ISSUE NO. 297 – THURSDAY 24TH APRIL 2014

ADM AUSTRALIAN DEFENCE MAGAZINE

DEFENCE WEEK

SUBSCRIBER EDITION NEWS | INTELLIGENCE | BUSINESS OPPORTUNITIES | EVENTS

IN THIS ISSUE

NATIONAL NEWS

INTERNATIONAL NEWS

PUBLISHING CONTACTS

ACTING EDITOR
Nigel Pittaway
Tel: 0418 596 131
Email: nigelpittaway@yaffa.com.au
Editor Katherine Ziesing is on maternity leave

SENIOR CORRESPONDENT
Tom Muir,
Tel: 02 6291 0126
Email: tom.muir@homemail.com.au

PUBLISHING ASSISTANT
Erin Pittman,
Tel: 02 6203 9535
Email: erinpittman@yaffa.com.au

MANAGING EDITOR
Judy Hinz,
Tel: 07 3348 6966
Email: judyhinz@yaffa.com.au

SUBSCRIPTIONS
Martin Phillpott,
Toll Free 1800 807 760
Email: martinphillpott@yaffa.com.au

Go-ahead for F-35 purchase

Tom Muir

Australia will buy 58 more Lockheed Martin F-35A Joint Strike Fighters (JSF) at a cost of more than $12 billion after the Federal Government gave the go ahead for the purchase yesterday. The extra aircraft will bring Australia's total Joint Strike Fighter force to 72 aircraft, with the first aircraft to arrive in Australia in 2018.

The $12.4 billion price tag makes the Joint Strike Fighters Australia's most expensive Defence asset.

The Government says it will also consider the option of buying another squadron of the next-generation fighter jets in the future, to eventually replace the RAAF's **Boeing F/A-18F Super Hornets**.

Prime Minister Tony Abbott, who formally announced the purchase on Wednesday, says the JSF is the most advanced fighter in production anywhere in the world and will make a vital contribution to Australia's national security.

"Together with the Super Hornet and Growler electronic warfare aircraft, the F-35 aircraft will ensure Australia maintains a regional air combat edge," he said. "The F-35 will provide a major boost to the ADF's intelligence, surveillance and reconnaissance capabilities.

"The acquisition of F-35 aircraft will bring significant economic benefits to Australia, including regional areas and local defence industry."

▶▶▶

The first Joint Strike Fighters will arrive in Australia in 2018 and the first squadron will become operational in 2020. As part of the announcement, more than $1.6 billion will be spent on **new facilities** at air bases in Williamtown in New South Wales and Tindal in the Northern Territory.

But a specialist in US defence strategy has questioned whether Australia's purchase is good value for money. The **Brookings Institution's Michael O'Hanlon** says the aircraft may not be best suited for the military options Australia has found itself undertaking in recent years.

"If you think more about your military needs being the Afghanistan-style operations, the troubled waters of the South China Sea, counter-piracy, peace operations, keeping some degree of regional calm with some turbulence in the ASEAN region but not necessarily China, then frankly it's a debatable proposition whether the F-35 is the best bang for your buck," he said.

"If you want to be in the high-end combat aircraft business, the F-35 is frankly about as good of a deal as you're ever going to find. But if you think that that kind of high-end threat is not realistically where you're headed with your military requirements, then it's more of a debateable proposition."

Vertical Launch System installed in AWD01

Six strike-length missile modules for the Hobart Class Vertical Launch System (VLS) were this week installed into Ship 1 *Hobart*, marking a significant Combat System load out achievement for the Air Warfare Destroyer (AWD) project.

The **VLS MK41 modules** are a critical part of the Hobart Class Combat System which will enable the Navy's new DDG guided missile destroyers to execute air warfare and ship self-defence tasks. It is the first major Combat System element to be loaded into the ship following consolidation. Each ship will be fitted with six VLS modules, each containing eight cells, giving a total of 48 cells per ship. Each cell is capable of accepting, storing, preparing for launch, and launching either a single SM-2 Missile or four Evolved Sea Sparrow Missiles. AWD Alliance CEO **Rod Equid** said the VLS load out is the first multi-module VLS load out and has built on the in-country expertise developed through the Navy's FFG Upgrade Project which involved installing a single-module VLS. "Whilst

▶▶▶

the **Anzac Class** and **Adelaide Class frigates** have a single-module Vertical Launch System, the new Hobart Class destroyers will have a multi-module configuration that will provide more capacity for air warfare. It will also be the first configured to fire **SM-2 medium range weapons** and has the flexibility to support multiple missile types within a single weapon launching system," Equid said.

