed gratification, but finally, it's going to pay off. The matrix isn't a bad place to start, though, when we're talking about the cyber battlespace. Someone asked me last week, "Will we actually even know when the next war begins?" So, if Australia's power grid is shut down in the summer and 20 elderly people die in nursing homes from heatstroke, are we going to know how many of them died because of their old age or because of the power grid being shut down? It might be hard to say exactly how many people have been killed because of that cyberattack on our electricity grid. The first shot in the next war may very well have been fired and we missed it.

For the last four years, at least in the possible matrix world that we've been living in at the Cyber Centre, we've been producing a metric of the cyber maturity of 25 countries in our region and I wanted to start off today with using that report as a bit of a foundation to give you a 30,000-foot view of where the region's at, some of the trends that we're seeing and, because in think tanks you're never really held to account for getting predictions wrong, a bit of gratuitous future-gazing. I'll finish up with a 'so what for Air Force?".

So, first the current state of play. Whilst cyber incidents are regularly making headlines, so far the region has escaped a major state-led cyber incident along the lines of the Russian attack on Ukraine's power grid. So, that's the good news. The bad news is that it's not because of our superior cyber security or our wonderful resilience. The reason is the relatively benign regional security environment. Russia is not currently, for example, engaging in a westward expansion and, while China in raising tensions in the South China Sea, and looking more and more authoritarian every day, it's so far not resorting to large-scale cyber-attacks targeting critical infrastructure. The closest we've come might be the WannaCry and NotPetya ransomware incidents or perhaps the massive heist on the Japanese cryptocurrency exchange that we saw in January.

Another dynamic worth noting is the fact nearly half the region is yet to gain proper access to the Internet. Now, the statistic that is widely reported is 55% of the region is still to come online. I think that number is very likely an exaggeration. You go to any remote part of Asia and see the ubiquity of mobile phones and it's very hard to believe that it's still that high, but the broader point still stands. There's a huge population still to come online and, while that creates lots of opportunities for those people and lots of cyber security challenges at an individual level, I think

there are other bigger-picture challenges like civil unrest that we need to be thinking about strategically.

Related to this prospect of bringing more of the region online is the rollout of new undersea cables. In our immediate region, this is becoming a security issue as we compete with countries like China to build and protect cables that connect our Pacific neighbours. For people in those countries, it's a great opportunity bringing in massively increased bandwidth and, with it, a host of cyber security-related challenges, but there's that broader strategic issue that we need to be cognisant of as well.

So, let me turn now to a couple of the trends that we've noticed. The first is the rise of cybercrime as a service. What we've seen over the last year or so is the increasing availability of a ready-to-use kit that essentially allows non-experts to buy and apply tools to conduct cybercrime. At a time when there's an acute skill shortage, this is essentially growing and expanding the pool of cybercriminal adversaries. The impact can be seen in reporting everywhere, where cybercrime statistics continue to increase. This general lawlessness creates a permissive environment for malicious cyberactivity. Law enforcement is currently overwhelmed with the volume of cases and hasn't yet come up with a strategy to turn the tide. In this Wild West environment, it can be easier for states to obscure and mask hostile actions.

The second trend concerns the perennial bad boy, North Korea. North Korea is a great example of the asymmetric nature of offensive cyber tools. A destitute and backward country, it's nonetheless managed to create a disruptive cyber capability that consistently has it ranked in the top four worst adversary states faced by the United States in that domain. Reports have estimated that North Koreans have up to 6000 people working in their hacking unit and have been blamed for a litany of offences. There's been the attack on Sony Pictures, there's been the heist on the Central Bank of Bangladesh and, most recently, the US and a string of allies, including Australia, have attributed the WannaCry ransom incident to the North. Interestingly, it's increasingly using offensive cyber capability for actions that are more commonly associated with organised crime, like the simple theft of money. As sanctions bite, we can expect North Korea to expand this enterprising criminal activity.

The third area I'd flag is China's actions in relation to commercial cyber espionage and espionage more generally. Back in 2015, President Obama convinced President Xi to agree to halt stealing commercial IP for use by Chinese companies back home and that was a big achievement and it was quickly turned into a multilateral agreement when it was included in the G20 statement later that year in Turkey. After that, there's been a string of other bilateral agreements, including one with Australia. While the jury's still out on whether or not China's fully complying with that agreement, I think there is a view that there has been a marked drop-off in that activity. And I think this also comes to a change of China into a more *status quo* power when it comes to IP theft. An old view used to be that China would steal IP and then bring it back domestically. Now, I think it's generating a huge amount of domestic IP and has a much stronger incentive to be in the game of protecting that under international agreements. And it's a good example of where diplomacy and strong statecraft can be effective in driving changes in state behaviour. Now, on one hand you've got this agreement around theft of commercial IP. On the other, you've got traditional espionage, cyber-enabled espionage, and there I think we'd see the opposite. This agreement does not specifically apply to traditional espionage and I'd expect to see that level of

activity continue. Just last year, we had reports in the Australian media with the launch of our ACSC report of a defence contractor being compromised who was working on a JSF project.

Now, I'd mentioned the NotPetya and WannaCry ransomware incidents. For several countries, including Australia, these shone a fairly unflattering light on our national preparedness. At an economic level, we dodged a bullet more from luck than from strong cybersecurity defences. But internal government processes and external communication with businesses and the public left a lot of room for improvement. The unfortunate thing is that this heightened awareness was short-lived. The discussion around NotPetya and WannaCry has all but dried up even though more similar attacks are inevitable. I think we can expect Australia to have a more coherent response next time this comes around but, with a few exceptions in the region, preparedness has not improved significantly, so the next attack could have a much bigger impact.

From a military viewpoint, the region's vulnerabilities create exploitation opportunities for adversaries, whoever they are. A final trend I'd touch on is the growth in offensive cyber capabilities. Something like 100 states are now thought to have developed some form of offensive cyber capabilities. As you'd expect, though, the range of abilities is vast. Some countries, such as Australia and the US, have been forward-leaning in talking about these capabilities. Australia has announced the formation of the information warfare division within the Defence Department. We've talked about some of its use that's been made in cases as well against Islamic State in Iraq and Syria and that it could be used in some circumstances against offshore cybercriminals. However, many militaries remain absent from cyber doctrine and policy discussions, suggesting the military desire for secrecy is still outweighing broader considerations, such as transparency, to reduce the risk of conflict. I'd anticipate resources for offensive cyber capabilities to continue to rise and the potency of these tools to increase. On transparency though, I don't expect many countries to be following Australia's lead.

Let me now look to the future a bit and offer a few gratuitous predictions. First, I think we can anticipate future big attacks like WannaCry and NotPetya that bring with them considerable disruption and financial losses. The types of gaps that those attacks exploited are still present. We are not yet in a position to regularly patch and our attack surface is increasing rather than diminishing as the Internet of things connects billions more devices to the Internet. WannaCry and NotPetya also highlight the willingness of states to deploy hugely damaging codes outside a wartime context, which brings me to my second prediction.

One of the differences between cyber tools and conventional weapons is that states employ them without fear of starting a major war. If Russia lobs a cruise missile into Manhattan, we know that conflict is almost inevitably going to break out. But when it manipulates the US presidential election or kills a few elderly people by shutting down a power plant, the consequences are a lot less clear. In just the last few months, we've had two massively damaging ransomware incidents publicly attributed to North Korea and Russia and so far, no major public retaliation taken by countries such as the US and Australia. If the West continues to fail to retaliate it will create a norm of doing nothing and that will only motivate bad actors to persist and be more destructive. At present, making attributions and not imposing consequences is worse than saying nothing. I'd expect peacetime attacks to continue until we develop a strong deterrence response and framework.

Third, if Donald Trump is not in fact the hugest dealmaker in history, and we end up with a war in the Korean Peninsula, I'd expect North Korea to use its cyber capability to be as disruptive as possible.

Not all this capability resides within North Korea, so it's possible that disruptive actions could still be launched even if North Korea's lines to the outside world were cut off. These attacks could range from WannaCry-style ransomware incidents to attacks on critical infrastructure.

Fourth, and this is a bit more of a medium-term prospect, I think you can expect to see a lot more disruption and civil unrest caused by the rollout of AI and automation.

The applications of AI and machine learning have the potential to be both brilliant and sinister. We're only just starting to scratch the surface of the change afoot here, but we can expect it to be massive. Automation is also going to be hugely disruptive. Already we've seen a major bank in Australia announce 6000 job cuts from automation and AI. We can expect to see a lot more of that in our region; things could be much worse than here. An ILO study estimated that 56% of all salaried employment in five major South-East Asian countries is at risk of displacement because of technology in the next two decades. Now, I think we're still at very early stages of making predictions around the number of people that are going to lose their jobs and the modelling is rudimentary, but the indications at least initially are of seismic change.

As automation becomes cost-competitive with cheap labour, multinational companies will be no longer prepared to make the old trade-off of heightened political risk for bargain-basement labour costs. That will see more and more manufacturing return to stable Western states or at a household level via 3D printing, thus leaving mass unemployment in its wake. The implications for regional development and stability because of those forces will be significant.

Fifth, I'd expect cybercrime to increase. Around the world, countries are still treating cybercrime as a local problem. We're gearing up local and state police forces to go after the bad guys and telling businesses and citizens to harden their cybersecurity defences. Notwithstanding this, cybercrime keeps increasing everywhere. The problem is cybercriminals are almost never residing in the same jurisdiction as their attacks impact and mostly, they live abroad. Any solution therefore needs major international engagement as a key component and states are only just beginning to realise that the current approach is failing.

Now for the Internet of things. As more and more devices are connected to the Internet, we're going to be able to create significant benefits and new business opportunities, particularly for Air Force, but we're also going to be expanding our attack surface and creating huge new risks. Think about a hacked driverless car, a tank or a drone. The challenge is that current market incentives mostly encourage companies to produce the cheapest possible product with security considerations often non-existent. Regulating a fix to this challenge is also not easy. Vulnerabilities are often not immediately apparent and might take a while to be discovered and the number of devices coming into the market makes checking them all impossible. Expect to see a lot more attacks exploiting IOT devices.

Finally, on the topic of cyber-enabled exploitation of our democracy. I think we can expect a lot more disruption here like what we saw in the US election. As a FIBOS partner and an American ally, we can expect to be a target of Russian interest, maybe not the top of the list, but a target nonetheless. And I think while other countries may not borrow directly from the Russian

playbook, we can expect to see a range of challenges to our democracy exploiting our openness and our information environment.

So, what for Air Force? First thing I'd mention is C4 ISR. Networks are central to the modern Western approach to war fighting, but they can also increase vulnerabilities. One of the reasons achieving robust cybersecurity is so difficult is that we constantly are increasing our frontal area to attack. The Internet of things that I just mentioned is a great illustration of this. Collectively, we're in the process of adding billions of new devices to the Internet and each one of these has potential security vulnerabilities. Many of them are built with no attention to security at all. The same goes for Air Force command and control systems. Using networks as a force multiplier can make a huge amount of sense, but it also makes it imperative to keep these networks secure and to ensure the integrity of the data that they transmit. Military decisionmakers require a high level of assurance of the accuracy of information provided to inform the planning and command of operations. So, verifying and guaranteeing the availability and integrity of information networks is a priority. This, of course, plays both ways. It is essential that Air Force invests to secure its own networks but it's also worth investing in the capability to penetrate and disrupt the enemies. To secure its own networks, Air Force needs to harden its military networks to make them better able to withstand attempted breaches. Perhaps, more importantly though, it needs to make them resilient. There needs to be an assumption that an incident will occur and when it does, the network should be able to retain functionality, limit damage and recover quickly. Achieving a high level of security and resiliency can also involve more active measures. That is, engaging adversaries in contested spaces and anticipating incidents rather than simply relying on the network's capability to withstand attacks or to recover after the fact. This could draw on red teaming, penetration testing, and intelligence collection on adversary systems. Penetrating and disrupting the enemy's network requires use of the offensive capability. This can involve both long-range actions taken from well away from the battlespace to proximate actions.

Second, I wanted to talk about kinetic enablers. Offensive cyber operations are much hyped. In 2012, the then-Defence Secretary, Leon Panetta, coined the term 'cyber Pearl Harbour' which massively overdramatised these tools. We'd just had out here Chris Painter, the former US Cyber Coordinator, who has a very nice line about this saying there is no magic cyber button.

A better way to think about cyber tools is as enablers for kinetic operations. An example is the 21st century cyber Wild Weasel operations to suppress enemy defences. If the enemy has their air defences on a network, then you have the capacity to turn it on and/or off, or to input misleading data. Electronic warfare and kinetic means will play a part in suppressing or destroying enemy air defences as well, but cyber tools will often be part of the package.

Third, digital AISA. Active Electronically Scanned Array, or AESA, is another area where cyber issues may come into play for Air Force both in terms of having to defend against penetration by adversaries and in the potential for them to be used in EW and cyber applications. Given the right knowledge of adversary systems, an AESA on a Super Hornet or a JSF opens the possibility of getting inside others' radar systems and making mischief, like generating false signals or masking your own signature. This sort of exploitation could be put to a range of malicious applications.

Finally, let me say a few things about our species. Just before I came on stage here, I was in the gents and I couldn't believe my luck. Sitting on the ground was an Allen's snake that someone had dropped and they're among my favourite candies, and can you believe it, it was a green one.

Okay. I was just kidding, but I didn't really pick that snake off the bathroom floor and for the international visitors in the room, I am really hoping this stunt is going to traverse cultural boundaries. Notwithstanding the fact that we all know that we shouldn't eat green snakes left on bathroom floors, we're still picking up USB sticks we find lying about and plugging them into computers. Of course, good cyber hygiene is about more than not doing silly things with USB sticks. It's about not clicking on too-good-to-be-true and suspicious emails. It's about using burner laptops and phones when you travel to certain countries. It's about being cognisant about your social media postings and how they could be used maliciously against you or your Fitbit, for that matter. In short, it's about how the whole workforce is made aware of its cyber security risks at work, at home and when traveling abroad. How we build a culture of cybersecurity that everyone takes responsibility for.

Another human dimension to this is a skills problem. As everybody knows, we face a huge stem shortage. It's a big challenge to attract and retain skilled staff. For Defence and for Government, it's also an issue how you compete with industry. This isn't the first time that defence has faced this sort of challenge and there's a whole string of advice that others have provided, which I think provides guidance on how you can work to overcome this problem, but it is a huge issue and it is something that I think Air Force would need to take very seriously.

So, to conclude, are we in the matrix? Right now, I'd say no, but looking further out at the confluence of technologies coming down the pipeline. It is going to dwarf the tech revolution that we've seen to date. AI, machine learning and automation are radically changing the landscape and I think we're only just starting to scratch the surface. Quantum computing offers huge potential and I'm not a quantum person, but I've heard arguments on both sides and there do appear to be some huge engineering challenges that still need to be overcome, as we've been saying for just 10 years of the last 30. So, I think there's still some way to go there. But if it can realise its promise, combined with AI, I think there's going to be some very, very dramatic change. For now, though, I think what we're talking about are a lot of very real-world challenges that we have to respond to and I hope that this presentation has sketched out a few of them.

Thank you very much.

AI and Security: Putting the Ghost into the Machine

Gregory Charles Allen

Hello. Thanks for the generous introduction. As he said, I spent the past few years working on a report for the Intelligence Advanced Research Projects Activity. If you're familiar with DARPA, IARPA is the sister agency serving the US Intelligence community, and that report was designed to look at the intersection of artificial intelligence and national security to find where these technological trends are taking us in military power?

I had a speech prepared for you today that was to go through that report almost line by line and share with you my conclusions. I have decided to throw that speech in the garbage after yesterday's presentation. This strategy, as you can imagine, is rather high-risk, high-reward. If you'll excuse what I sacrificed in polish and formality, I hope to make up for in honesty and frankness because I believe yesterday's presentations leave us with a conversation that we need to have about artificial intelligence in national security; that this is not merely just another technology, but it's going to affect national security.

This is a transformative technology on a par with the invention of aircraft or electricity. More than that, it has the potential to be a disruptive technology and while there were some amazing presentations yesterday, none of them actually talked about disruptive innovation theory. As the introduction mentioned, I went to Harvard Business School, which is the home of disruptive innovation theory, and its creator, Clayton Christensen, was my professor. I will borrow from him to talk about why disruptive innovation is meaningful here? It is not a synonym for a big change. Disruptive innovation does not merely mean a large technological change. In fact, it is a specific theory referring to in what types of situations *status quo* powers are likely to lose in competition and in what types of situations *status quo* powers are likely to win?

Now, Professor Christensen was specifically thinking about the business context, but I believe that this book, "The Innovator's Dilemma", ought to be required reading at every military academy in the world because this theory is incredibly powerful. It gives us the tools to analyse technology and where we believe those trends should take us. Let me introduce some terminology, if you'll excuse me. The first is sustaining innovation. This is the type of innovation that makes a better mouse trap. It works better, it moves faster, and it has higher performance. This is the type of innovation that is very attractive to the high end of the market, your customers who are most willing to pay. The second type of innovation is disruptive innovation, which goes after the low end of the market. The performance of the product is objectively worse than what it is replacing, but it is good enough for low-end consumers.

Disruptive innovations begin with products that are, excuse my French, crappy. They nevertheless take hold in the market because they are cheap and convenient. Let's use one of the canonical examples of disruptive innovation, which is the film and digital camera transition. A sustaining innovation would be like the transition from black and white film to colour film. It's an improvement over the existing technology. It's objectively better, and you'd be willing to pay more for it if you could. A disruptive innovation is like the transition from film to digital because, recall that, when digital cameras were first invented they were far, far worse than film cameras. The pictures were blurrier and had lower resolution.

The cameras were heavier, and overall, it was a more difficult system to use, but they had two principal advantages. They were cheap if you took lots of pictures because you didn't have to buy any film.

Moreover, they were convenient because you could look at the image you had just taken right after you took it and know whether it was good enough or you needed to take another one. What's amazing is that this disruptive innovation—going after the low-end of the market, the people who didn't want to pay for a tonne of money for film— ultimately disrupted the film industry and its incumbents. Kodak, a company that had dominated the photographic film industry for over 100 years ultimately declared bankruptcy. Why? Because, in the film industry, they were producing at profit margins of over 80%, but when digital cameras came along, they rode the consumer electronics industry with profit margins of 3%.

The winners in the digital camera industry tended to be companies like Sony who viewed digital cameras as an exciting new expansion of the consumer electronics market whereas Kodak viewed digital cameras as a frightening turf war that would reduce demand for photographic film. This is what disruptive innovation strategy or theory gives us is a notion of in what types of competitions are *status quo* leaders likely to win, and when are they likely to lose? Because the magic of a disruptive innovation is that the optimal strategy for the status quo power is the long-term one that leads them down the worst path. For instance, in Kodak's case, if digital cameras are going after the low-end of the market, this increases their temptation to focus on the high-end of the market. Folks like professional photographers or movie cameras that have the need for the utmost performance. That has the best profit margins and can secure their business while they lead digital cameras to take the low-end of the market, which is the least profitable for them overall.

Slowly but surely, performance of digital cameras creeps up at a faster rate than the film cameras. Every time you sell a digital camera, you're reducing overall demand for photographic film. As a result, you have this enormous fixed asset-based factory producing photographic film, and every time you take away demand, that fixed cost is spread over lower and lower product volume. Why do I bring up disruptive innovation theory in its specific and precise form? Because if you apply it to military theory, it again gives you a prediction of when *status quo* powers are likely to win or likely to lose in new technological competition. Right now, in the world, the United States is the *status quo* military power. It has the best technology across an astonishing portfolio of military capabilities.

The areas are, for example, nuclear-powered aircraft carriers and 5th-generation fighters, or cruise and ballistic missiles. These systems are incredibly capable, but they are also incredibly expensive and complicated. Counter intuitively for the United States, this is good. We love that our military systems are incredibly expensive and incredibly technologically complicated because we have a lot of money, and we have a lot of very smart engineers. If the basis of military competition comes down to who's willing to spend the most and who has the best technological engineers, we think we can win those types of competitions. The reason why disruptive innovation theory is therefore frightening is that it says that the future of military technology competition may hinge upon a different basis, the ability to make use of innovations that are crappy, but cheap and convenient.

Take as just one example, the Tomahawk cruise missile. This cost $1.5M per shot, not including the cost of the launcher. It can deliver an explosive payload over the course of hundreds of miles to a precision of within a few metres. In April 2017, America launched a strike of 60 Tomahawk

cruise missiles against Syria. The overall attack cost $100M. This is incredible performance, but it comes in an incredible cost. Now, think about a poor man's equivalent of the Tomahawk cruise missile, a consumer drone. As we heard yesterday, there are drones in the pipeline with ranges of tens of miles or hundreds of miles that cost as low as $500. You may say that these are a crappy substitute for the Tomahawk cruise missile, but this is precisely my point. They get cheaper and more capable every year.

Would you rather ride the cost and innovation curve of Augustine's law where an aircraft cost $5,000 in 1920 and cost $140M today, or would you rather ride Moore's law where the cost, or the performance-adjusted cost, of a personal computer has fallen by 95% over the past 15 years? Militaries with incredibly high-performance systems are at risk of looking at commercial technology innovations and saying, "These aren't as good as what I have now, and therefore they're not relevant to my mission." What they should be thinking is the exact opposite: "These aren't as good as what I have now, but wow, they are cheap. Wow. They are available to my adversaries who cannot normally get access to these types of capabilities." We are already seeing ISIS in Iraq and Syria using drones to create a poor man's air force.

Suddenly, they have airborne intelligence, surveillance and reconnaissance capabilities. Suddenly, they have airborne strike capabilities. They are nowhere near as good as the United States and its allies are fielding, but they are riding the consumer electronics cost curve and performance curve, not the aerospace cost curve. Over the long term and even in the near term, this has the potential to reshape the foundations of global military power, which now brings us to artificial intelligence. AI technology is a general-purpose technology. It is not a single capability that once you have it, it fundamentally changes your national power. That would be something like nuclear weapons, instead AI is a lot more like electricity, which in its early introduction to warfare, had a diverse set of capabilities, some of which were revolutionary such as radio and some of which are merely evolutionary such as the substitution of electric bomb detonators for lit fuses.

AI will be the same way. It will deliver a portfolio of capabilities, some of which will be revolutionary and some of which will be evolutionary, but a huge chunk of which have the potential to be disruptive military innovations in that the availability of commercial AI technology will give non-state actors and non-peer competitors, and even peer competitors easier access to capabilities that they would normally be denied. This is the essence of disruptive innovation. As I said before in my report, I went through the areas where I believe AI is likely to make a dramatic impact on military power and national security. I want to focus on a few here today, which is the future of military superiority and the future of intelligence superiority.

In military superiority, I see two important areas, the first being robotics and autonomy. In 2004, a book was written by a Harvard-MIT economist talking about the future of work in an era of computer automation. They held up one canonical example as what they believe indicates what computers would never be good at and what you could reliably depend upon as the future of your employment basis. That example was driving a car.

They said that making a left turn in the ongoing traffic was so complicated and so defied a listing of ordered rules that no computer could ever come up and figure it out. They were correct with the computing technology that existed then, which programmed by sequential instructions.

Ultimately before the modern machine learning revolution, every line of code in a computer was typed up by hand by someone, a series of instructions executing in the order that they are prioritised. The magic of the modern machine learning revolution is that the systems are, to

a certain extent, programming themselves based on exposure to data. While you and I would struggle to write down every single rule precisely of how to make a left turn in the ongoing traffic, by giving the system 10,000 examples of us doing it, it can devise those rules for itself. Thus, the modern machine learning revolution forces us to make our assumptions about what computers can and cannot do and throw them out the window.

Suddenly, new tasks are amenable to automation that only a short number of years ago would have been impossible. Driverless cars are simply the tip of the iceberg. In my perspective when I try to imagine what the future of military power looks like, I spend a lot of time thinking about nature and the capabilities that it has proven possible. I hope you're all familiar with the term of an 'existence proof', which is the simplest way to end an argument about what is or is not possible in technology. Before 1900, there was a large community of folks who said that it was impossible for anyone to ever build a propelled aircraft that could hold a human person. Once the Wright brothers were actually flying this aircraft, the argument was over. There was an existence proof.

I view nature as a sort of existence proof of what is possible in the future of robotics. Consider the Canada goose, which can fly 1500 miles in a single day at an average speed of over 60 miles per hour without refuelling. Snow geese form flocks that are clouds 12 miles long. They literally blot out the sun when they fly past, and they can cover similar distances at similar speeds to the Canada goose. How would an aircraft carrier battle group respond to millions of small drones with Kamikaze explosives flying slowly over an incredible distance and striking at any time' with the ability to loiter. We don't have to argue about whether these capabilities are possible. They already exist on planet Earth, and while the drones that we have today do not have those capabilities, as I said before, they get cheaper and more capable every year. The invitation is out there to experiment, and the modern AI revolution means that these drones can operate at a level of the autonomy and performance that simply has been unheard of in military robotics in the past decades.

The second area I think is very important is cyber security. Mike Rogers, the current head of the United States' National Security Agency said on October of 2016 that artificial intelligence will be foundational to the future of cyber security, and I believe he is absolutely right. His speech came only two months after DARPA's cyber grant challenge in which teams constructed autonomous cyber physical systems that could discover cyber vulnerabilities in their adversaries and exploit them, and at the same time, discover cyber vulnerabilities in themselves and patch them, all without a human operator. This was merely the stone age of what I believe we should expect to see in the near future of AI–applied cyber security.

There's a host of incredible possibilities here for what can be done, whether that be Automated Red Teaming, software verification and validation testing, increased automation and reduced labour requirements with any kind of cyber operation or discovery of new vulnerabilities and new attack vectors. This is an amazing set of capabilities in cyber that we should expect to see in the very near future. Next is information superiority. I think that we should take it a step back and consider the example of Stasi in East Germany. The Stasi had 102,000 members surveying a population of only 17 million East Germans. That's one spy for every 166 people in the country. That's how labour-intensive surveillance used to be in the past, but now we see that with modern computing capabilities and especially with machine learning capabilities, the amount of data that we're receiving is finally amenable to automation. It used to require humans, but now it doesn't necessarily do so.

The United States Intelligence Community collects more data every day than all its staff could analyse if they spent their entire lives upon it. If we cannot introduce automation, then most of this data will simply go unanalysed and ignored, but with machine learning, again it challenges what we believe is amenable to automation. Previously, it was almost impossible to write software code that could recognise a face in an image or recognise an animal in an image and, suddenly, we can now build AI systems with better than human performance. What is true in imagery is also true in audio data. There are now AI systems that are higher performing than the human ear and recognising spoken words, and a host of others.

In the military domain, I believe that we will in the near future see AI systems designed to exploit any type of data whether optical, infrared, radar, acoustic, natural language, documents, or spoken word. For these massive data sets that our intelligence communities have been collecting but don't have the staff to analyse, AI offers an opportunity to automate them in a way that has not been possible before. Of course, right now, the capabilities by and large are crappy, but they're also cheap and getting better at an extraordinarily fast pace. If you simply look at the capabilities we have today and say, "They're not as good as what I'm using now," you're missing the point.

The second area of information superiority where I believe AI will be critical is strategic deception and propaganda. In the same way that AI can be used to analyse data to generate insight, it can also be used to generate data to deceive. For instance, an AI system exists already that could sample the voice that I have been speaking to all of you, run that through a machine learning algorithm to deduce what is the fundamental properties of my voice. What does it mean for me to speak? Then, that AI system could generate my voice speaking any words that you can type into a computer. That could be me confessing to a crime. That could be me saying incredibly inflammatory things.

At the moment, these systems sound a bit teeny and robotic. Even the untrained ear can say that they are probably fake, but at the pace that they're making progress, we should expect that we are five years at most from them being able to fool the untrained ear. Over the longer horizon, they will be able to fool certain types of forensic analysis. This poses an incredible challenge to command and control organisations. You probably don't realise the extent to which you are using the human voice as an authentication technology. You know that it's someone because it sounds like that someone and you know that it's impossible to replicate their voice, but that's simply not the case in the future. What is true in audio is equally true in video. It would be possible to create a similar video of me confessing to a crime.

The implications here are incredibly diverse. Think of the future of the courtroom evidence, corporate communications, journalism and even international relations. I think back to, for instance, the Watergate scandal in the United States which brought down Richard Nixon. Most people forget that investigative reporting uncovering wrongdoing was ongoing for two years, and yet there was still not sufficient support in the senate to impeach and remove Richard Nixon from office. Only on the day that the audio tapes of him acknowledging ordering the criminal actions were released, did his support within the senate evaporate. Imagine what would happen in a world in which it was very easy to fabricate those types of tapes. We would struggle to know who to trust.

We're already seeing actors in the international system who are more than willing to use these types of capabilities maliciously. During the 2016 American presidential election, according to The Computational Propaganda Project at the Oxford Internet Institute of Oxford University,

fake news actually was shared on Twitter in a one-to-one ratio with real news. That's what we're dealing with in terms of fabricated text, but, usually, when one person argues one side, and another argues another side, HD video or recorded audio is a tie breaker. Nixon says he did not commit a crime. We say, "You probably did," but now there's tapes. This argument is over, but, in the future, this will not be the case and intelligence organisations like the Internet Research Agency of Russia, which has already shown adept skill at fabricating text and photographic evidence, are now going to migrate into these new domains.

Command and control organisations will have to think about how to secure communications and operate in this environment and this information ecosystem that has a lot more malicious intent. I'd like to ask how fast precisely are these changes occurring? Well, the answer is far faster than expected. In 2014, the expert who had built the world's best Go Plane computer program said it would probably be a decade until a system was able to beat a human champion. Instead, that decade came nine years early and the achievement heard only one year later. This is leading experts in AI radically underestimating the progress in their own field. How big are these changes? Well, the leading technology companies of the world report that they are remaking themselves around AI; remaking themselves, optimising every aspect of their organisational structure to take advantage of these transformational capabilities.

One anecdote that is rather illustrative: at Google, the AI team now sits directly next to the CEO. Why would they do that? Well, Google acquired a company called Deep Mind in London for $500M. This is the same Deep Mind Organisation that achieved the AlphaGo results that I mentioned to you previously. That $500M acquisition, Google estimates, repaid itself after their first project, which was using AI technology to optimise energy consumption in data centres. Literally, the first project they did with AI paid for itself! That's how precious the people who have the skillset to develop advanced AI systems are – PhDs, newly minted PhDs, in this field routinely command salaries in the private sector of $300,000 to $500,000. The capabilities that they give are transformational to an organisation. What is perhaps most shocking and most challenging for the militaries of the world is that these advances are overwhelmingly coming out of commercial industry. In the nuclear and aerospace era, the best scientists work for governments or for companies that were closely allied to governments. The best technology was possessed exclusively by governments and most research and development funding came from government organisations. That world is so far gone as to be unrecognisable. I can say this is not any kind of disclosure or classified information, but there is no super-secret laboratory in the US government developing super advanced AI that is way better than Google. They are behind the commercial private sector and frankly, it's not close.

In the West, commercial companies with leading AI capabilities have been reluctant to assist national security organisations. In the wake of the Edward Snowden revelations and Donald Trump's election, this has become harder, not easier. In China, it's a very different story; intimacy between commercial AI companies and military is deep. In fact, it's the official policy of China's national AI strategy released in July of 2017, which calls for a military civil fusion strategy where leading technology companies such as Alibaba or Tencent or Baidu work hand-in-hand with the government and its military organisations.

China's national AI strategy calls for matching the west technology in artificial intelligence by 2020 and leading the world an artificial intelligence technology by 2025 and dominating the world in AI technology by 2030. When China released this strategy, there were many who said that

China can't innovate, they can only copy. That may have been true 15 years ago, but it bears no resemblance to the technology landscape that we have today. In fact, maybe Facebook was making fun of Chinese tech companies ten years ago, but only last year, they confessed that many of the most recent Facebook innovations were actually copied from Chinese social media networks like WeChat. This is the world in which we live. There are many international computer science competitions, and Chinese scientists often win.

Chinese companies are producing legitimate artificial intelligence advances. For instance, the first company with the AI system that could recognise the human voice at above human ear performance levels came from China. The list of innovations comparable to that is quite long. If you think that China cannot secure a leading position in artificial intelligence technology, the simple fact is you're wrong. Former Google CEO, Eric Schmidt, said exactly this at my Think Tank's Conference in November 2017. He said, "If you think that there is something wrong with the Chinese government system or the Chinese education system that cannot produce these types of AI revolutionary people and technologies, you're wrong in the present tense and you're likely to be far 'wronger' in the future."

Eric Schmidt explicitly said that China's national AI goal of surpassing the United States in the West in AI technology was credible, perhaps even likely, without major government action. What is China's advantage in this? It's primarily strategic focus and funding. Leadership all the way up to Xi Jinping has announced that this is a top priority for the nation. In fact, his summer reading list included many books written by a Western computer scientist on artificial intelligence. The amount of funding that they are willing to commit to technologies that they identify as of strategic national importance is extraordinary. Consider their semiconductor plan, which in many ways, resembles the roll out of the national AI strategy.

In 2014, I was reading a semiconductor industry analysis that said, "Well, China probably can't lead in semiconductors because they're so far behind, they would probably have to lose at least $100B to catch up to the state of the art in countries like Korea."

Only a few months later, China announced the funding figure for the national semiconductor strategy and it was $150B. When they identify a technology as a critical national importance, their willingness to prioritise and fund is extraordinary and that is exactly the focus that they are placing on artificial intelligence technology right now, and it is extremely frustrating frankly, to me as a scholar working in these areas, to see some of my own recommendations to the US government be implemented by the Chinese government first.

Take for example, the Defence Innovation Advisory Board's recommendations in 2017 that said the Department of Defence should create an AI institute, something vaguely analogous to a Los Alamos National Laboratories or a Sandia National Laboratories but focused on AI technology. That was a recommendation made a year ago. Well, in January of 2018, China announced that they were creating the AI institute and their initial funding level was $2.1B, and the American government has yet to produce an AI institute or anything approaching a policy towards that. We are past due and it is extremely frustrating to watch our recommendations be implemented by China faster than in the West. Perhaps most worrisome of all is the fact that China recognises the essential disruptive nature of AI technology.

If you recall, the USA's third offset strategy said that we were going to use AI and autonomy technology to maintain America's leading edge in military technology. China's national strategy is a rebuttal to this document. It says that instead, AI is a leapfrog technology, meaning that,

because of AI technology, we do not need to invent or to match you in many of the sources of your existing military technology advantages. Perhaps China will decide that they don't need nuclear-powered aircraft carriers because of where they see autonomous drone technology going or maybe they don't need advanced 6th-generation fighter technology because of where AI technology and surveillance and reconnaissance will take them in long range precision strike.

That's what they mean by a leapfrog technology is that, instead of matching you in your existing military capabilities, we will develop alternative cheaper routes that make those advantages irrelevant and perhaps even weights that hold you down. Think again of the Kodak example. Every time you're selling a digital camera, you're reducing global demand for film technology, which means that, as you get stronger, you make your competitor that much more uncompetitive, that their strength that they have in film technology is the weight that holds them down as they try and pivot to digital camera technology.

The same is true for artificial intelligence technology. The West has extraordinary advantages and a host of military technology domains but, if we focus on our existing advantages, we will prioritise readiness and neglect modernisation such that our old technologies will weigh us down. The most recent defence budget of the United States was a readiness-focused budget overwhelmingly. It had goals such as a greater than 300 ship US Navy, and to me, this was an extraordinary mistake because it would be equivalent to Kodak in 1990 announcing that they were going to build a much larger film processing plant or film manufacturing plant, doubling down on the state-of-the-art technology of this era while neglecting to realise that the technological trends already ongoing are likely to make those advantages questionable, or perhaps even disadvantageous.

Think, for example, of German and steel companies in the 1960s. They out-competed American companies basically because they had been blown up in World War II. After World War II, they had the opportunity to design their steel industry from a clean sheet whereas the United States saw innovation from a, "How do we take our existing steel factories and make them better?" Germany and Japan had the luxury of being behind, the luxury of saying, "If we were starting a steel industry from scratch, what would we do?" Then, they did it and it was extremely painful for the United States steel industry as they lost their competitive advantage. China has a similar advantage of being behind. They do not have 13 nuclear powered aircraft carriers. They do not have the F35 or the F22, the most advanced fighters in the world, but because they are behind, they have the luxury of designing from a clean sheet and questioning whether those capabilities will even be relevant in the near future.

With AI, I suspect strongly that many of the capabilities from which the United States and its allies draw their key advantages today will not be relevant in the enduring future. Now, I want to bring this back to disruptive innovation theory, and Professor Clay Christensen, the father of disruptive innovation theory does have a prescription for what organisations should do when they're facing this type of challenge. The first part is that you cannot necessarily trust your existing organisations to navigate this challenge. Perhaps this sounds difficult, but I would remind you that, in 1942, Head of the US Army Horse Cavalry wrote a very lengthy memo to the army Chief of Staff arguing for the urgent need to increase spending on a horse cavalry.

In general, people who have organisations that are dedicated to using a military technology will be the last people to realise that that technology is increasingly irrelevant. Instead, what Professor Christens recommends is that you set up a new organisation that is restricted to making use of only the disruptive innovations and tell them to fight like hell to put the existing company out of

business. This would be the equivalent of Kodak setting up a new group that was only allowed to focus on digital camera technology and the CEO saying, "I realise that you're going to hurt my existing business. That's the point. I want you to do that because that's what will make us an enduring and surviving organisation going forward."

The militaries of the west need to replicate this insight. They need to create AI-first organisations that can acknowledge that some of what they're going to do is going to, in the short term, make the armed forces that they support weaker by exposing vulnerabilities in the systems upon which they rely. But if they succeed in exposing these vulnerabilities, well then, you'll be ahead in the disruptive innovation. You'll get to the future first and you can scale the new technologies and tactics as you divest the old, and, if these new organisations fail, great. Then you know that your capabilities are future-proof at least for now and at least until the next disruptive innovation. This is the true insight of disruptive innovation: that you must disrupt yourself or be disrupted.

In the public sector, this is extremely difficult. In the US private sector, we believe that our entrepreneurial ecosystem is the best at harvesting disrupted innovation because we are willing to let companies go out of business.

This is the nature of creative destruction: that we allow the capitalist ecosystem to tell us what the right way is to run our economy. But in the public sector, this is extraordinarily difficult, both because we have missions to execute today that are often life or death in stakes, but also because the organisations are mandated by congress and many of the technologies upon which US National Security depends are underpinned by a 50-state strategy, which is to say their manufacturing and servicing is designed for a political outcome maximising support in the United States legislature, not for a military technology outcome.

In a sense, our existing military technology ecosystem is designed to prevent creative destruction and, if we allow this, then it's almost certain that we will be overtaken by other military powers that are willing to deal with these trade-offs and are willing to go to the future first. That does it for me. As I said before, this was a high-risk, high-reward strategy working from just a scratch, but I want to say that these are the real stakes of artificial intelligence technology, that it really is the future of military power and it does demand reform across military organisations in the tactics, strategies, resources, processes and priorities that they use to set themselves up for failure or for victory. The stakes could not be higher and it's very important that we get it right.

Thank you.

Algorithmic Warfare Cell

Lieutenant General John Shanahan

Good morning. I am not an innovator or a disruptive thinker. When this book is published someday, rest assured, I will not rate my own chapter. My picture will not grace its pages. You will not find my name in the index. I don't even expect to be buried in some obscure footnote reference. And as far as operational air power relevance, I started my flying career in the venerable F-4D Phantom 33 years ago, and it's almost been seven years since my last operational flying mission in the RC-135 Rivet Joint, an airframe that came off the production line five years before the F-4D, believe it or not! So, what exactly qualifies me to stand in front of this august audience to talk about air power in a disruptive world? That is, in this era of innovation that is unfolding so rapidly that it could be both unsettling and continually chaotic. A fair question, to which I will return shortly with an answer.

Well, good morning, and first and foremost, let me thank the people who organised this conference, especially the RAAF Air Power Development Centre for graciously inviting me to speak. I am honoured by the opportunity to join you. I am hopeful that you will find that my remarks not only complement what you already heard from Dr Bell and Greg Allen, but also what you hear from several of the remaining speakers this afternoon, and I take Greg's point. I have never considered Project Maven to be crappy, but it's actually a good term, because what I'm going to talk to you about is so new, so different, so unfolding, that it's a fair characterisation of what we have now versus where we're trying to go.

I'll begin with a few thoughts on innovation and disruptive thinking in general,, then pivot to the proposal, or to the project I'm currently leading: the Algorithmic Warfare Cross-Functional Team, also known as Project Maven. Then Deputy Secretary of Defence, Robert Work, directed the Under Secretary of Defence for Intelligence to stand up this project in April 2017, and he then told me to run it. Secretary Work's initial guidance to us, which has not changed since, was to serve as an artificial intelligence pilot project for the US Department of Defence, integrating artificial intelligence with machine learning at speed and at scale, to augment, accelerate and automate full-motion video exploitation, or PED, for unmanned aerial systems. And even more ambitiously, to act as a pathfinder, the spark that ignites the flame front of AI across DoD. And I'll come back to Maven shortly.

Everyone views innovation a little bit differently. In deference to our location and a nod to Colonel Scott Gills, I will use surfing analogies to describe how I think about these central elements of innovation and disruptive thinking. This depicts how many of us spend our time: sitting on a board in calm waters, soaking up the sun, and worrying about little more than where to enjoy a cold libation that evening. Innovation; what innovation? This slide illustrates life for almost everyone else that wasn't already binned to that first category: that feeling you get when you miss the innovation wave entirely. A very small percentage of people, the innovators and disruptors, are up on the wave well before anyone else even knows where the hot spots are. And of course, for those same people, this final picture is as relevant to innovation as the preceding one. If there's a common thread in the life stories of all renowned innovators throughout history, it is that failure is inevitable. Yet, for the real innovators and disruptors, it is also never final.