"Complex installation work, such as VLS, involves different groups working together to get the job done and has drawn on the technical expertise of the **Commonwealth of Australia, US Navy** and **Thales**. It has been a true representation of how the Alliance operates."

"The installation has been a coordinated activity between the AWD Alliance's Production and Test and Activation teams for the preparation of the VLS compartment and providing the subject matter expertise for pre-staging work."

The modules were taken out of storage from an Adelaide warehouse facility earlier this year and moved into the purpose-built Mobile Staging Platform located alongside the ship on the Common User Facility at Osborne for pre-staging work prior to installation. Following installation, the system will be operationally tested during the upcoming Combat System Light Off period. The acquisition of the VLS modules was made by the Commonwealth of Australia, through the **US Foreign Military Sales** program.

Defence Minister attends Jakarta International Defence Dialogue

The Defence Minister, Senator Johnston, travelled to Jakarta, Indonesia, March 18, to attend the fourth Jakarta International Defence Dialogue (JIDD) at the invitation of Indonesian Minister for Defence, Dr Purnomo Yusgiantoro.

He was accompanied by Chief of the Defence Force, General **David Hurley**, Chief of Navy Vice Admiral **Ray Griggs**, and Air Commander Australia, Air Vice-Marshal **Mel Hupfeld**.

The JIDD is an important regional security dialogue which this year has the central theme of maritime security in the region. Senator Johnston will join panellists from India, Japan, Indonesia, Republic of Korea and Australia to speak on the emergence of the Indo-Pacific. This is the first time an Australian Defence Minister has participated in the JIDD.

Among other issues covered in his speech Senator Johnston said:

"I have to acknowledge that there are some difficult aspects in our current relationship that are slowing down our ability to cooperate more closely. I regret that is the case, but I also know that both countries are working hard to clarify and resolve this situation.

"Ladies and gentlemen, I think it is vital for both our countries that we work hard to develop a closer partnership which strengthens both our countries' national interests. Australia and Indonesia are at our best when we cooperate. Whatever the momentary fluctuations in our relationship, we will be better off if we commit to help bring out the best in each other.

"That is a far better legacy to leave for future generations. Australia's interest is in having Indonesia as a strong, cohesive neighbour, with a high-quality Defence force able to promote Indonesia's interests. That is the best Indonesia for Australia, a strong neighbour, a close friend and a partner in security."

DSTO seeks submissions for S&T security policy

The Defence Science and Technology Organisation (DSTO) has released a consultation paper, the responses from which will inform the development of a national security science and technology (S&T) policy.

The program will focus on 'aiding, enhancing and future-proofing the **Australian Cyber Security Centre (ACSC)** capability; advanced tools and techniques particularly for ACSC transition of technology and processes to national networks; and establishing national S&T workforce and skills that are relevant and responsive to operational cyber security needs'. Consultations will conclude 1 May.

The government is seeking the views of stakeholders from all sectors of Australia's national security **science and technology (S&T) community** – including national

security government agencies (federal and state), universities, publicly funded research agencies, other research agencies and industry, to help develop a new policy and program management framework for achieving a whole-of-government approach to national security science and technology.

The policy will articulate the strategic direction for national security S&T over the next decade, and will provide the mechanisms to deliver a coordinated National Security S&T Program. The Program will involve multi-agency, multi-disciplinary collaborations, of short to long-term focus, aimed at delivering tangible operational and capability outcomes for national security user agencies.

National security S&T community stakeholders from government, academia and industry are invited to make submissions on the policy and program management framework, including proposed priority areas for national security S&T. A series of questions throughout this paper provide prompts that may help structure your response.