Now, a little word association. Was innovation the first word that popped into anybody's mind? If so, I hear there is some medical assistance very nearby. Yet, it's there and not only in those organisations that are charted specifically as innovation hubs, such as Defence Innovation Unit Experimental, or DIUX, the strategic capabilities office, the Joint Rapid Acquisition Cell, and the US Military Services Rapid Capability Offices. There are plenty of innovators and disruptive thinkers sprinkled throughout the Pentagon, and many more across the military services. However, far more often than not, they are beaten back by the great tidal wave of bureaucracy and, unlike the surfing analogy I used a little bit earlier, once that bureaucratic bomb buries you, a real mullering as it were; there are few, if any, opportunities to get back up on the board.

I recently visited both Silicon Valley and New York City; the former, to learn a little bit more about AI from start-up vendors and some of the biggest names in data; the latter, to learn about how a few renowned financial institutions are integrating AI into their business models. My aide at the time, an army reserve major, accompanied me on both trips, and I thought it worthwhile to relay the feedback that he passed on to me after them: "One of the things that struck me the most was the professionalism and competency of these individuals." These individuals and firms were the ultimate expression of capitalism, the perennial game of survival of the fittest. If they don't perform, if they don't excel, they're gone, fired in a heartbeat. If they succeed, they're rewarded handsomely. Last year's performance matters far less than today's. This stark difference in culture is critically important. I remember returning from our Silicon Valley trip and thinking if we could simply capture 10% of that energy, enthusiasm and passion from those places, and bring it to the Pentagon, then we could solve any problem, no matter how complex.

It's not a matter of funding. It's not a matter of manpower. It's culture. Certainly consequences should matter more, just as companies from the smallest start-ups to the biggest data companies encounter consequences in the marketplace if they don't perform, we face consequences for lack of performance in the great game of strategic competition, with our adversaries intent on seeing our demise. But somehow, this does not provoke frenetic, frantic, all-nighters to ensure every nut and bolt of an organisation is ready, without a shadow of a doubt, to encounter and defeat a hostile, aggressive enemy. Why? How do you combine the best of capitalism, to provoke a survival instinct, passion, excellence, and dedication, with the best qualities of public service and national mission?"

That's a terrific question, even if somewhat rhetorical unfortunately, and drives right to the heart of what innovation is all about. Which brings me to the Algorithmic Warfare Cross-Functional Team, or Project Maven. In classic innovation fashion, we did not start with a disruptive solution in search of a problem. We began our Maven journey in late 2016. We faced a well-defined, discreet, tangible dilemma. One of such magnitude and duration, that it could not possibly be solved without disruption or innovation. For lack of a better phrase, we were facing an insurmountable challenge—the rapid growth in tactical unmanned aerial systems and medium-altitude remotely piloted aircraft, along with dramatic improvements in sensor quality causing intelligence analysts to be inundated with full-motion video without the commensurate capacity to exploit it all, or even a substantial portion of it, leading to this avalanche of data. Analysts were spending far too much time performing far too many tasks by rote. There was simply no way we were going to be able to buy our way out of the problem by adding more and more analysts.

Indeed, we recognised from the very start that adding more people as the preferred solution to this so-called success catastrophe would only delay the inevitable deep sweeping cultural changes

needed to accelerate adoption of new technologies such as artificial intelligence and deep learning across the intelligence community. Led by Marine Corps Colonel, Drew Cukor, the initial Maven team, a small, small handful of likeminded innovators and disruptors, with a deep reservoir of sheer grit and determination, began a journey of discovery to understand what was in the realm of the possible in terms of automating video exploitation.

As this slide shows, we soon appreciated that the only way to gain the returns on investment that we were looking for, to get to true automation, not merely 2x, not merely 5x, but 50x order of magnitude, was to embrace AI and machine learning and, specifically, computer vision. In surveying the US Department of Defence, primarily across the research laboratories, we discovered that it wasn't only a small handful of projects that were dedicated to AI and computer vision. All small-scale, with limited funding, limited sources of data, and limited compute power, and most importantly to us, not delivering capabilities to a war fighter in under five years.

Drew and his number two, Lieutenant Colonel, Joe Larson another Marine Corps colonel incidentally), then ventured forth both into academia and industry to better understand the state of the art in AI. Between DIUX's advice, multiple visits to some of the best AI universities in the United States, namely MIT, Berkeley, Stanford, Carnegie Mellon, and more, talking with a wide variety of vendors from Silicon Valley start-ups to the biggest names in the business, and absorbing reams of information from extant tech literature and other open-source platforms concerning AI, we found that there was, indeed, a solution to our problem: computer vision. Yet, at the same time, it had become immediately clear to us that no institutional architecture or pipeline existed anywhere in the Department of Defence to turn our vision into a fielded AI solution, never mind at speed and at scale.

We then worked with a start-up vendor on a pilot project, to demonstrate how computer vision could provide the return on investment that we needed for full-motion video exploitation. That is, by using a commercial vendor to develop an algorithm that could detect, classify and track a number of different classes of objects without human intervention. Our sole intent was to give back time to analysts so they could take advantage of the cognitive skills for which they were trained. Upon briefing this pilot project to Deputy Secretary of Defence, Bob Work last April, he immediately directed us to stand up the Algorithmic Warfare Cross-Functional Team with the overarching guidance that is shown here on the slide. And while that name is, admittedly, a little bit of a mouthful, Secretary Work envisioned a future in which algorithms would be fighting other algorithms; competing against other algorithms. And since that name does not roll off the tongue so easily, you'll also hear it called Project Maven.

And then we were off to the races. And in classic start-up fashion, our mantra from the very beginning was to start small, stay focused, and win early. However, we also quickly grasped that the magnitude of the work ahead was daunting. With the benefit of a lot of sage counsel from DIUX, think tanks, academia and industry, Drew and the team began to design the process required to field an operationally relevant algorithm. Beginning with data acquisition, to data wrangling and preparation, data labelling, algorithm development, algorithm test, validation and evaluation, integration into existing exploitation systems—systems, incidentally, that were never designed with AI in mind—and finally leading to algorithm fielding, optimisation and refinement, with user engagement throughout the entire cycle. We took a Darwinian approach to algorithm development, putting a handful of commercial companies on contract; commercial companies as we understood from the start that the algorithms that we really need for computer vision,

did not exist in the government. Then they all got access to the same data, and we structured the contract with a system of gates to evaluate performance at multiple stages along the way, eventually selecting a best-of-breed algorithm.

While I am the first to admit we made a number of mistakes along the way, we were, after all, ploughing completely new ground in the Department. Within eight months of standing up, within six months of getting our first funding, we fielded an algorithm at an operational site. For those of you in the audience who are not as familiar with our Department of Defence's acquisition processes, trust me when I assert that that is light speed. Using a typical innovation, multi-sprint approach, we continue to field tactical UIS algorithms today, expanding to more and more sites, while also now refining algorithms for medium altitude RPAs. Later this summer, we transitioned to high-altitude ISR platforms, with that same sprint methodology, simultaneously taking on a number of equally pressing requirements across the Defence Intelligence Enterprise that are right for AI and machine learning, such as captured enemy material, collection management, and target systems analyses, followed by building a plan for placing algorithms directly onto platforms and sensors.

In standard innovation fashion, it should not surprise you that our biggest breakthroughs are not emanating from initial fielding of the algorithms themselves. Instead, while admittedly still very early in the fielding process, we are seeing the most significant changes to processes, procedures and user experience as a result of direct user engagement. In other words, from there come the improvements demanded by operators and analysts during initial algorithm development, all the way through the fielding process. These include the innovative combination of the algorithms with other capabilities, such as geo-registration, and the conversion of algorithm detections from the full-motion video that then become icons on a map display. Also involved are creative applications of metadata, designed to improve the ability of centre operators and Intel analysts to do their jobs more effectively and efficiently. Now, two quick slides that show a few examples of what's in the realm of the possible, directly based on the feedback from the users at the first pilot sites.

The more we learn about the importance of metadata and the real power of downstream analytics, the more we envision a future, likely sooner rather than later, in which the video will become the least important part of the exploitation analytic equation; it is the metadata that matters the most. We are now developing solutions to ensure that such data is available not only locally to the analysts and operators, but globally as well. All of this is designed to allow analysts to provide all-important context beyond staring at video screens for hours and hours on end, or to put another way, thinking well beyond the 'what', to spend much more time on the 'why'.

As Fei-Fei Li said in a recent New York Times Op-Ed "humans are still best suited for the creative, intellectual and emotional roles. Let the machines do the rest." More importantly, we are still in the invention phase of Project Maven; real innovation is at least a year away. Maven was not designed as a technical solution to a technical problem, but an operational solution to an operational problem. For that reason, ultimately, I am the last person who will determine if Project Maven is deemed to be a success. That final judgment will rest squarely in the hands of the operators and analysts in the field. It is our duty to do everything possible to allow them to succeed. This implies engaging with them early and often, well after the fielding has been first downrange.

Innovation and disruption in case law are explicit. We fully expect that how operators and analysts use AI and ML capabilities a year or two from now, will be a far, far cry from what we anticipated when we first handed down the technology.

So, I'll now return to the question I posed at the beginning. Namely, if I am neither a wizard of innovation nor a Boydian disruptor, what do I have to offer to this all-important theme of air power in a disruptive world? This simply is to underscore the essential role that senior leaders must play in supporting innovation and disruption by recognising, encouraging, cajoling, shielding, and protecting the disruptors and the innovators; providing complete commitment and top cover to them; fighting for resources on their behalf; challenging the team, its facts, assumptions, risk, cost data, milestones; and in return, being challenged by them. My role also means accepting the inevitable false starts, missteps, dead ends, and mistakes; fully understanding and communicating all those projected risks to other senior leaders in the Department, risks that must be informed, substantiated, and balanced; inspiring the Mavenites, but in my case, more often being inspired by them; and to me personally, holding both the team and myself accountable, and knowing just how much I do not know already, and I do not yet understand, but I'm always willing to learn.

Put another way, as I expect everyone in this audience understands very well: while the innovation success formula is hardly as complex as the Schrodinger equation, it also does not comprise just a single variable on the left-hand side of the equal sign. While we're only now just coming up on a year into Project Maven, we understand very well the multiple variables that are in play that drive success of this disruptive project. And nothing on this slide would really surprise anybody in this audience: the Department of Defence is not a commercial for-profit company. It is an incredibly complex, highly bureaucratic, large organisation. Hard as it might be for some people to believe, very little happens simply because one person says so, no matter how many stars are on their shoulder, or their political pedigree. What a small, agile disruptive team can achieve in private industry, almost overnight, just does not translate well in the five sides of the Pentagon, where bureaucratic ***jiu jitsu*** is sometimes treated as an Olympic event. Innovation and disruption rely extensively on full-throated support from every layer of the Pentagon wedding cake, from the bottom all the way to the very top.

I am fortunate to be the beneficiary of one of those rare moments in a career when exactly the right combination of people came together in exactly the right place at exactly the right time. There are elements of serendipity in this. There are elements of design. To be honest with you, I'm not sure that I entirely yet understand the percentage of each, but it's okay, because it works, and it works really well.

To that end, Colonel Cukor and the members of his small team, growing from only five people at the very beginning of this project to no more than 15 people right now, share most of the same DNA, traits that should strike the right chords with this audience. First and most importantly, a shared vision about the existential importance of AI to the military. Followed closely by passion about their work; prototype warfare attitudes, fertile febrile imaginations, a willingness to work hard; really, really hard; constantly challenging orthodoxy; being tenacious and uncompromising, even ruthless in pursuing objectives. Constant friction begets evermore traction.

As much as anything else, Maven is chartered to help catalyse the creation of an AI-ready culture across the Department of Defence, by impelling change at the speed of operational relevance..

Every single person in the Maven team shares a vision of the importance and far reaching implications of human-machine and machine-to-machine teaming, not only for drones, not

only for other projects across the intelligence enterprise, but extending across every aspect of the military. And in keeping with the surfing theme, one of Maven's most important legacies will be the algorithmic warfare pipeline we have built and are constantly refining: a repeatable, disciplined, rigorous end-to-end process. This is nothing more than a very simplified version of the algorithmic warfare pipeline: Maven 1.0. To be honest with you, I can't wait to see what version 5.0 looks like, and how quickly it gets here.

We will continue to take on intelligent projects well beyond FMV exploitation, automation for unmanned aerial systems, leading some of them, but more and more frequently, serving to enable the success of others, probably in the military services more often than not, but also our combatant commands. Relying on a centralised direction, decentralised operations approach to AI across the Department. We may have a decision somewhere in the next few months, about how this will be organised across the entire Department, to take into account the needs well beyond the intelligence enterprise, perhaps resulting in the creation of something along the lines of a joint AI centre, or perhaps a joint program office. That remains to be determined. And, given the absolute centrality of data and metadata to everything related to AI, we see that there'll also have to be an accompanying joint data-clearing house to handle the critical elements on the front-end of that pipeline.

We are also striving to revitalise a triangular relationship between the military, industry and academia, returning to that same kind of deep collaboration on common national security problems that was critically important to sparking innovation in the United States in the 1950's; which, by the way, led directly to what we see today: this explosion of innovation and disruption in this data-driven age.

After the initial visceral recoil inherent in losing to an unemotional, cold, calculating, unblinking machine that was powered by an artificial intelligence algorithm, world champions Garry Kasparov, Lee Sedol and (25:03) all reached the same conclusion: it is not the grandmaster or the algorithm; it is the grandmaster and the algorithm, working together, that will forever result in the greatest progress in the shortest amount of time. So, it will be in the military, in every domain from subsurface to space, and throughout the electromagnetic spectrum.

Like a lawyer making closing arguments to a jury, I want to convince you beyond any reasonable doubt that artificial intelligence will forever change the character of warfare. It will require reinventing almost everything, from how we recruit, train, and retain, to tactics, techniques, and procedures, to how we will design, develop, field, and sustain weapon systems. To that latter point, from now on every military weapon system, or C4ISR capability, must have some sort of AI baked in from the very start to include an enterprise architecture that is designed to optimise algorithmic warfare.

Colonel Cukor and I have even had fairly spirited debates about whether the introduction of AI military-wide will actually change the very nature of war. I'm not there yet, but he keeps chipping away at me, and the more we think about AI, the more we realise that it is something we really have to start thinking about.

In closing, a new generation of people, some of whom are in this audience right now, probably in the back row like all young officers, will look at AI entirely differently than people like me! It took 40 years to journey from this to this. When it comes to AI and the future of DoD algorithms—when translating to Maven, the type of leap that's represented by the differences between Pong

and Dota 2—we may well soon begin measuring the same kinds of exponential advantages in months and maybe a year or two, rather than in four decades at a time.

And finally, as incredibly challenging as the Maven journey has been so far, when looking back at it through the lens of history, with the benefit of let's say a decade of hindsight, I expect our FMV project will be viewed as basic, perhaps even trivial. We have a long way to go, however, before that happens. To me, the future is bright. I do remain an optimist. But we have to seize the moment together. This is not one country; these are all countries working together. And if we don't do that—and this is where I'll go right where Greg left off, and where I'll leave off—if we don't do that, and we really don't embrace this, we will risk being on the wrong end of an algorithm ourselves. And we don't want to be there.

Thank you very much.

The Disruptive World and the Integrated Force: Achieving Readiness through LVC

Jennifer McArdle

Good afternoon, everyone. First, I'd like to thank the Royal Australian Air Force for inviting me to speak to this distinguished audience. I realise that I'm the last one standing between you and lunch, so I'll do my best to hold your attention for the next 30 minutes. What I've been asked to do today is to talk about the integrated force and live, virtual and constructive training, which I realise is quite a mouthful, so I'll be referring to it as LVC.

On November 17, 2011, General Martin Dempsey, then Chairman of the US Joint Chiefs of Staff, asked a question. "What's after joint?" What he meant was how do we do a better job at integrating new aspects, rapidly evolving aspects of warfare like cyber or electronic? Six years later, the US Army answered with its multi-domain battle concept while, today, the US Air Force is finalising its concept of multi-domain command and control. To cut a long story short, what multi-domain battle seeks to do is move beyond Services as organising constructs, to instead harness joint experience to produce integrated effects though multiple domains: air, land, sea, space, and cyber.

So, this past June, speaking here in Canberra at Aspley, Vice Admiral Ray Griggs, the Vice Chief of the Defence Force, noted that joint was now a limiting descriptor and, while multi-domain struck him as a bit of a faddish concept, the key he noted to the future force is the integrated force, integrated at an organisational level as well as culturally and technically. He advocated for what he called a one-domain concept that moves away from Service and domain-level silos. Putting aside these debates over semantics, it's clear there's a sense that we need to work more seamlessly between Services and domains by focusing instead on the desired effects that one wants to bring to bear on an adversary rather than on a given Service or domain. Thinking along these lines should give war fighters and decision-makers increased options. Although multiplying our adversary's challenges, there's also a recognition that technology on its own will not be a panacea; that the way militaries choose to fight, seamlessly integrating kinetic and non-kinetic operations, will also influence the outcome on the battlefield. We need a truly integrated force across Service, domain and kinetic and non-kinetic operations.

In today's operating environment, such integration is necessary. Potential adversaries China, Russia, Iran and North Korea have invested heavily in a range of military capabilities with the intention of depriving the US, allies and coalition partners the capacity to project power into their near abroad. Labelled "anti-access area denial", these capabilities afford their owners a degree of strategic depth by raising the risk and cost of intervention. In tandem, these capabilities have provided cover for other more revisionist actions. Russia and China in particular have manifested an iridescent proclivity for grey-zone approaches or salami-slicing tactics that stay just below the threshold of armed conflict, but nevertheless have already insidiously changed the *status quo* in their respective regions.

Moreover, potential adversaries have recognised that conflict is not solely defined by the exchange of fires, but that shaping the information environment through lawfare, economic statecraft and information operations can also serve geopolitical ends. While these asymmetric strategies may

differ in their capabilities or tactics, they all rely heavily on cyber, electronic and information operations. Our militaries must be able to fight in and through an increasingly contested and complex battlespace and they must be able to bring those same cyber, electronic and information operations to bear as forced multipliers for more lethal effect. So, the question becomes; how should militaries fight as an integrated force in these contested environments? And then, how do you train for that?

LVC provides the environment necessary for more integrated training, all while providing a high-fidelity rendition of a military's current and future operating environment. There are three types of techniques militaries use for LVC. So, you've got live, real people operating in a real environment; virtual, real people operating in a simulated environment; and constructive, simulated people or equipment operating in a simulated environment. LVC entails linking live aircraft with manned simulators in the virtual world and computer-generated constructive forces. LVC is increasingly beneficial today because the live environment is not conducive to many of the training needs of the fifth-generation force; for instance, like the F-35 drone strike fighter. Live training ranges are spatially too restricted for fifth-generation training, and they often fail to produce realistic fifth-generation threat scenarios. There's also the perennial concern linked to inadvertently revealing the unique war-fighting attributes of fifth-generation platforms. And then, last but not least, the live environment fails to integrate with fidelity cyber, electronic and information operations.

So, of course nothing can replace the sensations driven from the dust, sweat and adrenaline of the live environment, but in some cases, however, it may well turn out that when preparing for the future contested and complex battlespace that the synthetic training environment may actually prove more realistic. Indeed, to truly achieve an integrated force along the lines of multi-domain or one-domain battle, or even Plan Jericho, for that matter, training will need to be increasingly pushed into the virtual and constructive environments.

I'm now going to try to spend the rest of my talk explaining why and the rest of my presentation's going to be structured in four parts. So, first, I'm going to discuss the need for military forces to train to fight in and through a contested environment saturated by adversary cyber and electronic operations. I'll also detail how the military and the defence industrial base can begin to conceptualise injecting cyber and electronic effects into the synthetic training environment. I'll then discuss why it's necessary for the military to train for offensive, integrated kinetic and non-kinetic operations, looking specifically at some of the challenges unique to integrating offensive cyber operations with more conventional operations. I'm going to detail some really interesting initial work that integrates kinetic and non-kinetic synthetic environments. I'm then going to switch over and look more broadly at today's information environment; in particular, how we're starting to see cyber and electronic operations converge with social media, big data, and artificial intelligence, alongside more traditional information operations, like psychological operations or military deception, to influence the information and cognitive dimensions of the battlespace. I'll talk a little bit about why training for these types of operations must occur synthetically and how the environment needs to evolve to provide the war fighter with that experiential learning prior to combat. Finally, I'll conclude by exploring how the synthetic training environment is uniquely suited for the military to experiment, to design new operating concepts and tactics, techniques and procedures for this future battlespace.

So, in December 2011, Iranian cyber warriors alleged that they hacked into an RQ170 stealth UAV operating near the Iran-Afghan border. Iranian cyber warriors claim they spoofed the UAV's

navigation control, sending it false GPS coordinates. They also claim they jammed the UAV's communications, forcing the system to autopilot mode, meaning it would have to rely on its GPS to return to its base in Afghanistan. If true, the false GPS coordinates fooled the RQ170 into thinking it was close to home, so it landed in Iranian territory. So, it's unclear in the open source literature whether Iran did conduct a cyber electronic attack on a stealth UAV. But unencrypted UAVs have been spoofed and their feeds have been intercepted in the past. However, regardless if this incident is true, what the RQ170 incident does indicate is that the cybersecurity of our military platforms and systems are of utmost importance. It seems self-evident that any complex system with high interconnectivity will have cybersecurity vulnerabilities. We all know that the same capabilities that give us a certain technological edge over certain key competitors also present unique cybersecurity risks. Military systems can fall prey to adversary cyber operations for the purposes of espionage, sabotage or subversion.

Information security professionals often refer to what they call the CIA triad. These practitioners work to ensure the C, confidentiality, I, integrity, and A, availability of data within a system. While this model's typically used to guide information security policy, it also provides a really useful starting point to start to extrapolate how adversaries might try to undermine military systems and platforms. Adversaries will work to undermine the confidentiality, integrity and availability of military platforms and their communications backbone. In combat, the network attacks the military will most likely face are availability threats, distributive denial of service, jamming. Enemies could also manipulate the micro-electronic supply chain or employ cyberattacks to sabotage communication networks or key weapons systems. The confidentiality of data on weapons system capabilities or vulnerabilities could be revealed via cyber espionage. By accessing command and control networks, adversaries could also glean intelligence on operational planning and decision-making. Finally, the integrity of system information could be compromised by spoofing or the insertion of false information. Synthetic training must evolve for these types of cyber-attacks, but how?

Exactly how a platform or system is disrupted by a cyber-attack depends of course on the details of that system. This requires a deep understanding of how that system works. For instance, how a SA400 surface-to-air missile works. But it also requires an understanding of how the system parameters are set and how that system fits into the broader network, and this understanding needs to evolve as the platform changes with each software update, each patch, each new interconnection, etc. Moreover, cyber exploits are evolving. They aren't static. They reflect the tacit knowledge learned by the hacking community. What they choose to target and how they have structured an exploit will have different effects on a system. So, it may be impossible to model all the possible effects of a computer network attack on a system. However, that doesn't mean that developing a suite of simulated cyber injects that may be slightly divorced from reality is not helpful. Given the number of ways that a cyber attack can impact a system, the goal should be to get the trainee to troubleshoot a diverse range of effects and creatively identify ways to maintain mission assurance despite the attack. How should a pilot react if their GPS coordinates no longer seem to reflect reality? What should they do when the primary interface between their aircraft and their weapons is sabotaged? What if their fire control radar no longer seems … the information on the fire control radar does not reflect previous information of the mission? In some cases, the pilot may need to turn back. In other cases, they could troubleshoot and carry on

with the mission. They need to be trained to each of these ends. We need to start to think about how we can evolve our suite of synthetic training options to include these scenarios and others.

On September 6 2007, Israeli F15 Eagles and F16 Falcons bombed a North Korean-designed nuclear facility in Syria. Even though these aircraft are far from stealthy, they were invisible to Syria's Russian-built defence network. So, what happened? The images on Syria's radar screens weren't real. They depicted what the Israeli military had put there through cyber means and while there are various theories on how Israel may have penetrated Syria's air defence network, one thing is clear: the Israeli Air Force had successfully and skilfully integrated kinetic and non-kinetic operations. More recently, from late 2014 through 2016, Russian malware was covertly implanted in a legitimate Android application developed for the Ukrainian artillery. The original application used by over 9000 Ukrainian artillery personnel enabled artillery forces to process targeting data for the Soviet-era D30 Howitzer. The deployment of the malware likely facilitated superior Russian reconnaissance and targeting of Ukrainian artillery units. Some folks have assessed that between 15 and 20% of the Ukrainian D30 inventory has since been lost in combat operations. So, it's obvious that cyber and electronic operations can be used as a force multiplier or support function in conflict, but that's easier said than done. Current LVC training for cyber operators tends to focus entirely on the cyber aspect of our operations and it often ignores the broader picture, placing it at odds with the realities of cyber support on the battlefield.

Conventional war fighters tend to see cyber as a strategic capability rather than something that can also be applied tactically as part of a range of mission effects. Few training opportunities, if any, exist for the conventional war fighter to gain a broader understanding of how it can best leverage cyber capabilities at the tactical or operational level. The US Air Force knows that if its ambition is to have a multi-domain force, they need to produce airmen that know how to combine air, space and cyber together for more lethal effect, yet a gulf exists between those cyber warriors who are assigned to cyber protection teams and those who are assigned to support conventional forces as part of cyber mission teams. Some of the stuff we've seen during recent Red Flags do show some promise, however much more needs to be done. New training and tools need to be developed to support this type of training. So, for instance, one could imagine a scenario where a cyber combat mission team has gained access to an adversary's air operation centre. They now can understand how an adversary plans to deploy air power in a given phase of operations. If the cyber combat missions team connection is via fibreoptic cable, it's in their interest to ensure that friendly forces do not damage that cable during operations. However, that same fibreoptic cable could run across a bridge that friendly forces seek to deny to an adversary. Coordination and integration across the force needs to take place as bombing that bridge could deny the cyber combat mission team vital mission intelligence.

So, however, perhaps more importantly than just designing combined cyber kinetic scenarios, war fighters much better understand the strengths and weaknesses that cyber brings to the fight and this is something that could be developed through integrated synthetic training. Cyber brings unique attributes that differ significantly from more conventional weapons. For example, the timing and sequencing of non-kinetic and kinetic attacks can be challenging. Targets cannot necessarily be hit at a moment's notice. Cyber operators often take months or even years to work through the cyber kill chain, from reconnaissance to exploit development, delivery, vulnerability exploitation, malware installation, remote manipulation to finally achieving their objectives. Plus, obviously the more critical system is to an adversary the more likely it is highly protected and

the more difficult it will be to penetrate. However, once the system is penetrated, the effects of a cyberattack can be near instantaneous, requiring rapid reaction on the part of more conventional war fighters so that everything is nicely synchronised.

Secondly, war fighters and commanders need to know what a cyber attack will do to a target. In the US, the Department of Defence has developed joint munitions effectiveness manuals which indicate the characteristics and size of the kinetic weapons to that nation. The effect of a cyberattack, unlike a kinetic weapon, isn't dependent on the weapon or malware itself; its effects are based on the system that it is targeting. Therefore, it's likely impossible that one can precisely know the exact effects of a cyberattack on a system. Instead, what is required is the ability to quickly do battle damage assessment, feeding that information back to the commander or war fighter for their subsequent action or decision. Furthermore, combat and cyberspace can be a rapid measure/counter-measure game. The effect of a cyberattack isn't necessarily permanent. Target system administrators can restore system functionality integrity. Therefore, it's not enough to just integrate non-kinetic and kinetic effects. Cyber and electronic operations must be synchronised and layered in time and space.

So, what is needed is a sandbox, a place where war fighters and commanders can experiment, a place where they can start to imagine what these integrated operations look like. We need to start to identify ways where we can integrate cyber simulators or ranges with kinetic simulators allowing the effects in one environment to change the environment or the computer-generated forces in the other. And so, this type of integration has actually already been demonstrated. In 2016 at its (18:50Expanded Warrior), a cyber kinetic effects integrator was showcased. A team at Carnegie Melon developed a program that bridged their cyber synthetic environment with a third party kinetic mission training program. The program would detect changes in the cyber environment, like for instance the triggering of an alarm, which would then be reflected in the kinetic mission training program. Carnegie modelled all the systems involved in the mission so that war fighters could creatively determine the best path to success. The synthetic nature of the environment allowed it to be continuously reset so that teams could develop and test new operational concepts as well as tactics, techniques and procedures.

So, I think the time is right for Australia to start thinking more about this, particularly with the recent inauguration of Defence SIGINT and Cyber Command. How can the Australian Defence Force start to integrate their new cyber command with conventional war fighters? The use of cyber and electronic operations extends beyond the sabotage, subversion or espionage of platforms and systems. The information environment has changed and adversaries have increasingly sought to level the playing field through the adept use of information. At its core, strategy is about the human mind. It's about the ability to bend an adversary to your will. Information operations employ tools, any tool, to shape the information environment, whether that's undermining adversary decision-making or creating conditions for various entities to make decisions that benefit friendly force missions. From the use of cyber and information operations and in the Russo George Award, to the blending of electronic information and cyber operations in Ukraine, Russia is preparing to fight and win harshly through shaping the information environment.

So, to our non-state adversaries. For example, during Operation Valhalla in 2006, US Special Forces engaged a Jaish al-Mahdi death squad. They killed 16, captured 17, destroyed a weapons cache and rescued a hostage. Shortly after US Special Forces had left the site, Jaish al-Mahdi fighters returned and they rearranged their comrades on prayer mats, making it look like they

had been slaughtered while praying. They released press releases of the alleged atrocity in English and Arabic on social media and it took the US three days to respond with their story, and by that point the success of their mission had been undermined.

In some cases, training for information operations can be done in a live environment; for instance, Youssef's use of an EC130J aircraft to broadcast their own signal over radio or television, or to override broadcast stations on the ground. Likewise, an exercise viking, which simulates training for peace operations and crisis management, a media gaming cell injects different types of news into the scenario, forcing the participants to manage media response. However, in other instances, when cyber, electronic, artificial intelligence, bots may be involved, the live and training environment will fail to mimic with fidelity the information environment. Moreover, the use of those capabilities in the live environment may risk revealing them to ever-curious adversaries. While the integration of cyber and electronic effects into LVC training is still in its infancy, information operations are routinely discounted or underutilised in training and this is surprising, as information operations have historically been a key component of integrated operations and they will remain so in the future. Indeed, the need for the military to shape the information space is not new. During World War II, allies mounted an elaborate deception and misinformation campaign, causing German attention to be diverted from the beaches of Normandy to Norway and the Pas de Calais. Four years earlier, the Germans had themselves misled the allies, causing them to concentrate their troops in northern France on the Belgian border rather than in the Ardennes, prior to Germany's Blitzkrieg offensive through the forest.

More recently, we have seen operations live-tweeted in real time by unwitting civilian observers. In 2011, a Pakistani live-tweeted the US raid on Osama bin Laden's compound in Abbottabad. While his tweets had no operational impact, one should wonder what the operational impact of that could have been today now that countries have much more exquisite social media data mining capabilities. What would have happened if the ISI, the Pakistani and Military Intelligence Service, had caught wind of the ongoing operation in real time? Information operations exclusion or marginalisation in LVC exercises can be often explained by their difficulty in simulating the effects over the exercise's time period. Moreover, when one starts to include military deception, psychological operations, public affairs, electronic warfare and cyber, the modelling and simulation challenge grows exponentially. How do you model the complexities of the physical, technical and cognitive dimensions of the battlespace? We need to start working towards this future. We need to start to identify ways our adversaries plan to use information operations in battle so that we can accurately model those for the war fighter. How will we and our adversaries use information operations for psychological warfare, command and control warfare, denial and deception?

So, there are some interesting opportunities emerging for synthetic information operations training. Indeed, virtual training environments have started to emerge that emulate social media. These environments could be used to train intelligence officers, but they could also be used to train war fighters like cyber information warriors to find and identify esoteric pieces of information that may actually have an impact on mission assurance. The potential for these types of training environments is immense as they could be used to experiment and train for psychological operations, intelligence gathering and public affairs. Training goal-dependent, integrating these types of environments with other traditional platform-based synthetic training environments could provide multiple trainees with a deeper understanding of how the information environment

may impact mission assurance or how they can leverage information operations for more lethal effect. Developing interfaces that bridge these environments, propagating effects across these environments, would provide war fighters a test bed for information operations prior to the crucible of combat.

So, according to the Department of Defence's military dictionary, readiness is the ability of military forces to fight and meet the demands of assigned missions. Moving beyond this somewhat broad definition, readiness at its core depends on the articulation of a coherent strategy. The military must describe what it must be ready for, when it must be ready and what components of a forestructure should be maintained in a state of readiness. If that's not challenging enough, Defence players must then decide what inputs to readiness personnel, equipment, sustainment and training should be allocated to achieve those ends. Readiness requires not just a trained force, but a trained force that can meet the strategic and operational requirements of future wars. LVC is not simply a training platform; it's also a tool for innovation and experimentation. New operational concepts, doctrines, technologies and integrated force structures can be tested in virtual worlds, virtual worlds that can evolve autonomously to reflect changing requirements. LVC provides the environment to experiment, potentially fail, regroup and adopt innovation before the first shot is fired or the first weapon is deployed. Achieving a truly integrated force that breaks down Service and domain-level silos should not be considered a finite objective, but an ongoing pursuit, a moving target as warfare evolves and forces us to innovate. An integrated force should be intrinsically tied to readiness. We need to experiment and then develop synergy across the force through realistic and repetitive training.

As the Australian defence Force begins to conceptualise how they can best integrate cyber electronic and information effects, particularly with the recent inauguration of the new Defence SIGINT and Cyber Command, LVC should provide a path forward and with that, I think I'll end there. So, thank you very much.

The Human-Machine Interface: Operational Decision-Making

JD McCreary

So, it's been a pretty good two days. And second day, post lunch, that's a challenge in itself. You'll see on my slides there's, I think, there's goodness in the fact that there's not gonna be a tremendous amount of new information in the bullets, but what I hope to do is actually connect the dots and talk a little bit about why. Why…are we in a competition? Does it matter? How do we question our assumptions? And how do we actually kind of come up with a game plan that takes us to where and what's AI doing for us? How do we expect to engage in combat? Are we in combat right now? And how can we change our thinking?

So, there's a lot of Sun Zu quotes that you could throw up throughout this conference that have been really good. Both MINDEF and Cath talked about integrating the force and speed of decision. CJOPS also talked about speedy response. So I think speed is really important here. And AI naturally lends itself to the discussion of "How do I accelerate my decision cycles?" So I'm going to talk a lot about decision superiority. I'm going to talk a little bit from an operational perspective. I'll talk more operational perspective tomorrow at William's. The exciting part is there's so much to talk to about here, and so many examples and stories that we give. Fortunately, some of it's been covered. So I'll try and breeze through and actually make it through my nine or ten slides.

So, besides the decision space, there's the technologies. How do we mitigate that? How do we develop the trust? That's a big impediment. We've talked about driverless cars. We've talked about ethics. We're not all in the world playing by the same set of rules. So, our ethics could be handcuffs when our adversaries decide to go down a totally different path, and we'll talk a little bit about that. But how do we actually generate trust and transparency? Jennifer talked about LVC and cyber. And we talk a lot about how do we practise things that we don't understand? How do we actually take advantage of the enablers? And in the USA, we just added information as the seventh war-fighting function. What does that mean?

What does information warfare mean today that it didn't mean five or 10 years ago, because it does not refer just to the technology, but the way our digital natives out there in the back rows are thinking? And how do they interact with information and decision making, and visualise the battle space in ways we've never thought about before. And General Shanahan threw a slide up there and showed pong and showed DOTA 2. And if you looked at the bottom of that screen on DOTA 2, there were 15 other screens. For those of you that have kids that are digital natives and have tried to play Xbox games with them, they're smoking you because you're linearly progressing through your target sequence and the actions. They're in parallel absorbing 10 times the information that you are. And they're making different kinds of decisions.

So how do we actually take advantage of new ways of thinking and displaying what that man/machine interface looks like? Obviously, we've foot stopped the commercial investment. How do we best leverage that? How do we not try and go for the perfect? How do we make sure that we can stay up with the speed of software development and prototypes? So we've started hearing terms like "algorithmic warfare" and "prototyping warfare". What does that information mean,

particularly when we've got a military industrial complex, we've got headquarters, and we've got structure and organisation?

DGPERS and I were talking a lot about what are the human beings like that we want in our force that allow us to do this? And do they look like us? Do you ever want to interact with them, or do you want to use a virtual environment 'cause they don't want to interact with you?

What does that look like? How do we challenge the norms of the way we do business in anticipation of doing war, and build our mainstream profile as we talk to industry about what we want as our future kit building sets? How do we actually think through all that? And oh, by the way, this isn't a thought experiment. The others out there that we consider competitors are doing this. And they're investing hundreds of millions of dollars a year just in this area. I just read this morning that France is going to put a hundred million euro per year into AI to enhance air combat capabilities. That's a significant investment. Obviously, you're taking this fairly seriously. Will there be a human being in that loop or not? What does that look like? Obviously, the Russians full-out believe that whoever dominates AI is going to win the war. Hearing similar things in the past doesn't mean that it's wrong.

It was talked about "Replace a soldier in the battlefield, replace an airman in the cockpit". That probably makes a lot of people uncomfortable. No; people number one, first and foremost. Yes, but we need to use our people in the ways that are best for human beings and allow machines and software and algorithms and visualisation do what they're good at, and free us to be that cognitive additional piece that differentiates us from the machine. China? Obviously, we've talked about that. They've got a plan and they're moving out. China is unambiguous in its messaging to us about what they're planning on doing. So we don't need to guess. They are telling us. They also have the advantage of that military/civilian fusion and leveraging that for military applications.

AI for AI's sake; lots of advances are going to be made in cars and Internet and things, and lots of other capabilities. But there are people in countries that are set up to take advantage of those technologies and capabilities and inject them into their force much more easily than us. So, is this just a military discussion, or is this a whole government approach and what does it mean? And the question is, does this change the nature of combat? Does this change the nature of our military industrial complex, and how we interact at national security and our national economic profile? That is intertwined. And so, how do we best leverage that as our adversaries are?

What are the attributes of our future force design? If we think speedy decision, and I'll talk a little bit about that, how do we actually go about describing that so we can tell our academics, our industry, "This is what we need. This is what we're thinking". We don't necessarily know exactly how it's going to become manifest in our ships, planes, tanks, etc. But we know we need this kind of stuff. How do I buy a bucket of that? And are these the right attributes? Probably not. It's a good start, though. How do we actually expand? And again, several speakers have talked about being flooded with information. Actually, you're flooded with data. We're trying to generate information. We're trying to generate knowledge. We're trying to generate decision making. How do we go beyond just simply connecting things and making more data available?

And why do we do any of this anyway? Is this a luxury for us to say, "You know, eventually maybe we should bring in some AI. Maybe it will make some things better. Yeah, I got a lot of data, but you know what? Budget crunch! I need to bend metal. I need to put planes in the sky, subs underneath the water, etc, etc". This is the life blood of the future. You cannot just cut it because it's intangible. And I think that's another great point that Jennifer brought up: LVC is not just

about reps and sets 'cause I can't afford a range, or I need to hide a capability. It's also showing you what it takes to do an integrated force, what it takes to inject innovation of artificial intelligence into the future force, and what the value is.

Here's my decision making, running around with a piece of paper. And this is describing stuff I've done in the past. 3000 launches have to go out today. We gotta support sub con missions. We gotta support land missions. We gotta do counter ads. We gotta do XYZ, by running around with a piece of paper through the HEO cycle, and trying to put that plan together. Most people don't understand anyway 'cause it's non-kinetics and it doesn't go 'boom'. And I don't really understand it, so go off and make some of that stuff happen independent of kinetics. So certainly, we gotta bring this together. We have to.

Australia certainly is a great example of being force limited. You only have so many human beings. You've just introduced a new capability in the E18G Growler. Most of you don't know jack about electronic warfare or information operations, or any of that weird gooey stuff that brings things together, but I can't quantify. So how do you prove the value of multi-demand C2 battle management, data decision, decision superiority, artificial intelligence? How do you actually demonstrate that value so that you can go back to the bean counters and say, "I cannot do Jericho without this? I cannot do Australia integrated joint force without this". If I have to give up a ship or a sub or a couple of planes, how do I demonstrate the value?

Some of it is decision superiority. How do I measure the ability to...the blue loop is on the inside because I want a tighter, faster decision cycle than the adversary. And how do I keep that adversary's OODA loop outside mine? I orient, you know, OODA, observe, orient, decide, act. We spend a lot of time in the observe. We've talked about connecting things, bringing sensors, bringing lots of information in. We're really really good at observing and generating those inputs. Project Maven is trying to get after a piece of that and go, "I've got so much information. How do I actually make sense of it and do something with that?" So it's starting to get into the oriented phase. We do a lot of 'act'. Go bomb something. Go jam something. We know how to do that. But the key is decision making. Are we really that good, or do we think maybe we could be better at decision making? And how do I constantly measure how I'm doing in that OODA loop and challenging assumptions?

Because somebody wants to influence our OODA loop. And there's a couple of examples that I think I've heard mentioned, at least obliquely, in a couple of previous presentations. That is, if I give you too much information, you're never gonna get out of the orient phase. You won't be able to decide. So if I can just cram enough information and slow your decision cycle down, I can prevent you from executing. Or I can give you false information and shape your perception of the world. That is going to have the same type of effect. But we have to practise this. This is truly part of the art of war: understanding what the decision space is and how to exceed the other guy. And the other guys have already said AI matters to them. So again, we can't just pretend that this may or may not happen. We're at a critical moment. Some examples of that: we talk a lot about autonomous, and autonomous versus AI. And I thought Genevieve delivered a fantastic discussion. And she talks about the umbrella of artificial intelligence, which includes perception, machine learning, reasoning, code generation. There's a lot of stuff packed into that AI term.