The government will consider all feedback received before finalising the national security S&T policy and program management framework. Submissions can be lodged per email: **NSSTC@dsto.defence.gov.au** or by Post: Director, Science Strategy and Policy Branch, DSTO, Department of Defence, PO Box 7931 Canberra ACT 2610. Submissions should be received by 5.00pm, 1 May 2014.

UXC partners with Senetas to deliver ADF security solutions

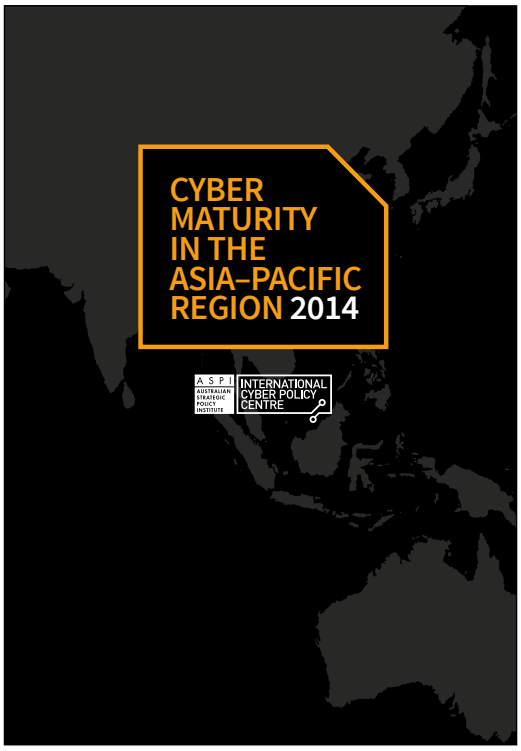
UXC Limited has announced its partnership with Senetas as part of a strategic initiative to provide the ADF with tailored data security solutions and services.

The partnership brings together the certified high-speed, defence-grade encryptors of Senetas with UXC's end-to-end ICT offering of advisory, consulting, and network infrastructure services and makes this solution available to UXC's Australian government and commercial customer base.

Senetas, an Australian public listed company, specialises in protecting data as it is transmitted across networks whilst retaining maximum network performance.

Cris Nicolli, managing director, UXC, said, "It is often assumed that data networks are inherently safe, but as the list of organisations affected by cyber-attacks continues to grow, it is clear that no company is immune. Data networks are vulnerable to security breaches. To be protected from a data network breach, cyber-attack or innocent routing error, organisations need strong encryption products.

Senetas CEO, **Andrew Wilson**, said, "With the number of data network breaches on the rise, we're encouraging both the business and government sectors to understand that the true cost of data breaches extends beyond regulatory penalties, and often includes financial losses, the damage to reputation and trust, and loss of intellectual property. Businesses must be proactive in protecting their customers' data and aware that they will be held accountable when that data is compromised."



ASPI launches cyber report

The Minister for Communications Malcolm Turnbull was on hand last week to help ASPI's International Cyber Policy Centre launch its inaugural *Cyber Maturity in the Asia-Pacific 2014 report* and interactive map.

The report looks beyond rhetoric of cyberwar and cybercrime, using the rubric of maturity to study the presence, implementation and operation of cyber-related structures, policies, legislation and organisations. The report looks at a spectrum of issue areas to build a more comprehensive understanding of the field and spur discussion and debate around how the region can constructively engage in cyberspace.

With the hope that the report will be 'suitably controversial', the International Cyber Policy Centre team welcomes input, comments, and criticisms. - *The Strategist*

Hostile network reconnaissance

Last week in *Defence Week Premium* we looked at DSTO's current area of priority defence capability interest and elaborated on what we thought might have been a solution to their extended range BLOS without repeaters.

ADM reported that improvements to the tropospheric scatter system – a method of transmitting and receiving microwave radio signals over considerable distances – often up to 300 km, might be the answer. A number of Australian companies have experience with troposcatter microwave systems although our example was drawn from US firm **Comtech Systems**.

This week *ADM* have been intrigued by DSTO's inclusion of 'battlespace awareness in the information domain' as a priority defence capability with the brief description that it might include the ability to conduct adversary network analysis to support time critical targeting and effects assessment.