Autonomy: probably a lot of people think of unmanned platforms as autonomy. Unmanned RPA; that's not autonomous. And there's degrees of autonomy. I'm going to send it out and I'm going to send to an away point. It's going to do its thing. That's a degree of autonomy. If I'm gonna send

out a swarm of UAVs that have ISR and EW payloads along with kinetic payloads, and they're gonna have a mission-planning module that gets uploaded to them with all the constraints of JOA, ROE, PID, resource management, digital commanders' intent, how do I tell it what I intend it to achieve. And then I let it loose just like I would a division of hornets. You know what your orders are. Don't crash into each other. Don't crash into somebody else; on time, on target, and then come back.

How do we make sure that we're doing that in autonomous weapons? There's huge ethics questions. Some of those ethics; I think we impose challenge on ourselves because we do autonomous weapons today. A torpedo is an autonomous weapon. Yes, a human was in the loop, made the decision, pressed the button, and then it's off. Ant it's going to find the target, and it's going to kill it. You may have not have been able to give it the exact coordinates for that target, whether that's an AMRAAM or a torpedo or an ageist weapons system, there's a full robo mode. There's a human decision maker in that process. But we do autonomous weapons. Now, the Russians are very interested in taking that further. They've made a statement right there. There's a position in front of the UN right now about lethal autonomous weapons systems and whether they're ethical and what the requirements are. Russia's pushed back on that, saying, "We haven't done enough of this. You can't tell me whether I can do this safely or not. So I'm going to proceed further. And I'm gonna generate data, and then we'll make decisions". So, they're moving forward whether we are willing to address that ethically or not.

They're not just doing this at a torpedo, an AMRAAM; they're putting robotocised battlefield platforms, and swarms of platforms, in multiple domains that work together to achieve effects. And they want to engage our manned forces with unmanned forces, and that changes the barrier to entry to war. It's a completely different set of calculus. They're going after LVC, models with 3D virtual environments, to actually do joint force optimisation. They're doing their ''tidfit' programming. They're doing their future con-ops planning in LVC with manned, unmanned, and artificial intelligence. That's a pretty big leap. We're barely thinking about LVC, just to do reps and sets as an integrated force. They're jumping to another level. Are we ready to jump to that level in terms of how do I exercise everything from individual platform execution up through force experimentation for con app TTP, up to force design; do I actually have the right force for the future and how do I test that out and evaluate that?

China's doing similar things. They're expanding the discussion to, really, how does AI help me make decisions? So they're going behind the autonomy and the swarming to AI in decision making. And you see at the bottom there, an article that came out about a week ago. They are putting AI on nuclear submarines to assist the captain in making those decisions. Now, decisions are relatively rudimentary. It's kind of still in that spacial manoeuvre. It's safe. This is where you want to be bathymetrically to meet weapons employment criteria. But that frees up that commander to be a tactical decision maker and not mired in the details, to understand what the options are and what are the risks of those options. We need to be progressing down that path, again, not just at our platform level, but at the AOC, at the JOC, at the force-design level. What are the inputs? How can we make better decisions about our force?

So, this ties into: we're getting into a little bit geekier part of the discussion. So, Gartner? Has anybody heard of Gartner? It's highly recommend, a fascinating read. And if you really are interested in to see how the trends are actually accelerating beyond anybody's wildest imagination, go back a few years and they're called Hype Curves, H-Y-P-E, Hype Curves. And you go, and you

look back five years, and you'll see the rise of all these kinds of machine intelligence and natural language processing and autonomy, etc, etc. They're like, "Yeah, these are 10 years out". And then, the next year, they're like, "Oh they're actually, they're only five years out". And the next year is like, "Well, they're being deployed". And these people; this is what they do. They're trying to attract all the most interesting technologies as they develop from emerging disruptive, to over-sensationalised, to now we're kind of in the trough of disappointment, to plateau out and say, "Hey, there's real stuff going on".

The timelines are staggering in terms of how fast these capabilities; this is something new for this year that I've, at least, that I've seen. So, they're actually taking portfolios of those crazy, interesting, new technologies and going, "What happens if you smash all this together?" And so they're termed, "intelligent digital mash". How does AI, the intelligent part; how do I make all my systems intelligent? How do I blend virtual? How do I blend digital? How do I actually connect everything? And then down there at the bottom ... so, certainly you all are trying to do the same thing in the integrated ADF, and plans like Jericho, Polaris, etc, understanding that you got a great collection of capabilities. Now, how do you strap all that together, make 'em work, network 'em together so you can share sensors and share information? But again, you gotta go beyond the data decision, which is kind of the collection of technologies that get you there. You gotta go beyond the fleet tactical grid, which is the navy's challenge to, "connect everything because then I've got options". And you want to go beyond multi-demand C2; now that I've connected everything, what do I do with it? What are the actions and activities that change?

There's gotta be a reason that we're smashing all this stuff together. And so, it's happening out in the commercial world; an Internet of things is related to this. This is actually a much more esoteric discussion: the Internet of things. It's not just the connective layer. It's actually both machine to machine, and human/machine intelligent decisions on why you've got all this stuff smashed together. And again, kind of, if you've heard of Zabrowski, Zabrowski's Revolution of Military Affairs really talked about there being a computer developed, and then we networked computers together, and then we looked at the data that networking those computers together allowed us. And that was really net-centric warfare, or net-enabled warfare. And that big revolution of "Wow, there's a lot of information that we could access". But we didn't really go, "Now, I've got tonnes of data. Now, I'm drowning. I've actually slowed my own OODA loop down". So now we're into, "How do I actually make sense of that, all that information, and how do I generate knowledge from information. And then, how do I generate decisions from that? Again, we have to remember, why are we doing this? What is the art of war asking us? We're trying to influence the adversary. We're trying to have more information and faster decision making than the adversary. And these are just tools that are being developed for other purposes that we can use to do our jobs better and differently. And what has caused the change is faster computers, understanding how to do big data analytics. What's the algorithm that actually let me process information better and make better understanding of all that big data? But then again, at the end of it, am I learning from it? I can't look at big chunks of data in random ways that don't last to the next function. And that actually gets to my bottom point.

We talked yesterday, if you remember: TX talked about specific knowledge, specific AI, specific tasking. And that's kind of the generation ... we've talked about generations. I don't know what, generation 4.5 maybe, of "I gotta task something. It's gonna do something". Then it's gonna come back to: "I'm gonna just represent data. I'm gonna give it a plan to execute 'cause I don't know

what that's gonna look like once it hits the adversary or hits the environment". Things change. Not all the planes show up to the rendezvous point, so you gotta figure out what your new plan is. There's a cloud over the target. I gotta change my angle of attack. How do I allow that in a digital domain as I'm thinking about truly autonomous AI functionality at platform through force? We've talked a lot about supervised and unsupervised, whether you know it or not.

We've talked about what ... do I need human beings to massage the data? Do I need them to be interacting with the algorithms? Or can I say, "This is what I want to happen. Now you go look at it and stare at it for a while. And you're gonna come up with patterns that I'm incapable, as a human, of understanding". And that becomes really important when I think about an ordered complexity of branches and sequels. And as things start to go bad, how do I stay ahead of that? How do I use AI to help me do that? So am I learning as I'm moving forward? Deep learning, values and policies, and why that matters is we gotta figure out what matters. We gotta give more thought to what is commanders' intent, and what are we trying to achieve, and how do I identify the values? What do I want the AI to focus on? And there's a give and take, because it's gonna come up and say, "Well, I think this is what you've told me to do. Is that right or not?" But we've gotta figure out those human/machine interactions to have that conversation with the AI, so it's not a stupid AI.

We're maximising the value of the AI. We're maximising the value of the human. The memory augment, I just kind of want to point out, is a geeky thing. So, some of those deep learning networks, they gonkulate on the data for a little while and they spit out an answer. And then, some more data come, and they have to start over. They are now talking about adding memory, long term memory, so that you can recall hours, months, days, years of pattern analysis, and say, "Hey, I remember seeing something like this before. I don't have to start over from scratch". And wouldn't it be great if, at a mission level, as you're coming out of country, the next guy's coming in country, you're able to transfer all that knowledge? As you go all the way back to the ready room, you can upload the knowledge of your mission into a larger database that tells you everything that's been going on in theatre for as long as you and everybody else has been in that theatre.

If you're the force commander, wouldn't you like to know what the 15 force commanders before you have thought so you don't make the same mistakes, and you're doing a deeper longer pattern analysis, and it's a deeper understanding? It's a long-term relationship. We might treat AIs like parrots because they're going to outlive their masters. Data is always a problem. And so imitation learning actually tries to tackle that. You can go with simulated data. You don't have to have all the data in the world. You can figure out what you need to actually see the machine and move forward. Reinforcement learning, again, everybody's pretty familiar now with Alpha Go versus Alpha Go zero.

That's an example of why you don't need tonnes of data. That's, that actually super super exciting part about Alpha Go zero: very very little data and it introduces new capabilities that no human in 3000 years of playing had ever seen before. That's something very valuable about AI. How do we let it help us be creative and look for solutions that we might not come up with ourselves? And certainly, explainability helps us trust that it's not an aberration or something that we just don't want to bring into our system. But we have to be willing to understand when we train JOs, start with NATOPS; you just make sure they're safe for flight. You're not giving 'em deep strike missions on day one after they've figured it out. It takes 15 years to develop in the US Navy—15 years—to develop a full, level five, strike lead qualified in everything and we're gonna trust you

and a bunch of your friends to go downtown and wreak havoc; 15 years, because of the experience and expertise and exposure and opportunities; 36 hours to develop Alpha Go Zero; and it's the top of the game. It's the best player in the world. It's a level five strike. So how do we actually make all of our AIs back-seaters that are all level five, and you're the decision maker but they've got your back. And then, transfer learning; and that's kind of, "How do we make sure that we capture everything and don't let it drop?"

That is perhaps one of the most exciting pieces of all of this. So again, the long-term learning, and we think about AI as a partner, not as just a tool, but as potentially an intellectual partner in helping us understand our decisions and accelerating that decision cycle. And so, to the user interface: I have a bunch of different things up there in that top line. Everybody talks about Ender's Game, both from an LVC perspective, but also if you remember when he turned the whole battle space to have a totally different perspective. That's not just an LVC thing. That's actually, "What works best for me to understand the problem? How do I design the user interface to best understand the data that's been presented to me?" And honestly, this is where the JOs, and the digital maydays run the show. A great example is the latest USS Virginia class submarine as just launched I believe last week, maybe the week before.

It has on it Xbox controllers because that's that the JOs said would ... and JOs and the NCOs say, "You know what would make my job a lot easier? I spend a lot of time on my Xbox. I know that in and out. And I can do all kinds of cool stuff with it. If you give me these other clunky 1950s controls, it's going to be a lot harder and you're limiting what I can do. But if you give me an Xbox controller, my training goes down, my creativity goes up". And I'm just so impressed with the submarine community for going, "Yep. You guys are the operators. You got it. We're gonna change that". So that makes you start thinking about all the other displays that we interact with in war fighting, in combat information centres, or air operations centres, or "How do I actually interface at the headquarters level with all the programmes and all the strategy? And how do I bring it all together into a coherent understanding of where my risks are and where my force design pivot points are?"

And certainly, there's information called "Project Quantum". United States Air Force is doing the same thing. There's programs going on at The US Navy for the same purpose. And it's about visualisation and being able to interact. Just because we've got high performance computing. And we've got tonnes of data. And we're trying to transition that into knowledge. Again, how do I visualise it in ways so that I can interact with it and make decisions about it? Otherwise, it's useless and it's slowing me down. And I don't want it in my system. So, Star Trek; why do I bring that up? He just talks to the computer, right? It's natural language processing. It's a conversational interface. It's a lot easier than going over to that keyboard and trying to figure out what do I need to say on this stupid keyboard that's connected to a proprietary information system? How about I just talk to my AI, wherever that is? That's a ubiquitous kind of interaction.

Most Western movies about AI are negative:"Terminator", you name it. We're afraid of the machines. That is not helping us, so I'm trying to pick some examples of how do we actually visualise our positive interactions with the information environment? "Minority Report", probably a lot of you, Tom Cruise, anticipating that something bad's gonna happen and being able to do something about it. And if you see, he's wearing gloves and he's manipulating data really really rapidly. How do we manipulate that data? Oh, by the way, those were real. "Minority Reports", what; ten years old? That system was really built by the Oblong Company for that movie. And

they've moved on. They've progressed much further since 10 years ago. Why aren't we using that stuff? Why can't we interface in totally new and different ways in all our combat systems and information systems? Watson, very conversational; Alexa, Siri, Cortana, conversational AI. It's a faster way to think; it's so much faster; it's intuitive. We talked about how you raise your JOs and trust 'em, and give 'em more experience and expertise. Thinking about AI as a human partner allows us to figure out different ways to interface and different ways to trust.

How do you do it with a human now? Why can't we apply that in some way with AI? And it's not just the interface with the AI. It's the augmented, virtual, and mixed reality that actually allows you to lay your data right up with you in case you're not in a conversational kind of environment, or there's a security element to it. So, there's a lot of different options out there for us to figure out how to work with the information and have a relationship with the artificial intelligence. And actually visualise our decision space, maybe do offline modelling right before you're going to commit to the final decision. So, there's a couple UI guides there. The computer has a job. We have a job. It's our job to actually set the perimeters and set the intent. And then it's going to go crunch it. And then it's gonna come back and say, "Here's your options".

Maybe it's going to talk to you differently than it talks to me because you guys learn differently, and you absorb information differently. So personal AI and personal UI is a very real and important thing to think about. How do you configure it for your decision-making process obviously within the limits of the mission? iPad versus laptop; it's a good example. You can't really interface with your laptop unless you're doing keyboard. And that is it's non-intuitive. You give an iPad to a two-year-old, and in ten minutes, they're charging your bank account for stuff they want to play with. So why can't we build more intuitive interfaces; personalised interfaces? I think we talked about all this.

So just to kind of wrap it up. Why do we care? We want better operations. We want better combat operations. We want better institutional operations. We need to understand how this plays into differentiating ourselves from our adversaries and how we need to think about our future force. If we all agree, which all our doctrine seems to point to, we're all going toward cognitive netted, distributed, manned, unmanned, multi-domain. That's complex. It's way more complex. We're going to need AI to help us figure that out 'cause we then pose the complexity upon ourselves. But we're not taking full advantage of the integrated force because we can't actually think through some of that complexity. Algorithmic Prototype Warfare, faster and funnier, right? We have to be agile. We have to be flexible. And we have to try things out. And it can't be that number one is the same as number five 'cause it's constantly gonna adapt to the world, to the mission, to the availability of the processing and algorithms and information that goes back behind that.

And I do like this statement that I ran across. We're not trying to take the human out of the system. Human judgement is essential. Human decision makers are essential. But let's free up the humans. Let's shift some of that to AI and take on some of those heavy burdens. And it is a centaur approach. It is a man–machine. There are some cases where fully autonomous goes out. But even before you sent them out, there was a human being that was working out what those mission parameters were, and what the intents and decision criteria are. So, it is all about man and machine. And General Shanahan spoke very well to that. I talk about R2D2 because, again, I don't want you just thinking about sitting in front of a computer. We're going to have a relationship with our AI at individual platform and force levels. And how do we think through what they're best capable of helping us at all those different levels? And again, we talked about

human experience and expertise and how that plays in, and how we ought to be thinking about engaging the AI on a similar kind of approach.

Trust, transparency, and training; we brought up LVC. There's explainability. DARPAs got a program there we need to understand. But just because we don't fully understand the logic behind everything, doesn't mean we should shut it down. What's the acceptable decision space? And honestly, again, for the aviators in the room, you expand the decision space as you see the trust, as you interact with it. And you grow from NATOPS to mission commander to division lead to strike lead. So how do we quantify that acceptable decision space? Because I couldn't always explain why I did what I did. The mission was accomplished within parameters. But maybe I had a more creative way than somebody else had. And we need to be willing; and again go back to DOTA2. You don't know how it won. No-one had ever seen that. So, should we have thrown that away and said, back to TX, "We're going to disallow that"? We're going to disallow something that was a winning combination just 'cause we didn't understand it or it didn't fit our norms. So we need to push the envelope in that as well.

I think we've covered LVC. And at the end of the day, it's all about extending the speed of decision in command. So again, we go from the computer, the network, the data, to knowledge, to decisions. It's all about decision making. That's what warfare is.

Thank you very much.

Strategic Communications: Disrupting our World

Mr Mark Laity

Okay, folks, chill. I'm going to talk about people. I'm a strategic communicator. Before I start hitting the slides, I just want to highlight what strategic communication is. It is not public affairs on steroids, neither is it social media on steroids. Actually, sometimes, it's not just strategic in the military sense because you need to do StratCom at the tactical level.

What it is, is communicating which is more than a speech. You drop a bomb, you're communicating. You dig a well, you're communicating. When Genevieve Bell came this morning and she was wearing clothes which she drew your attention as not typical of what this audience had, she was communicating a message to you saying, "I'm not like you." Strategic communication is communication for a purpose. If any of you are hiring or using strategic communicators, if they do not think strategically, get rid of them because unless they understand the strategy, they're no use to you. That's strategic communication, and I want to highlight that because it gives you the breadth of what we're talking about. I have also tried to talk about the topic and I'm also going to do something really unusual. I'm going to have a picture of an aeroplane.

Transformation is disruption, so disruption is not necessarily bad. It just depends on which end of it you're on. The reason I've put that up is I want to highlight that the level of disruption that is caused by information, by AI, is actually to some degree due to its level of maturity. That sequence of pictures shows you that, when you first had aeroplanes in 1914, they were not transformational. They were just extended range artillery. And in the same way, they were just long-range reconnaissance—and I claim my prize for the most pictures of aeroplanes on the slide. I don't think that's going to be big.

In the First World War, frankly, although air power was important, it was not transformational because it was an immature technology. Now, it's a very mature technology and as a result, it's the new norm. But now, you're being succeeded by other transformational technologies.

In the same way, information is a disruptor. It's been disrupting for a millennia, from the Gutenberg Press through to the telegraph, telephone, television and computer. At each level, each time, there has been a jump in technology in the information. It has become more important. But the latest leap has put us right at the front. Information is now the ultimate disruptor. In the picture you see up there, all of the pinpoints of light are actually smartphones. So, there we are, a millennia gone and we have created an electronic candle!

The smartphone and the technology around it, and the behavioural changes around it, are what have, if you like, made information so central as a disruptor because what they've done is complete the democratisation of communication. When I started in journalism, I spoke and people listened, I hoped. I wrote and people read. I went on to BBC television and I broadcast and millions watched. And they could not interact with me. Even though I was a journalist and journalists all like to think they're mavericks. In fact, I was part of the establishment. I was part of the people who spoke to the people and the people listened. And I control that means. Now, I don't control that means. The smartphone is everyone's tool. When I first went and did big foreign stories, say the Gulf War, we have what was called the fly-away kit for television. The fly-away kit fitted inside a Boeing 737 and it went on the back of a three-ton truck.

Now, everything that could get on that truck is in the smartphone. Almost everyone in this room will have a smartphone and you can do things on it which were unimaginable then. It's even silly in a way to call it a phone because actually young people call less on their phone than they do anything else with it. And it's everyone's tool, which means that everyone is a player, absolutely everyone. It has also changed the nature in which people interact with the establishment. We have lost control of the information marketplace, so we're no longer Wal-Mart or Tesco or Carrefour. We're just another street trader because everyone who has a smartphone cannot only talk to everyone else as well as us; they can communicate with everyone else. And the wiring has changed; they expect to be listened to. It's no longer any use paying lip service to people because what the smartphone has done: it has enabled democracy to be broadcast worldwide. Everyone is now a player. And that's incredibly disruptive, and it has changed the very nature of our relationship with each other.

We have influence because we're a player and we have significant power, but we don't have control. We need to change the interaction, so it's no good having a spokesman, you may need an interaction. If you were dealing with the public, one spokesman won't do it because everyone wants to talk to you. There aren't enough hours in the day. The laws of physics do not allow one spokesperson to do it. You see, time and time again, government after government getting it wrong because they want to control output. They want to focus in. They want to decide exactly what to say, who to say it to and when. And it doesn't work anymore because people will not accept it because they've got the smartphone. They can speak to anyone. They can say anything, and if you don't damn well listen, they will find someone who will listen.

This is a truly radical transformation. So, information has been fundamental forever. But this has never been as fundamental as now because it's never been as spread as it is now. We have to listen as much as we speak and then take notice, not pay lip service. And of course, we then need many voices. Your best advertisers are your people. If am a 21- or 22-year-old, whom do I want to interact with? Not some 62-year-old, old fart from Britain. I want to speak to somebody like me. If you want to influence, then you're going to have to have your 22-year-olds speaking to their 22-year-olds. Of course, what are they going to do? They're going to do a really good job most of the time. Some of the time, they're going to totally screw up and that's going to be disruptive and you're going to have to live with it because the balance of advantage is yours.