But the reconnaissance and analysis of hostile computer networks goes well beyond identifying information for plinking by **M777A2 lightweight artillery**. Courseware

▶▶▶

on cyber-attack and cyber reconnaissance from the US Naval Academy provides an illuminating account through the various phases of cyber-attack which we find thought provoking.

According to the **USNA**, the goal of the first reconnaissance phase is to identify weak points of the target suggesting a successful military strategist would dedicate ample resources on reconnaissance to find weaknesses in the enemy's defences or to assess the enemy's capabilities. In either case, any information gathered about the target may be the crucial piece needed to reveal a critical weakness in defence or an unknown offensive capability of the enemy.

Gathering information without alerting the subject of the surveillance is passive reconnaissance. This is the natural start of any reconnaissance because, once alerted, a target will likely react by drastically increasing security in anticipation of an attack. Passive reconnaissance is commonly referred to as footprinting and, in context of a cyber-attack, means minimising any interaction with the target network which may raise flags in the computer logs. The best starting place is the target's public website. View the source html files to find any clues. Users may provide personal information on their company website or a social media site, which could give hints as to what their user account password is. Names can be entered in a white pages search to reveal home addresses and telephone numbers, which can expand footprinting to an employee's home.

If footprinting is like 'casing the joint', then active reconnaissance would be actually trying to open doors and windows to see which ones are unlocked. Active reconnaissance is commonly referred to as scanning. A simple scan would be to ping every IP address owned by the target network to see which ones belonged to real hosts. More sophisticated scans attempt a TCP connection with every port number of a specific IP address to determine which ports are open and, therefore, which services are running on the host at that IP address. Scanning is more intrusive than footprinting, but provides more specific information. There is also more risk that the target may be alerted to a potential attack since scanning results in more abnormal connections to target hosts, so it must be done carefully to avoid alerting the target network.

The goal of the next phase, infiltration, is to gain control of a host on the target's network. This is typically done by gaining remote access to a shell or terminal as the administrator on that host. Knowing a weakness is not enough to infiltrate the target; an attacker must discover a way to take advantage of that weakness. This does not necessarily require advanced knowledge and skill of computer programming, but having it can significantly improve the probability of success.

The goal of the final conclusive phase is to achieve the intended objective and back out leaving no trace of the trespass. In practice, this is the most difficult phase because computers keep records of every log-on, log-off, start-up, shut-down, network connection, program execution, and error received. With so many records left on every computer accessed, including routers, it is nearly impossible to eliminate all traces of an intrusion. Often times, an attacker will use techniques to deceive authorities as to the actual origin of the attack or attack from which the attacker will carry out the objective motivating the attack. Finally, the attacker may either terminate the connection, if no further access is required, or create a backdoor for future access of the target. - *USNA/edu*

Wi-Fi for our Squaddies too?

The Defense Advanced Research Projects Agency (DARPA) plans to extend connectivity for forward military units with the use of small Wi-Fi-hosting drones.

The aim of the **Mobile Hotspots project** is to provide a reliable, mobile source of bandwidth to all echelons of the military on a scale unthinkable using current methods.

DARPA has recently completed the first of three stages designed to test equipment vital to the success of the program. The first round of testing has yielded successful results for the steerable millimetre-wave antennas, which demonstrated their ability to swiftly acquire and subsequently track their target, thus creating a stable communications link between moving platforms.

"We're pleased with the technical achievements we've seen so far in steerable millimetre-wave antennas and millimetre-wave amplifier technology," states DARPA program manager Dick Ridgway. "The novel networking approaches needed to maintain these high-capacity links [will be the] key to providing forward deployed units with the same high-capacity connectivity we all enjoy over our 4G cell-phone networks."

Phase 1 also tested a number of other systems, including the signal and power amplifiers necessary to boost the Wi-Fi signal to the 50 km (32 mile) range required for the project. Systems also displayed 20 percent increased power efficiency that was achieved in part by utilising a single gallium nitride chip.

Arguably the most important piece of hardware to have been tested in Phase 1 was the **Low-Size Weight and Power (SWAP)** pod. All equipment vital to the Mobile Hotspots program will be housed in the wing-mounted pod, to be fitted on **RQ-7 Shadow UAVs**. In order to be viable for use in the Mobile Hotspots mission, the pod had to weigh less than 20 lb (9 kg) and have a power consumption of under 150 W.