But that's disruptive. The digital era introduces certain elements, which are awkward. One of the earlier speakers made the point: digital video imagery is incredibly easy to manipulate. It was very hard to fake photographs. It was very hard to fake wet film, but digital video is incredibly easy. I have seen the stuff that they've done where George Bush has been morphed and then words put into his mouth and he has said extraordinary things. Of course, it's getting easier and faster. One of the dangers that we all face is the fact that the digital era is so easy to manipulate. One of the questions I have, not for you but a question you should put as people in authority, is why is it that people are spending so much damn money on making things fake and those same companies will not spend money on discussing how to discover its fake? Every company that has the gall to come up with a program so that you can have great fun creating fake images should be told, "All right, why're you not spending some money on helping real people understand that they're being misled?" That's the world we live in.

And actually, to some degree they're beginning to realise it. You know you're in trouble when the inventors of the trouble decide there's trouble, so there's a few quotes from people who are

recognising that social media is a beast that we don't quite control any longer. Civic engagement, the damage the Internet can do to even a well-functioning democracy, a guest blogger. At best, it's a problem; at worst, it's dangerous. Then the inventor of Napster highlights that one of the features of social media is this kind of self-licking lollipop where we feed each other what we want to hear. These are very real things that are happening and they are very dangerous because they're being fed by the amoral or immoral in order to achieve things.

For my purposes, the worst victims at the moment, because I work at NATO, are the Russians. Margarita Simonyan, RT's editor-in-chief—RT is the Kremlin-funded propaganda outlet for the Russians—highlighting no objectivity. This is a very important thing. Remember, we're talking about people. If you don't have a firm basis, in fact, if there is no agreed level playing field, then objectivity goes, fact goes and what replaces it is what you think, what your instinct is, what your viewpoint is. In fact, my ignorant viewpoint based on nothing more than my instinct is as good as your well-founded fact, and you can see there a quote from Hannah Arendt, the best-known philosopher of totalitarianism, highlighting that the people who are most vulnerable to extremism are people for whom the distinction between fact and fiction, true and false, no longer exist.

This is a definite target of the Russians, as they have admitted openly. There is no objectivity. Now, that is not what they say to their own people. It's what they say to us and then I put at the bottom that X-files picture because it goes to a point that's in all of us. We distrust governments. Remember the X-files? Most of you of a certain age will and they've done a repeat, "Trust no one." That's the zeitgeist of that time. Since the weapons of mass destruction debacle, since the 2007–2008 financial crash, faith in government is gone. People are very willing to believe that we are lying to them because we have a credibility problem.

If you are a disrupter and the Russians are a disrupter, you have fertile ground. The Russians do not have a strong narrative for us, other than to make us distrust our own government. And they do. Their logo, "Question more." In other words, don't trust anyone. They're fairly open about what they need. This is a quote, from the same Margarita Simonyan, which is talking with a Russian media outlet. "So, anyone who ever tells you the RT is like the BBC, remind them of this, because I worked for the BBC for 21 years and that is why I worked for the BBC. It's a weapon like any other. Do you understand? So, RT is quite constantly being used as an information weapon to shape the situation for when the Russians need it." It's their accurate quote. That's the fact for information space.

Now, this is the famous Gerasimov slide. He used this in the military industrial carrier. For those of you how don't know, he's the Russian Chief of the General Staff. And it is the Russian view of how war is fought. Some people have more inaccurately said it is the Russian doctrine of war, which is actually not what they meant. This is their view of how warfare is fought, so they think we're doing this as well. More accurately, I call it the Gerasimov slide. Now, you'll see in the yellow ring, there are faces of conflict and it starts from the blue ring's covert origin. From a Russian perspective, war is already under way because that's what they think is happening.

They think we're doing that to them. But it is quite logical that, if that's what they think war is, they're doing it to us, and all the empirical evidence would suggest that's true. What I want you to look at for our purposes though is where the big red arrow is conduct of information confrontation. The Russians don't do StratCom; they don't have a term for it. They call it information confrontation and what I want you to notice there is that you'll see "non-military, military". There's only one thing that goes from the beginning to the end and straddles non-

military, military. And that's information confrontation. That's what they think is going on. That's what they're doing.

This is a quote from Gerasimov highlighting the incredible importance that they put to information: "Information dominance is an indispensable prerequisite of common actions." Ponder that. Think about that. Take that aboard. Now, there's actually two views in Russian current thinking. There is the view that information dominance will set you up for an inevitable victory. There's another view which is that you will succeed without having to fight at all, or without having to fight a major combat. And this is something we will need to think about. There is serious thinking in Russia that basically they can win without a major conflict. They can achieve their geopolitical aims.

If we're getting ready for the big one and the Russians are saying there isn't going to be a big one, then are we planning for the wrong war? Are we going to be ready for the victory parade that won't be ours? These are things we need to think about, and, seeing as I am where I am, there has to be a sensible quote.

But I want you to look at it in the context of what Gerasimov said: "Victorious warriors win first and then go to war." Information confrontation is an indispensable prerequisite of shaping operations. It's that important. There's nothing magical about this and there's nothing they're doing that we can't do, only we can be moral about it. We should be moral about it. Is information the new domain? Actually, the Russians already regard it as a new domain. They do not see cyber as a domain in the same way that we do. They actually regard cyber as a part of the information domain. You can see two quotes in one of their main journals and from their military doctrine. The cartoon incidentally is from Vestavia, referring to when they announced the formation of an information operations troop, which is about 50 years after it'd actually happened.

NATO has responded. You've got there the quote from the current secretary general, "The blurred line between war and peace," which is where we are operating more or less all the time. He says, "We have to do things differently. We have a new playbook. To be honest, we're developing a new playbook. It's a work in progress but it's not going to look like it did in the Cold War days; it certainly isn't." Remembering information is about people, there's a quote from the historian of all historians, E. H. Carr, "History is an unending dialogue between the present and the past." The Russians and others are very good at using history as a shaping tool to support their strategy; what I would call strategic narrative. They have a strategy and they have a story to go with it because we operate by stories.

That picture you can see is a statue of Prince Vladimir of Kiev in Red Square. Vladimir is the ultimate Ukrainian hero. When, in 2016, the Russians put up a statue to him in Red Square, they, in effect, subjugated Prince Vladimir to them, and they use as a narrative line to both the Russians and Ukrainians Prince Vladimir, "Your hero is a unifier and defender of Russian lands."

In other words, if you support Prince Vladimir, your ultimate hero, or your King Alfred, Winston Churchill, or Henry V, then you should support being part of Russia. Never underestimate the power of stories. We have not been speaking in code. We invented the PowerPoint in 1987. We've been doing stories for millennia, so we're hardwired for stories.

They used history, ancient and modern. When they wanted the Ukrainians and the Crimeans to vote to unify, they didn't say, "Do you want to be Ukrainian or Russian?" They said, "Do you want to be a Nazi or a Russian," because of the great patriotic war narrative. It's called a binary choice.

Remember, yesterday our keynote speaker talked about the fallacy of binary choices, and the Russians used binary choices to make life simple. Do you want to be a Nazi, which is not a nice thing to be, or a Russian? This is part of an overall strategy. They used this narrative to justify their intervention in Eastern Ukrainian Crimea. They use historical narrative as I've just described. They used tricks and techniques with binary function, framing, priming. These are things, which people can use to sell you cars because human beings work to them.

But most of all, they took their information confrontation. They took their history. They took the narrative. They took that strategy and they operationalized it. They used information like an information smokescreen like pretending that the Spetsnaz were, in fact, local militia and they used that to get inside our decision-making cycle. We had somebody just talking about the OODA loop and that's a part of it. We, at a critical time in Crimea, didn't know what the hell was going on and couldn't make up our mind what to do about it. By the time we did work it out, it was too late to be undone. It's a very successful use of information operations.

Strategic narrative is critical to how we do it. It's the heart, plan and the end state. I'm going to go back, because I'm a people person, to Aristotle. We are human beings. Human beings in their instincts haven't essentially changed. You'll be reading, or some of you may have read these books, "Tipping Point", "Nudge", Daniel Kahneman's "Thinking, Fast and Slow" from behavioural psychology. Actually, the great rhetoricians of the great period, they were there before us. The three things that dominate how we decide what we do are logos, pathos, ethos: argument, passion and credibility. And the least effective is logos. Every behavioural psychologist will tell you the thing that drives us is Pathos. We are rationalising people, not rational people. Our instincts drive us and then we decide to have an argument to support what our heart has already told us to do, and the key people that will make us do it are people we believe in, people we trust. Remember what I said about the 22 year old? A 22 year old has more credibility with a 22 year old than a 62 year old. It's just the way it is. When you are trying to persuade people what to do, whether you're dropping bombs on them, whether you're digging wells, or whether you're speaking to them, you need to understand those are the three things that drive us. And that comes back to people needing a story.

If you go back into the 1700s, less than 11% of the world's population could read, write or do the numbers. How the hell did we get from bare skins and loincloths to that point? We did it through stories in which we organised ourselves. You can see quotes about counterinsurgency there from the US counterinsurgency manual highlighting that the story is also an organisational scheme. The structure of a story is actually very similar to the structure of a strategy, of a strategic plan.

When you want to persuade, you have to get the emotions right. You have to get the right speaker, and these are all disruptive things because most of us are not credible. Most of us don't understand the cultures we're in and we're now living in this digital environment where trust is at a premium, where the digital world is faking stuff, where the Russians and other players are understanding that what motivates people is not a cold, hard, dry fact. But I don't want to use this as a critical thing. The Russians aren't the first people to understand that shaping the information environment is something you should do. China has the three types of warfare, which they approved in 2003. It builds on older Chinese thinking and has been adapted and updated to the new information age, and has three elements. Public opinion warfare, you can read about it for yourself; psychological warfare, and legal warfare or law–fare. And you can see none of them involved an explosion. These aren't shaping us. Now, none of us is naive about this; we have all

had it in our Western area. We're well familiar with dying, diplomatic information, military and economic. This is the critical environment in which we're operating now in phase zero or phase one.

How does this fit with air power? You can applaud me if you want. There's another aeroplane out there. I would say that air power is being undermined. There is an eroding asymmetric advantage. We've already had one speaker who highlighted that ISIS have some kind of poor man's air force. Now, I don't want to overplay the psychological effect on Iraqis, the first time a bomb from ISIS dropped on their heads. It was extraordinary because how the hell could this happen? We also do have to acknowledge that drones, this kind of technology, has put at very least effective aerial reconnaissance in everyone's hands. The psychological impact is considerable. A lot of some of the basics of air power are now more accessible because of information technology in the main, but also, air power is more and more vulnerable to disinformation campaigns in law fare.

It has been very evident to me. I've done three tours of Afghanistan. I covered the Kosovo conflict. Air power is an incredibly powerful weapon which is very difficult to use fully. We cannot afford to miss. Now, we're seeing in Syria that the Russians don't see it that way. The Russians are doing stuff in Syria, which would cause governments to topple if we did them. But the ability of air power to be fully used in anything other than an existential major conflict is very, very constrained without any question at all. And we've seen this effect. Air power is constrained and that is mainly through disinformation campaigns and the effect of collateral damage and so on. Can we fully exploit air power? The answer is no. We can certainly exploit it but not fully. This is enhanced by differing attitudes to collateral damage.

And, if we are in a situation where shaping operations means that the actual kinetic phase of any conflict is going to be relatively brief, what is air power's role? And I don't mean that in a critical sense. I mean that as a genuine question and you can actually equally apply that to any kinetic weapon. But what is the role of air power? How can we find a way to make air power contribute to this messy non-war, non-peace situation especially when we actually operate with serious values and ethics?

I want to end by going back to narrative. A lot of people have already spoken about AI and social media, which I've touched upon. But on the things I've learned as a strategic communicator is that the person who wins is the one who's got the clearest idea of what he's trying to do. If you've got a clear strategy, strong leadership and you do your planning, you'll usually come through and you will be fairly proofed to disinformation.

One of the reasons that we're vulnerable to Russian disinformation is because of our own uncertainties in that we are not so sure what we're trying to do. And I would argue that part of what it is, is that we need a new narrative. We are in what I've called the new great game. Earlier on in the first few speeches, a couple of our speakers talked about the rules-based order. Now, that has got to be the worst bumper sticker in the entire world. What the hell does that mean, the rules-based order? I used it myself. I'm not criticising others. What it actually means is the right of everyone to get a fair shake. That's what it means. A common set of rules, which apply whether you're big or small. Now, what you see there is a quote from Thucydides—I'm always very pleased when I pronounce his name right—from the history of the Peloponnesian War: the Melian Dialogues.

Now, this was the Athenians, who were the superpower of the time, who went to Melos and said, "I know you're neutral. I know you're staying out of it, but I'm afraid we need to take you

over in order to be sure you'll stay on our side against the Spartans." And the Melians said, "Hang on, we've had a deal, had an agreement. We're neutral. Why do you want to do this to us? We're not going to threaten you and it's unfair". And the Athenians said, "Yeah, of course it's unfair, but so what? Because you know as well as we do that right, as the world goes, is only in question between equals in power while the strong do what they can and the weak suffer what they must." In other words, might is right, simple as that.

And this is the central thing that's going on now. Throughout human history, we have always had might is right. Since the end of the Second World War, to a large degree in Europe but to a more limited degree elsewhere, we've had a situation where we have had the rules-based order, which, in other words, is the big guys playing to the same rules as the little guys. And what is happening now and the true disruption that is going on in the world is that the geostrategic-level rules are under attack by people who have a different view. Social scientists would call it neorealism, and you can see there from quotes. What is going on is Russia is saying that we have privileged interest and they are not the only country. Big countries all over the world are basically challenging the narrative. And they're using it by saying, "If you were as big as we are, you'd do the same." But the curious thing is, that's not what happened.

The United States after the Second World War accepted the rules-based order. I've worked in NATO since 2000. I have watched the US through gritted teeth accept that it is first among equals but everyone else is an equal. We've had a situation, especially since the end of the Cold War, where nations basically agree that, even if you are small, you have rights. And that's the true disruption that's going on, because the reality like when the Norwegian prime minister said we cannot have a world where big countries decide what to do with their neighbours, is a massive narrative.

But of course, we can have a world where big countries decide what to do with their neighbours. And so, the question is, what are we going to do about that? Because there's only two countries—remember the Melian Dialogues, the Athenians were the great power, the Melians were the ones saying can't you be fair. There are only two countries in this room who are not Melians; there is the great strategic communication disruption. There is the great clash, so the question is, what are we Melians going to do about it?

Thank you very much**.**

Digital Natives and Security: Are We Living Ender's Game ?

Mr Bernard Salt

Thanks. Thanks so much Mark for that introduction. Thank you also to Air Power for the invitation to speak. Bernard Salt, I'm the managing director of the Demographics Group. You may recall that I worked with KPMG Demographics for almost 20 years, after founding that group. I retired from the partnership in June last year and am effectively doing the same thing under my own consultancy. My presentation today, is Dealing with Digital Natives, Dealing with Generation Y or the Millennial Generation as you might know it. Looking at the future and looking at engaging that next generation, in fact.

I want to start, however, by asking both a really big picture question and much simpler question of the Australian people: is Australia a good place to be over the next 20 or 30 years? If I were a millennial, if I were 25, I would ask that question, "Why should I invest my youth, my energy, my career, and my life into this country over that period?"

Here is the reason why I think you should.. Here is the world population, effectively over 200 years, that's 1900 on the left and I'll show you through to the end of the 21st century on the right, and it shows the number of people on the planet very simply. So two billion people at the turn of the 20th century. We have around about seven billion people today. Then the best demographic brains on the planet, the UN Demography Department say that, by the end of the 21st century, there will be close to 12 billion people on Earth. Another five billion people, in fact.

What can you say about the world in say 2070 or 2080 towards the end of today's millennials' lives, because I think there are some things you can say about the world in half a century's time? I think that we will see a mad scramble for food, energy, water, resources, commodities, space, security, lifestyle. What is it that Australia has to offer the rest of the world? Food, energy, resources, commodities, space, security, lifestyle. We have what the rest of the world will progressively want over the next generation. That makes Australia a valuable commodity; I think it makes Australia a vulnerable commodity. I think that military issues, defence issues, will become increasingly important in a crowded world.

If you actually take that squiggly line, this is produced by the UN and it shows world grain production, and the scale is off to the side from 1960 through the 2016. The world produces three billion tonnes of grain, wheat, barley, rice, corn to feed seven billion people.

It's not evenly distributed of course; but that's the world population, this is world grain production. I wonder how much grain we need to produce up there? That needs to be up there somewhere I would have thought. That's all right; we'll just plant out all the used arable land on the planet; well, in fact, there is none!

That makes Australia a valuable commodity; that creates opportunity for the Australian people. All we need is to ensure social cohesion, security, independence, prosperity. These big picture matters will deliver a prosperous, safe, secure and liveable life for the next two or three generations of the Australian people; that's all we're asking. It's a big issue I would have thought, a big challenge, but in actual fact, you would have to say that Australia is pretty well positioned in that regard.

Let's take another big picture perspective and look at the biggest countries on earth in our time in history. Of course, this is by GDP, Gross Domestic Product. It's effectively the business worth, if you like of the world's biggest countries. The United States, 19 thousand billion dollars in GDP every 12 months. This is in US dollars. United States is the Roman Empire of our time. There's China at around about 60% of the US. In the year, 2000, China was at 30%. In 1990, it was 10%. At no point during the Cold War did Russia or the USSR ever get to any more than 10% of the American economy. China is already at 60%. This is in US dollars. Purchase price parity, of course, it's almost level pegging. Australia is, of course, the 13th biggest economic force on the planet. Interestingly, at the Olympics we also come in at about number 13. We're about fair value I think in terms of the Olympics. We're medium sized when you think about it.

That's not the real measure; the real measure is in fact in GDP per capita. Just take the economic output of the country, divide it by the population, it's not evenly distributed of course. Then I remove any country with fewer than about four million people. You're looking at places of critical mass. The richest places on earth, Switzerland, it's only seven million people but very, very rich, very well to do. The United States, with 320 million people, is the largest economic force in history, of course, and Australia's key ally. Denmark, Australia, we're rich. We're the third or fourth richest people on earth. Where are the forces coming from? Where are the rising powers across the planet?

Another way to do this is to actually look at the rising income per capita over the last five years in GDP per capita in US dollars. Here are the fastest growing economies; this is GDP per capita in US dollars from 2012 to 2017 and we see Australia going backwards. A lot of this is explained by a shift in exchange rate, so the Australian dollar relative to the American dollar has dropped quite significantly over that time. Again, eliminating any small countries, here are some places of economic worth if you like, or economic value or impact shaping the world as we know it, and several of those are in our direct region.

Let's take a big picture look at our direct region. Here is the continent of Australia and a number of outposts, islands of course: Cocos, Keeling, Christmas Island, Coral Sea Island, and Macquarie Island. We have two slices or claims to slices of the Antarctic continent; they're suspended, of course, those claims but historically we have them. Here is the State of Texas in the US by the same scale. More people live in Texas than on the Australian continent. When you look at the extent of our land claim, it's a most extraordinary claim by the Australian people; not even the Americans make such an outrageous claim in terms of an entire continent.

With a third of the Antarctic continent, and all the other little bits and pieces, the only way 25 million people—there's 27 million people in Texas—the only way 25 million people can make such a land claim, in fact, is if we have the imprimatur of the prevailing world superpower—the Brits in the 19th century, the Americans in the 20th century; who'll be the prevailing world superpower in the second part of the 21st century? These are big and uncomfortable questions for the Australians to ask. Big picture demographic trends, mega-trends if you like, that set the trajectory, that ask the questions that are really quite uncomfortable for Australians.

Let's take this forward, and bring it back to Australia and compare Australia with a number of other world countries, particularly in terms of cities. Those numbers against the Australian cities are drawn from the 2016 census and they show the proportion of the population born outside the Australian continent. The biggest city is Sydney, with 39% of the Sydney population being born outside the Australian continent. That actually sounds like quite a lot. Find me another city on

Earth where more than 39% of the population was born outside that country. There's only two on the map. One is, Dubai. These are guest workers. They do not have the same sovereign rights as migrants. The other is Toronto, and they're Americans just across the border.

Sometimes these simple high altitude figures speak to a profound cultural truth about a people and a nation. I do not believe that you can credibly make the case that the Australian people are fundamentally racist. Racist incidents occur perhaps, but we are not fundamentally racist when 39% of the biggest city was born outside the Australia continent. Go to New York, it's a great melting pot, 29%. Go to Paris, 22%. Go to Berlin, 13%. Go to Tokyo, 2%. Go to Shanghai, 1%. The Germans get all angsty when Berlin gets to 13%. Sydney, Australia is at 39%. If we had a problem then this would've been rioting on the streets at 20%, 25%, 30%, 35%. That must make Australians the most plastic, pliable, absorbent, changeable, dynamic culture on Earth; and if we're not, show me who does a better? A changeable people, an absorbent people, an influential people, a malleable people, you could argue, but a profoundly prosperous people, who assume a right to prosperity and who assume a right to security. These are, I suggest, dangerous assumptions for the Australian people.

The other observation I have here is that every wealth-generating region on the planet for 100 years has had a lifestyle area nearby. In the 1990s, wealth was generated out of the Middle East, so you make your money in Saudi Arabia or Kuwait, but you park your money, your family, your lifestyle, you buy an apartment and live three months of the year in the haven of Dubai. That's why Dubai exists, it's a safe haven in a troubled world. Russian billionaires do not live in Moscow. If you have a billion dollars to spend, are you really going to live in Moscow? You're going to live in London, or in Belgravia. You would set up transnational residencies, in fact. So you make your money in Moscow, but you live in London.

What is the greatest wealth-generating region on the planet in our time in history? That'd be China. Make your money in Shanghai, Guangzhou, Beijing, Shenzhen. Park your money, your family, your lifestyle, buy an apartment, live three months of the year. Educate your kid in a local university; go to a hospital, have a facelift; go to a casino; play golf; go shopping. An overnight flight away from Shanghai, 8,000 kilometres. What are my options? No, no, no, no, no, no, no, yes, yes, yes, yes, yes. Money will flow from there to there for as long as the regulatory environment permits it. China does not deliver lifestyle cities; Australia does. There are still Russian billionaires living in Belgravia 25 years after the collapse of the USSR because it is a fundamental cultural truth. London is a better lifestyle city than is Moscow, and Sydney, Melbourne, Brisbane, Adelaide, and Perth are better lifestyle cities than Shenzhen, Shanghai, and Guangzhou. This is a fundamental truth I think about our bigger picture region.

Here is another perspective. I chose what I think is the great diaspora, if you like, if we're going to see the great middle classification. We need a new verb to describe the middle classification process coming out of China, and maybe out of the Philippines, maybe out of Vietnam, maybe out of India. If you're describing the totality of the 21st century, in fact and you go to Vancouver, 41% actually have Asian, Indian heritage, either born there or with one parent actually been born there. You can see, I reckon, that there's a fault line that says, "Asian or Indian" down to perhaps San Francisco. Then in Los Angeles and south, it's more of a Latino heritage. So those two plates, if you like, collide somewhere between Los Angeles and San Francisco. There's Sydney at 20%, Melbourne at 17%, from which you can see the direction that this is actually going. The most

plastic, pliable, changeable, absorbent culture, Australia, will move, shift, change as a consequence of these trends.

Here is a bigger picture perspective of the Australian population. Here's Texas. Here's 25 million people on the Australian continent broken down into the different generations, with the baby boomers about four and a half or five million people between 53 and about 70. Then you have the Generation Xs sitting in the middle. Here are the millennials, the next generation, the generation that you are recruiting, the generation which will deliver the next round of management, if you like, of defence personnel. You can see the components of the demography. Here is that millennial population, aged 18 to 34 or 35, over 100 years. This is 1980 on the left, and it goes through to about 2060 on the right. It shows you the net growth or reduction in the young population of Australia. These are baby boomers in the late '60s and '80s, and then the baby boomers move into their late 30s and 40s and there's not enough people coming along behind, so you have this diminution of youth, this echo effect.

Here is the next 40 years, and you can see a stronger level of overseas immigration, particularly Asian, Indian and Arabic reshaping Australia, reshaping a culture that is already plastic, pliable and absorbent. Over this time in history we had a stronger Mediterranean influence. You can see that reshaping our culture: out with tea, in with coffee, in with arugula, in with olive oil. Who knew what quinoa was five years ago? Who knew how to pronounce quinoa five years ago? It's an Arabic grain.

If you go to America, the Americans are unimpressed by anything outside America. The Australians are impressed by everything outside Australia because we are a colonial, isolated culture much impressed by what is out there, and quite suggestible when you think about it. Here is the next 30 or 40 years or so. You would say there's quite a strong pipeline, if you like, in terms of straight demographics. It's a matter of recruiting that demographic group going forward.

Here is a big picture perspective of the Australian population. We have a census every five years. We ask 62 questions. Here's one of them. The Americans have a census every 10 years and they ask 12 questions. One the questions we ask is, "What is your religious affiliation?" I'm not particularly interested in the religious set numbers, but there is something so compelling about this, it's never the numbers it's always the story behind the numbers. There is something happening in middle Australia and it's reflected in this chart. When we ask people, "What is your religious affiliation" seven million people said, "I'm nothing. I'm an atheist". This is incredibly important because that figure is up 45% on the number just five years earlier. I would've expected that figure to be 10%, at most.

It's almost like a bomb has gone off across middle Australia, exploded, and shifted the Australian heartland's thinking. I wonder what could've happened between 2011 and 2016? The Royal Commission into child abuse, has shifted the way Australians think. The bigger picture narrative here is that middle Australia is saying, "I no longer trust big institutions like the church. I no longer trust big institutions like the major political parties, like big unions and, most certainly, I do not trust big business. If you wish to connect with me, connect with me locally, tribally, in a communal, authentic way."

That is what I think is happening across Australia: a shift, a loss of faith, a loss of trust in big institutions. Connecting with middle Australia is far more complicated today than it has been at any time in the past, and it all comes down to that figure; it speaks to something else. Never look at the raw figure; there is a bigger picture story behind every one of those numbers. In fact, all

the Christian religions are going back except for the Pentecostals; they are the Hillsong Church, of course. On the Gold Coast, the Hillsong Church has increased by 25%. I don't know who the pastor is on the Gold Coast, but he or she is doing a fantastic job for the Pentecostals.

Here is another perspective, I love this chart because it looks at the topic of economic confidence by the Australian people in the Australian economy over 60 years. This is 1961 on the left, and it is 2017 on the right. It is quarter-by-quarter GDP growth and contraction across the last 60 years. Your working life, maybe even your entire life is stretched out across these bars. Let's just read this time in history together. From 1961, when Bob Menzies was the Prime Minister, we had growth, then recession, then growth, then recession, then growth, then recession, then growth, growth, growth, growth, growth, growth for 25 years.

If you had a choice to be a 25-year-old going into the workforce in any time over the last 200 years of Australian history, what year would you choose? Because I would choose to be 25 in that year, 1993. I'd have 12% unemployment behind me in the December, but I'd have 30 years of economic prosperity ahead of me. I'd be 50 years old today and I'd look back and I'd say, "I've been pretty damn successful in my career." Maybe you should have been pretty damn successful in your career; you have had a dream run, in fact.

Go back to the 1960s, start a business in the 1960s, and you're selling product to people that can remember the Great Depression, that fought in the Second World War. Don't get too uppity, don't get too ahead of yourself, don't cross credit, don't get into debt. You know these people because they're your parents. Whereas, today, today you're dealing with your recruiting, you're dealing with people at this time in history who have forgotten what a recession looks like. We think it's outrageous if unemployment has a six in front of it. No, it can actually have a 12 in front of it. Of course, you're dealing with a culture at this time in history that has a sense of entitlement, a sense of aspiration. We don't want to go on the caravan holiday to Coolangatta, we want a Jet Star holiday to Bali. We've lifted the bar, our outrageous expectation and entitlement. We presume security. We presume prosperity, the two dangerous assumptions of the Australia people, I would have thought, going forward.

You can see this writ large in how we live. Let's go back to this time in history to see how we lived and compare that with today. Here's how we lived back in the 1950s. This is a quarter acre block. It's a three-bedroom brick veneer. It might be your home.

It might be your parent's home; mum and dad and four kids. Dad works, mum's a housewife. Two kids in bunk beds per bedroom. Let's visit grandma and grandpa back in the 1950s. Up the pathway, onto the porch. It was called a porch. Then you turned right into the lounge room. The lounge room was a modern incarnation of the parlour. The parlour was the good room. There was only one good room back in the 1950s. The good room was where you entertained guests and suitors. Suitors never got near a bedroom back in the 1950s; very different today, of course. Then off to the side would be a mahogany side stand with a silver tea service. The purpose of that was to showcase the wealth, the prosperity, the social status, and the values of the couple that ran this household.

Let's compare that with how we live today, how you live today, how middle Australia lives today. After 25 years of unbroken and outrageous prosperity, here is how we expect to live today. It's not a 1,000 square, it's only 500 square, metres, but it is four bedrooms, not three bedrooms; it's two bathrooms, not one bathroom; it's two income earners, not one income earner; it's two kids, not four kids.

Come with me into the house of today, into your house; down the pathway, through the entry. In this configuration, you have a central hallway with bedrooms off to the side. Guests are entertained not in an English parlour at the front of the house, but in a Mediterranean kitchen family room in the belly of the house. It means that guests must now pass the open doors to the bedrooms, which means the bedrooms must now be glimpse-perfect. As a consequence, you've had he 'pillowfication' of the bedroom over the last decade, not two pillows, not four pillows, but six pillows. A thing that I now know is called a bolster, and a thing at the other end of the bed that's called a throw.

The purpose of the pillowfication is to showcase the wealth, the prosperity, the social status, but importantly the social harmony of the couple that run this household. Both partners work but they've got enough time in the morning to fluff up the pillows exactly right, and men can never get the pillow architecture right. You grab the pillow by its ears, you fluff it up into position, and then you karate chop in the middle to give it this perfect V. This is as important to us today as was the silver tea service a generation ago. Then you take your guests down into the belly of the house and you mill around an island bench, which means the island bench must move upmarket. It's now marble, Calcutta marble in waterfall style. Rising out of the centre of it will be a silver Grohe gooseneck tap. Tapware is now the new silverware, it matters to the colonial Australians that it is Italian marble, German tapware, Danish closing mechanisms in the soft-closing drawers, in fact. Out the back is what we used to call a back veranda, then we called it a deck, today we call it alfresco, which is a Mediterranean term. On the alfresco deck would be a barbecue with a wok burner. You can see the direction that this is moving in.

I think the Greeks and the Italians who arrived here in the 1950s went, "What the hell are you Australians doing living in an English house? You have a Mediterranean climate even in Melbourne, when you should have indoor, outdoor"; actually you're right. It took us 30 years, plastic, pliable, absorbent, tolerant, changeable, aspirational outrageously entitled people. This is what you're dealing with: a presumption to security, a presumption to prosperity going forward. You can actually see that, out the back is a little butler's kitchen. You have the show kitchen and then you have the real kitchen. When you do that you need butler's kids, I reckon, these sort of things.

Here is my avocado column. I have a column in the Australian newspaper on a weekend, in the magazine. I wrote a column about 18 months ago where it was a parody on a baby boomer wandering into a hipster café. It was totally autobiographical. I made the point as a baby boomer wandering into a hipster café: you can't read the menu because the writing is too small. You can't hear yourself speak because the music is too loud. You can't even sit on a milk crate because that means your bottom is lower than your knees and you can't get back up again. Then you secretly whisper to each other because you could never say this out loud, "Look at all these young people eating smashed avocado; shouldn't they be saving for a house?" It was all done as a parody on middle age, of course.

Well Twitter came along and took my comment about young people, saying, "Bernard Salt said this about young people and smashed avocado, what do you think about that?" Without the context of a parody it didn't look good. That tweet went live at 6:27 am on Monday morning; by 10:00 am I was fielding calls from the BBC in London. This thing went global, viral and feral immediately. It made page three of the Stuttgart German newspaper. Made the newspapers in Caracas, Venezuela. I particularly liked the social media around this, "I stopped eating smashed

avocado and now I own a castle". It was all the work of the millennial generation, of course. I thought the whole thing had died off about six months ago, then the local 60 Minutes did this interview with a Melbourne developer and asked him about the smashed—he said, "No, you can't have smashed avocado and buy a property." It was off again. The American *60 Minutes* picked it up, ran it throughout America, and now the Americans will refer to the, "Avocado toast generation". It all comes back to that one column, showing of course, a sense of tension, if you like, between the generations, which I think is very real, right across both America and Australia.

Here is where prosperity is created in the 21st century. Between November 2000 and November 2017, the Australian economy has added 3.9 million jobs, full-time, part-time, good jobs, bad jobs. I'm interested in broad-brush, high-altitude demographics. We lost; let's call it 300,000 jobs. Alcoa closes in Geelong, that's a 1,000 jobs. Queensland Nickel closed in Townsville, that's 250 jobs, but does that mean for every job we have lost thus far in the 21st century we've created 12 others? 12 to 1, that's good real action. When I do this for America, it's 6 to 1! 12 to 1; where else would you rather be on the planet thus far this century? We've created 3.6 million jobs in 17 years. Where are those jobs? Well that would be up here in healthcare, 800,000 out of 3.6 mill, is that 20%? 25% or so? The oldest baby boomer is what 68? 69? Is this the space to be in? Absolutely.

Healthcare, construction, professionals; never look at the numbers. The Australian people are talking to you through this chart and they are telling you where prosperity lies. In order to share in the prosperity of modern Australia, you need to play in this space; you need either a university degree or technical training. These are knowledge workers, in fact. Where do you not need to be? Well this will be down here, manufacturing. We have outsourced that functionality to Guangzhou. Then agriculture; well, we're producing more agricultural output than ever before, we just don't need the labour in the regions. This is unskilled work, this is skilled work. This is them, this is us. "How did you bastards get to be so rich?" The greatest threat, I think to Australia is this issue of willpower; a galvanised nation is the opposite of a divided nation. Almost a Blade-Runner rich world of the haves and the have-nots of gated communities. I think Australia works better when everyone believes they have a chance at prosperity.

National unity: a galvanised, focused people working hard, paying tax and all pointing in the right direction; that to me is the strongest way of securing our long-term future. What jobs have diminished most thus far this century? The job of photographic developer and printer. It's instructive but I feel it necessary to explain to the millennial generation exactly what this job involved. Prior to digital cameras you used to take your film into a chemist in a Australia, they'd send it off, two weeks later you'd get 24 colour photographs. There were 5000 people employed in that job in the year 2001, it's down to less than a 1000 today; complete digital disruption. Does that mean that there are 4000 people sitting at home festering and fomenting revolution or have they been redeployed? I say they've been redeployed. That, to me, is the great strength: the agility, the redeployment of disconnected, disaffected, unemployed disruptive workers; that is the great opportunity for Australia, the great opportunity and threat.

Word processing operator: there were 14 000 of them, in the year 2000. Over the last 15 years, everyone has learned how to type. No need for a word processing operator, everyone has learned how to talk. Sewing machinists: well those jobs are now done in Guangzhou. What jobs are being created? The job of barista, of course. This is why I love demographics. We might be losing sheet metal workers by the thousands, but we desperately need 37 000 baristas on the Australian continent. The word, barista, was not acknowledged by the census as a job prior to 2006. The

boffins in Belconnen said, "I think there's a job called barista, let's run it in the 2006 census". 8000 Australians said, "Yes. I am a barista". It's now 37 000. What this shows is that, within 10 years, you can have a job that no one has even heard of and, ten years later, 40,000 Australians said, "Yes. That is my job."

What job in 2028, which we have not even heard of today will exist? Agility, adaptability, these are the great traits that will ensure Australia's future. Yes, we need the defence issues, all those sorts of things, but there are soft cultural shifts. A united nation, an adaptable nation, that's what I'm seeing in these figures. It's never the numbers. If you're just looking at the numbers, you're not seeing enough from the census. Management consultant or truck driver: I think we're actually passing peak truck driver right now, with the driverless vehicles we'll see steadily emerge over the next two censuses, over the next 10 years or so. And so, do 137 000 truck drivers sit at home festering and fomenting revolution, or can we as a nation, as a people, as a society find a way to redeploy those people in a meaningful and gainful way to make a contribution to Australian society? That to me is legitimately part of holding us together and creating a strong nation into the future. There are two sides, the hard side and the soft side. This is the soft cultural side of creating a stronger nation.

Here is the Defence Force in 2011: 73 000. I don't know whether that's exactly right or whether—so people were asked, "What your job was and what industry?" 73 000 Australians said they thought in the Defence Force in some way. In fact, it's more than the number of people actually in the Defence Force; the age profile, so about 14 000 in their early 20s. Here's five years later, so it's up around about 2% or so, that should be +3% in fact. Here's a little gap there, a little gap there. Engaging Generation Y or the Millennial Generation; there's enough of them, you can actually see the pipeline, but actually getting them into the Defence Force is part of the great issue going forward, and a slow ageing of the population here, at big, broad brush sort of level.

Just finally, some key points about the millennials; these are the 20-somethings effectively, around about six million now, six and a half million by 2025. They have never experienced a recession and think of unemployment with a six in front of it as outrageous for the most educated, the most widely travelled, the most digitally connected community in history; the most ethnically diverse generation of Australians, pretty much ever, you would say and famously changeable, adaptable. The criticism of this generation by the baby boomers is that they can't settle to anything, but in actual fact, if you think about the skills that are required in the 21st century, it's about adaptability, flexibility, agility, fit in ability; and many of those qualities I see very much marking the characteristics of that generation.

To me, I think that the issues are as much around soft culture, a united nation of Australians, a prosperous Australia, an ambitious and aspirational Australia, all of those factors unite us and create a much stronger nation to support our defence force into the future.

Thank you very much.

Air Force Next!

Air Vice-Marshall Gavin Turnbull, AM

Thanks, Chewie. And as, a third of the room just discovered, it was 81 Wing, not 82 Wing.

Sirs, ladies and gentlemen, it is the second-last chat over what I believe has been a very successful two days. What do I do as the Deputy Chief of Air Force in following the professional presenters that have gone before me? Will I speak with hubris? No. I speak as a Deputy Chief talking to you about where we're going with Air Force and I'll speak a little bit more about some reflections on the speakers as I get toward the end of my particular part of this.

So, we framed this conference as—each third conference we do—it becomes a higher-level activity and we like to speak at the strategic level. And I think we have achieved that this time with a cogent flow of speakers, through the themes that we wanted to explore; that being the exploration of disrupters that will affect our national security, our military, and our air power policy and practice into the future. I think we've done it usefully and I think we've done it practically, raising the level of knowledge across the strategic space in the room, and about the disrupters that we may face. And I'm primarily directing those comments to everyone who is sitting in the back two-thirds of the room.

Disrupters, like most things, are a double-edged sword. They reflect opportunity for the wise and clever—— and there are risks for those who are not wise and clever. Due diligence in choice and implementation is needed to affect a right balance and to rebalance over time, particularly for those systems and technologies, which can turn on their creators if not properly controlled.

For a smaller air force like ours, we have to appreciate what current and future disrupters means to us as a large measure of our effectiveness while the central combat provider of air power is gained through efficiency. Our population size and geography limit our ability to generate air power through mass, thus making efficiency an essential element of our force design. That's not necessarily as important for larger forces where mass can remediate inefficiency. For us, needing to be efficient drives innovation that is the hallmark of our Air Force transformation to Air Force *Next*.

Our tyranny of distance and our geostrategy dictates that we will transit and fight at distance. Australian regional operations will be maritime-focussed and we are archipelagically based. This both a blessing and a challenge and is why we place importance on effective reach, global manoeuvre, and maintaining a balance between partnering and independent action in our force design. This approach is unusual in smaller air forces and equally true for our naval and land forces.

We don't pretend to have all the answers. Many challenges have been posed over the last two days, some international, some domestic some- not onlyjust military. But we do need to be able to provide advice to government on the national effect on security posed by some disrupters so that leading policy can be formed. It's fair to say we do have a plan, which will provide the government with choices about the options needed to address the central challenges that the Royal Australian Air Force and its partners may face into the future. As the Minister for Defence noted yesterday, science fiction can become fact very quickly.

Our plan is to transform into a Fifth Generation Air Force that is fully networked, integrated, with inter-joint operations and agile in thought and operational implementation. We will develop a force by design that will provide the effects necessary to prevail against the increasingly complex and lethal threats present in the information and warfare age. We will maximise the potential of our current capabilities and those yet to enter service, to generate a new mindset built around networks that harness both the individual and collective potential of the systems.

The Air Force strategy, as discussed by the Chief of Air Force at the start of the conference, deliberately sets the goal of Australia becoming one of the world's Fifth Generation Air Forces as our aim point. It's a pathway where we have decided to invest for our future and not just talk about it. To realise this transformation requires a significant reformation within Air Force.

This is the reformation that will represent a step change in our approach to the delivery of air power, both technical and intellectual, and a step change in the way that we develop and interact with our workforce and our partners in security and military operations. We are not undertaking this reformation because we needed a challenge. We are reforming in response to the rapid change in the strategic circumstances in our region, many of which we have heard about over the last two days.

The conference highlighted many of the strategic disrupters that shape our future world. I'm not going to repeat these but I will reflect on them toward the end of my speech this afternoon. I will say, "rock on pensioners," and I'll say that again later on. Rather, I'm going to talk about our plan to shape our Air Force so that it will be ready for whatever the world presents.