The project bears many similarities to the recent initiative by Facebook and internet.org which, in part, proposes to increase global internet access with the use of its own solar-powered drones.

Phase 2 of testing for the Mobile Hotspots program took place in March, with the goal of further testing Phase 1 assets now integrated into the SWAP pod. The session was planned to conclude with a demonstration of four UAV-compatible SWAP pods, two vehicle-mounted pods, and a single fixed ground node. - *DARPA*

US/AUS logistics tracking system launched

The US Army and the Australian Defence Force (ADF) have jointly launched a new logistics tracking system in an effort to enhance logistical interoperability between the two countries.

Dubbed the **Pacific Radio Frequency Identification System (PRFID)**, the system features commercial technologies used for tracking of goods from manufacturers and warehouses to buyers; it uses the capabilities of the **NATO system** used for the automatic location and tracking of shipments bound for the International Security Assistance Force, in Afghanistan.

US Pacific Command logistics director and air force Brigadier General **Mark McLeod** said the system is designed to support the US Marine Rotational Force in Darwin, Australia, in addition to expanding military-to-military cooperation across the Asia-Pacific region.

Until now, the US DoD has been using barcode technology for monitoring shipments, from an aircraft's washers and nuts to armoured vehicles parts, throughout the transportation process and also to check inventory stocks.

The new system can read barcode information on both militaries' equipment and supplies using radio frequency identification technology, and the information is subsequently recognised and transmitted by the Australian RFID readers to the Nato routing hub, helping US logisticians monitor equipment or shipment deliveries.

"It gives everybody near-real-time access. When an individual supply-line item passes along a tracking device, it is automatically read up into a database and distributed," McLeod said.

Besides saving the US around $560,000 in deployment and installation of its own RFID systems in Australia in the next five years, RFID is also expected to support closer US-Australian interoperability during exercises, humanitarian assistance, disaster-relief missions and other contingencies.

In addition, the system, launched in April 2013, is anticipated to establish a framework that could be expanded to include more regional allies and partners in the future, according to McLeod.

The two countries have earlier tried to share logistics information through directly linked systems, but the project was cancelled in 2011 due to problems related to servers and accreditation processes.

Connick confirmed to speak at ADM Cyber Security Summit

Lynwen Connick from the Department of the Prime Minister and Cabinet has been confirmed to speak at *ADM*'s fourth annual Cyber Security Summit.

▶▶▶

The Cyber Security Summit will be held on the 19-20 June 2014 at the Hotel Realm, Canberra. The event has consistently attracted over 130 attendees and this year the Department of Defence, Prime Minister and Cabinet, Australian Signals Directorate and Attorney-General's Department have already confirmed their participation.

The program features international keynotes, panel discussions and networking opportunities where you will be able to hear about and discuss the following topics:

- Modern warfare
- Preventing the cyber theft of intellectual property
- People management in mitigating cyber threats
- Educating the cyber warrior

Click **here** for more information and to register.

ADM Online: Weekly Summary

A summary of the latest news and views in the defence industry, locally and overseas. Check out our webpage for daily news updates on the *ADM* home page and make sure you bookmark/RSS this for a regular visit.

This week, the team behind the **DSTO Future Land Force Conference** called for papers that describe innovative concepts, effective solutions to the ADF's challenges, and leading-edge technological advancements.

Lockheed Martin Australia confirmed delivery of its **MH-60R electronic warfare support system** to the Royal Australian Navy.

And, the British Defence Secretary has announced that the **F-35 Lightning II aircraft** will fly in Britain for the first time this July.

COMING SOON!
ADM May 2014

- Armed UAV for the ADF?
- DSTO MAV research takes flight
- Offensive cyber warfare
- ACSC to become one stop shop
- The emergence of 'cyber labs'
- Raydon Gates chief executive of Lockheed Martin Australia and New Zealand speaks to *ADM*
- and much more!