So we began this journey back in 2000. We planned and designed and acquired a networked Air Force to conduct operations, which we described back then as beyond joint. Today, we call those operations integrated and, since then, we have moved on. We've invested in the machines to realise our intent, to enable us to exploit network systems early and well and connect to our partners in innovative yet disciplined ways.

In 2014, we publicly launched Jericho and we have used it as a catalyst to explore and induct solutions to high value and complex problems and opportunities that are either preventing the transition to an integrated Fifth Generation Air Force or pushing it. And our Jericho team are hiding in here today, taking copious notes, after which they have now copious tasks to come.

Our next evolution, Plan Jericho 2 or 2.0, however, you would like to say it, will seek to accelerate the transition by identifying and exploiting disruptive innovations to deliver capability advantages and develop generational change in organisations and our workforce. Mmm hmm, can I have the next slide please up in the box? Thank you.

To develop and exploit a sophisticated understanding of what it means to be that future Air Force, and to provide signposts for our pathway, we have chosen to view Air Force Next with five attributes: agile, integrated, resilient, collaborative and informed. Next slide please. Thank you.

So, what is agile to us? We know that to transition our Air Force we must be able to quickly adjust and adapt to exploit emerging technologies, if we are to maintain a war fighting advantage in dynamic and uncertain environments.

The war fighting advantage I refer to is not that of past generations. The pace of potential adversary capability evolution and its underpinning technologies can rapidly erode any advantage we may have. We need an air force that can rapidly identify, adapt to and plug emerging gaps, as well as simultaneously seize opportunity.

This type of agility is an attitude as much as an attribute. If we are to deliver air power that is effective in future environments, we must think differently about how we apply that air power. We must fight the adversaries' capabilities and supporting systems, kinetic and non-kinetic, not just their platforms. We must consider non-traditional and asymmetric applications of air power as the new normal, while still delivering on enduring convention.

As part of agility and at the heart of the reformation of our air power capabilities will be our people, not an unusual theme. They are the ultimate disruptors on one hand and the antidote to disruption on the other. Our people are the ones that turn complex, connected machines into instruments of national power. And when I refer to people who deliver air power, I'm not referring just to our aircrew.

Our people are the communications operators who secure and maintain our EW and cyber networks that are so critical to our way of life but so easy to disrupt if we are not careful. They are our medical staff, technicians, engineers, logistics teams and operations officers, and these are just some of the wide variety of personnel that we train and employ. They will be people trained and educated to work together as a team, people who are practiced in the operational art needed to prevail in a complex digital age, the people who are also resilient enough to cope with and adapt to reversal.

This workforce is being recruited today. The rate of social and technical advances produced a generation of school leavers with a greater propensity to embrace change than those in the past. As we heard just with the last speaker, they are highly adaptable. We must ensure we can recruit from this generation those who have potential to excel in both our traditional air power roles as well as new-age capabilities. They will be both innovative and disciplined in their approach. Now this may sound simple, but the marketplace for this group is becoming increasingly competitive. One of the benefits of a modern, exciting Air Force with new platforms is that we are attractive and we need to leverage off this attractiveness for the current generation.

But attracting the right people is only the first part of the challenge. We need systems that reflect the new generation, and the submarine example was a good one. Thus we are developing a total workforce framework that will bring the required skills, accelerate our requirements definition and create a more appropriate remuneration packaging system, flexible employment, adaptive training and all other aspects necessary to develop our future personnel needs.

We are already seeing requirements for an agile framework in areas such as cyber, intelligence and our incoming high-end capability workforces. This trend will grow and our personnel systems must evolve to keep pace. The shift in our workforce framework and the professional culture that we aspire to in the Air Force will be a journey of many years. It's one we are already on and an agile workforce is essential to realising the potential of our new generation of networked air power capabilities.

For years our Air Force has developed in stovepipes we call Force Element Groups, or FEGs, where we manage like capabilities. We tried once in the past to break free and failed. Through the FEGs we are really good at individual tactical air power capabilities. They have served us well but perhaps we need to think harder about the enterprise structure we need to generate and sustain an integrated force. Perhaps we won't fail the next time.

We've been talking about network-centric warfare and the importance of integrated operations since 2000, but we have struggled to generate the cultural mindset or technical ability to realise

either. We lack the tools, mindset and focus to make the transformation. We needed a catalyst to create and sustain a transformational imperative.

The F-35A is that catalyst. It began as the only advanced platform on our horizon but is now one of the many tools driving the cultural and intellectual change we need. It is our other new connected capabilities that are the technical step change we have been looking for. The F-35A's capacity for networking, and its ability to fuse data and present information to the pilot and others on the network, changes the way we must consider the kill-chain and how we design and manage operations. But I just alluded to the F-35 being only one element that is driving this reformation inside our Air Force.

Our EA-18G Growler electronic attack systems are a significant forcing function for change. In the digital age, the electronic spectrum and the information it bears will be an integral part of warfare and an essential one to master. Growler is essential to Australia's force-level electronic capabilities and is both a military and national asset, useful in peace as it is in war. Again, at times, Air Force has talked a good game on its use of the EW spectrum, but we could never truly master it as a combat effect that covered the spectrum of operations. With Growler that is changing now.

The Growler is both halfback and forward in an airborne electronic attack realm. It can carve out a single slice of the adversary's EW spectrum or it can block large swathes. It's greater—it's part of a larger system to disrupt our adversaries and it's something that we have not had to deal with in the past and we need to be careful that we don't shut down our own systems in the process.

The Growler is a complementary capability to our other network systems but, particularly the F-35, the P-8 and the E-7A. It may be surprising to some in the room to realise that our E-7 is over 15 years old. In its own way, it was a catalyst for change. It provided commanders with an agile air-battle management system being integrated across the joint force. It has provided our Air Force with tangible experience of how technology could support and speed up all force decision-making in a highly complex and dynamic environment. We took a risk on it and, before it was fully operational, we deployed it to the Middle East where it has proven its worth. We've now commenced the next phase of the Wedgetail development through a program that will improve its utility for ISR and Command and Control missions. It's an exciting space to be in.

The P-8 Poseidon maritime patrol and surveillance response aircraft, like the P-3 before it, has acknowledged that we are a maritime nation; we must be vigilant in our maritime environment. The P-8 provides Australia with greater risk and enhanced capability to respond to challenges in national waters and global maritime commons.

To some, it may simply look like a P-3 replacement but that would be wrong. The P-8 has already taken our maritime surveillance capability into the networked age and has already surpassed what the P-3 can do; it's at the beginning of its development cycle. Like the P-3, the P-8 will have surface and sub-surface sensors, as well as a modern weapons suite. But it is what it does with the sensor data that makes it different.

Through an on-board system to come in the future called Minotaur, we will witness a revolution in data and track fusion for that platform. On-board sensor data will be fused with networked data that may come from other air, maritime, land and potentially space-based systems to feed its own weapons or the network-capable weapons in the battle space. If you look at our force mix, we are a hybrid, primarily US-Navy-generated platforms. It makes us an interesting customer for both the USAF and the US Navy.

Now if that wasn't enough, the P-8 is also air-to-air refuelable. It increases its persistence in the battle space, enabling it to reach out to locations previously not accessible, generating mission lengths that will be limited by human endurance and not the endurance of the platform. Network surveillance and control agility through these new capabilities will ensure we can fight, shape and respond over water and land from search and rescue through to high-end combat operations.

In network combat operations, Command and Control's focus should be on the effect needed at the target, physical or virtual, and not so much on who or how. Mastering who and how is necessary, but is not sufficient if we are to prevail in the contemporary and future conflict space. Mastering the orchestration and delivery of networked effect will require our C2 to be fully cross-domain. We must be able to link, sync and integrate capability for effect across the joint and combined space.

Further, we, the Australians, wish to be part of the design of the next generation of coalition C2 systems. We seek them to be scalable to a large and small force, scalable for military and security operations, scalable for security access, scalable to national or international leadership, effective in networked and rapidly evolving operations, and not people-heavy. We don't want much. It should be easy, right?

Our investment in the next generation of C2, currently in analysis with the Jericho team through our collaboration with MITRE, will look to realise real-time operational decision superiority. And for the Jericho boys, if you have your pens out, that includes AI.

Good decisions are made by people whose skills are developed and tested through effective education, training and practice. We are beginning to implement the latest in education and learning technologies to emulate some of the characteristics of the networked cyber capabilities that Air Force will be operating into the future. Whiteboards and PowerPoint are not effective. The learning generation does it differently, on their iPad and in the cloud. The evolution in gaming technologies for simulation opens an entirely new world for operational education, training, assessment and practice. Simulation is a technology that enables people to practice command for operational as well as technical mastery across the networked force at low cost, and it's a technology we are investing in.

We are embracing live, virtual and constructive environments. We understand that live, virtual—live test and training is—is expensive and standing up a whole network force is a rare occurrence. Nor can the full capability of the force be exposed. Through LVC environments we will generate the scale, complexity and fidelity required to emulate modern networked systems and platforms.

Air Force is committed to significant enhancement to key ranges and LVC capabilities in order to establish the advanced test and training environment. This is an environment that's built predominantly around Woomera and Delamere and further enhanced through the interconnected and integrated simulation assets, which allow our high-end platforms to train together in the virtual environment.

As well, we are committed to the provision of training facilities capable of replicating the advanced electronic threat scenarios. All of these systems are mobile and networked and, when coupled with a mature, integrated LVC system, they will provide the ADF war fighters with a realistic scenario required to maintain the combat edge into the future.

Air Force will maximise its effectiveness through the deliberate integration of capabilities across the services, regardless of their developmental generation, against an assessed priority and need.

A contemporary air force will not survive if it communicates, senses or fights at the speed of its oldest asset. Our Air Force will only realise its potential if we integrate our older capabilities with those being introduced now, again, a not uncommon theme throughout the last couple of days.

We cannot afford to develop capabilities without understanding its place in the network. This is why our approach of a force by design is so critical to us. We understand that integration reduces ambiguity, but we have learnt the hard way that add-on integration post acquisition is outrageously expensive and you buy a lesser product. We can and will leverage innovation so that challenges are viewed as the art of the possible, not just the art of the preferred. And opportunities will be viewed as the means to gain combat advantage, even if the advantage is transitory.

We recognise that integration does not have to be perfect, but it does need to be right. And it needs to be right enough to be resilient enough to stand up to the reality of conflict, where chaos and violence remain the defining characters.

Future contested environments may come in many forms but, in future conflict, we should expect attacks to be simultaneous on many fronts. We must be able to recover when hit, whether that hit is kinetic or non-kinetic. Our people, processes and systems must be tried and tested to be resilient, coherent and competitive despite the shock of conflict. They must continue functioning effectively and provide options to win in complex contested environments. They must be designed and tested to degrade gracefully and recover swiftly in the face of challenge.

Adversaries are likely to apply new and unpredictable attack vectors that will test our force like never before. That is the product of a disruptive digital world. We need the ability to absorb shock, take a first blow and, if necessary, be able to punch back with sufficient weight to get the job done or to give the opponent pause in striking in the first place.

We should also be seen as unpredictable to the adversary; in fact, networked warfare properly mastered will appear orchestrated to us but utterly chaotic to those who are looking inside. They should feel unbalance and the effect because they cannot sense what is happening to them in the conflict space.

From our end, is it in the cyber and electromatic spectrum where we are most obviously vulnerable and where an adversary may strike first? Attacks may be subtle and well in advance of any traditional conflict, or in parallel. At the high end, we almost certainly can expect disrupted national infrastructure and communications to affect national military C2 and ISR. Through good design we will degrade gracefully and recover resiliently.

It is no secret that air power is delivered through air bases, whether those are major facilities, forward staging areas or afloat. We need to develop greater operational resilience in our bases, applying camouflage, concealment, deception and recovery measures.

We must be agile in our basing and the mobility of our supporting infrastructure. This concept is being actively explored in collaboration with the US under the Enhanced Air Cooperation program. In fact, in November 17, 40 RAAF and USAF personnel from our respective forces gathered at RAAF Base Scherger, right up on the northern tip of Queensland, and practised austere operations and austere base activation. And these bases form the legacy of some hard lessons that Australia learned in World War II about keeping all their assets in one place.

We have participated in the US–Pacific Air Forces' Agile Combat Employment exercises. These have informed both capability development proposals as well as operating concept designs for

Air Force expeditionary airfield operations. We are designing in the flexibility to manoeuver in our basing options to suit the threat.

We recognise that Air Force does not have the monopoly on good ideas; building an integrated force is a shared effort. We acknowledge and welcome that fact. We are an Air Force of partners and therefore an Air Force of seams to be managed. Proper management realises synergies; poor management opens those gaps further. Good adversaries probe for gaps and we are planning to close them by design.

National security challenges are becoming increasingly complex, demanding cross-functional teams to resolve. To meet that end, our people will have to develop strong personal networks, both within Air Force and among the broader Defence and whole of government space, our allies and the industrial world.

Domestically, I think the most fruitful form of collaboration is between the public and private sectors and here I mean industry. Industry owns the creation of the information and the technological edge that we seek, not Air Force. Air Force owns its realisation. Collaboration with industry is a surer way to develop and deliver that next big disrupter to counter disruptive threats.

Partnering with industry has long been a core element of our Defence policy through a number of iterations of the White Paper; however, we took a major step along this journey when industry was directed to be part of the Force in Being and was funded with an integrated investment program. We recognise the trusted places in industry inside Air Force. We understand its role in the national security enterprise; an example of this trust can be viewed in the classified briefings that the Air Force Jericho team provided to industry last year on the Air Force Operating Concept. This is our approach to delivering air power to the joint force for the next 10 years, at least.

You would have noticed that the dominant thread through my presentation has been people and systems—get some of that tash action—noting, of course, that our new platforms are systems in their own right because they are designed to be networked. I do not wish to understate the importance of material acquisitions in the delivery of our future air power, but it is our people, not only the machines, that will ensure we realise our goal of reforming Air Force into a networked, integrated force.

An informed workforce is central to our efficiency and thereby our effectiveness. As a medium-sized air force, an informed workforce is one that is strategically, operationally, tactically and technically aware of the effects they are to generate and their role as part of the integrated force. We have commenced a serious of high-performance programs and revised our professional military education and training—no groaning. Through coaching, mentoring and leadership, we will strengthen the resilience, mental health and well-being of our airmen and airwomen across the organisation.

Now, before I conclude, I just want to reflect on some of the lessons from the last couple of days, and I was stunned, having worked on the speech that I was going to give over the last two weeks, that it needed very little modification. Did I change it? No. I think what we achieved in speaking strategically across the last two days supports the strategy that's in place for Air Force, and I feel very comfortable in that regard.

A few things to be cautious of: binary thought is a slippery slope; hubris needs to nothing good and complex problems require calmness; the Canberra consensus is something that is what it is

and we need to be aware of it; complacency is a serious problem for Australians because that's just who we are sometimes; and an absence of strategy is a dangerous way to run a country.

I particularly liked and I—and the Chief remarked at the time that—when Mark was speaking just recently, "Trust your people in the comms space; accept the occasional disruption of screw-ups because the balance of advantage is on our side". It also requires some courage and some leadership.

If you apply disruptive technology to the military and you compare those disrupters with what you currently have, you are missing the point. We can hold on too tight.

And finally, to good old Bernard who always provides an amazing insight into what Australia actually looks like compared to what we think it looks like. I know that I can get a good coffee while a management consultant uses my watch to tell me the time. And we are intimately changeable.

So, I started by describing Air Force's strategy vectors in which we will invest so that we can transform an air force into an air force that is networked and integrated. We'll deliver air power for the joint force to ensure Australia's security. We are making the investments in leading-edge capabilities, and in partnerships, critically, in our people, to take advantage of some of the disrupters highlighted over the last two days. We acknowledge that we don't have all the answers and that the last couple of days have provided a lot of food for thought and a lot of introspection to come over the next few weeks. And I encourage everyone in the back two-thirds of the room not to be buried back in your day job and forget what you have heard over the last couple of days. Mull over it, sip on it over a coffee, and use your own watch.

Our commitment to achieving this transformation runs from the most junior recruit through to the Chief of Air Force; however, the drive for strategic change ultimately comes through commitment and practice of Air Force's leaders. The Chief and I, together with the senior leadership team, have taken ownership of our reformation and together we will deliver what we have promised to the Australian Government. Government has trusted us enough to recapitalise the Air Force for the digital age. As has been pointed out, we have a unique opportunity to become an integrated force right now.

To exploit the opportunities offered and repay Government's faith in us, we now commit to meet the biggest intellectual challenge in our history: reformation for effect in the digital age. We owe that future a debt and we have already started paying it off. Thank you.

Closing Address

Air Marshall Leo Davies

Ladies and gentlemen, the tash is a constant in a disruptive world. Thanks, Gav.

This is my second and potentially the last time of closing our Air Power Conference, but in tradition of air evolution, I'd have to say this has been the most interesting, it's been the most intellectually stimulating and, for me personally, one of the most enjoyable of those conferences. So, I'd like to thank everyone here for the part you played in making that so, particularly to our sponsors: to Boeing, to L3, to Rolls Royce and to Defence Bank for making this conference possible.

When planning really began for this event, my direction to the organisers was that I wanted the presenters to challenge our preconceptions and, where appropriate, to be critical of Defence, broadly, but also particularly to be critical of Air Force because, in this disruptive world, we cannot indulge, as we have heard over the two days, in just using today's lenses. We need to see the realities to the complexities without eluding the challenges that we need to address. The speakers over the last two days have certainly met my original intent.

Deputy Chief has done an excellent job of drawing together the issues that have been raised over the last couple of days, so I won't rehash what he's already covered. I would however like to thank the individual speakers for their efforts in preparing such excellent presentations, for their travel to Canberra and their ability to, like I've never really heard in too many places before, the ability to present on complex issues in a way that was relatively easily digestible and, in many cases, frank and fearless.

Despite the best efforts of the presenters, it is however nearly impossible to leave this conference with a complete understanding of all the elements that were covered. Therefore, I encourage you. I encourage you all to continue engaging with each other on these topics and to do that long after we leave here today. So, to support you in that future discussion, the conference planning team have ensured the presentations will be published and distributed to all that would like a copy.

The contributions have deliberately had a future capability and disruptive technology focus and, as the Minister highlighted in her opening address, we are already living in a disruptive world, so we need to adapt to, and evolve within, it.

Since I joined the Air Force in 1979, my life, like yours—I lost my mother, my younger sister to cancer, my career—heck, they made me the Chief; that's disruptive. And the Air Force itself has been disrupted many times. I've witnessed a number of pivotal events that have required the Australian Defence Force to adapt. We adapted at the end of the Cold War, again in our involvement in East Timor, the Bali bombings, the 9/11 terrorist attack in New York and, of course, more recently, the emergence and the defeat of ISIS.

But it's not just these type of events that cause or enable disruption. Technical advances are similarly significant. The exponential rise and the prominence of social media such as *Twitter* and *Facebook*, as well as near real-time news reporting, continues to change how we communicate, consume and process information. These online platforms are readily available; they're relatively simple and have the ability to be used to our advantage. But they do expose us to far greater public scrutiny and can be used tactically against us, as we have heard.

Our world is changing fast and it will continue to do so. Ten years ago, smartphones, *Facebook* and *Snapchat* were just emerging. Now they are defining our age. With these as exemplars, we need to identify opportunities to innovate and to be creative in solving the problems we face today and those we might face tomorrow.

I ask all of you here, but particularly the members of the Australian Defence Force, how can we operate within disruptive environments? We need to use disruption to our advantage and to learn to deal with its effects as a degrading factor to our operations. In my view, we need to experience failure in training, not an 8v8 in a traditional sense, but an 8v we don't know.

Any smoothly run conference—and this year has been exactly that—is only made possible by a lot of frantic activity initially, both in the lead-up to and during the event. Many people have worked long days over many months to shape this conference. I however would like to particularly recognise the tireless efforts of Miss Sandra Finney and her team in what they've contributed, what they've worked on, and what they've delivered to produce what I'm sure you'll agree has been another very successful conference. Ladies and gentlemen, could I ask you to join me in congratulating Sandra and the organising team?

I'd also like to thank our MCs. Air Commodore Steve Edgeley and Mark Green have kept the program running along very smoothly—thank you—ahead of time, at times, which in conferences I've attended is a pretty rare thing.

To our international guests, ladies and gentlemen, I'd like to echo the Minister's opening words, highlighting that we all need to take an international approach in responding to our regional and our world events. As Chief, I have made international engagement one of my five strategic vectors that will enable the Royal Australian Air Force to truly become a Fifth Generation fighting force. This recognises that we collectively need to understand both technical and operational issues, so we can cooperatively ensure a stable and secure global force. That is what makes your presence at this conference so important. Thank you for your participation over the past couple of days and I wish you all, those that are travelling, safe travels home.

And with that, ladies and gentlemen, I'd like to close the 2018 Royal Australian Air Force Air Power Conference. I thank you very much for being with us and hope perhaps to see you at the Williams Foundation event tomorrow and perhaps at Avalon in 2019. Thank you very much ladies and gentlemen.