International

USAF yet to decide on Pacific JSF base

The US Air Force has yet to settle on a time line for basing F-35A aircraft in the Pacific theatre, according to a service spokeswoman, but a congressional delegation with a keen interest in the service's decision expects an announcement in the next several months.

Basing decisions are lengthy processes when conducted in the US, necessitating environmental impact statements and public comment periods, but they can take even longer when they involve foreign countries. The debate over which Pacific location to send operational **Joint Strike Fighters** covers both of those possibilities. Sites in Alaska, Japan, South Korea and Guam are being considered.

The Air Force's first two operational F-35 flying units will be stationed in the continental US - an active-duty unit at Hill Air Force Base, UT, and an Air National Guard unit in Burlington, VT. But the service has long maintained its next operational site, and its first outside CONUS, will be in the Pacific region.

Air Force spokeswoman **Ann Stefanek** said in a statement that the service has conducted site surveys at each candidate base in the **Pacific Air Forces (PACAF)** area of responsibility, yet she declined to name all of those bases or say how many candidate bases exist because of "host nation sensitivities." She also said a time line for selecting preferred host sites has not been determined. - *Inside Defense*

USN Littoral Combat Ship replacement task force named

In a story with implications for both current and prospective Australian shipbuilders and consortia, the US Navy Times reported "The effort to re-evaluate the Navy's small surface combatant program is underway under the direction of a new Small Surface Combatant Task Force (SSCTF).

As directed February 24 by Defense Secretary **Chuck Hagel**, the task force will examine the **Littoral Combat Ship (LCS)** and compare it with other designs, all with a goal to buy "a capable and lethal small surface combatant generally consistent with the capabilities of a frigate."

US Navy exploring common combat system for LCS variants

The US Navy is actively looking at a common combat system for the two variants of the Littoral Combat Ship, having briefed Navy leadership and conducted a business case for the concept already, according to LCS program officials.

"We have briefed Mr Stackley," Rear Admiral. **Brian Antonio**, program executive officer for the LCS program told reporters at the Navy League's annual Sea-Air-Space symposium in National Harbor, MD this month, referring to Navy acquisition chief **Sean Stackley**.

The program completed a business case analysis for the common combat system, but is still looking for a way to fund this idea, according to Antonio and other LCS program officials.

"We've got to identify the funding," he said. - *Inside Defense*

FORTHCOMING EVENTS.....page 13

FORTHCOMING EVENTS

For a full list of defence and industry events, head to *ADM's* online events page at www.australiandefence.com.au

ADM Cyber Security Summit

DATE: **19 - 20 June, 2014, Canberra**
ENQUIRIES: **ADM Events - Adam Wiltshire, Ph: 02 9080 4342;**
Email: adam.wiltshire@informa.com.au
Web: www.admevents.com.au
Over the last 2 years, the summit has gathered 150+ senior Defence, National Security and Industry executives to address current and emerging cyber threats to Australia's security.

ADM will be in attendance

Defence and Industry (D+I) conference 2014

DATE: **29 - 30 July, 2014, Adelaide**
ENQUIRIES: **Defence Materiel Organisation**
Email: DMO.Communication@defence.gov.au
The Conference is an opportunity for Industry to discuss with Defence officials acquisition and sustainment investment opportunities.

ADM will be in attendance

SimTect 2014

DATE: **25 August, 2014, Adelaide**
ENQUIRIES: **Web: http://www.simtect.com.au/**
SimTecT is the annual Simulation Technology and Training Conference held by Simulation Australia. Since its inception in 1996, SimTecT has grown to become Australasia's premier simulation conference for industry, government and academia.

ADM will be in attendance

Northern Australia Defence Summit

DATE: **15-16 October 2014, Darwin Convention Centre**
ENQUIRIES: **ADM Events - Adam Wiltshire, Ph: 02 9080 4342;**
Email: adam.wiltshire@informa.com.au
Web: www.admevents.com.au
Bringing together key figures from the NT Government, senior military figures, and senior industry representatives, this conference is all about the continuing development and support of Defence in the Top End. Hear about the current and new initiatives offered by Government and what industry can bring to support Defence's strategic objectives

ADM will be in attendance

New Zealand Defence Industry Association Forum (NZDIA Forum)

DATE: **21-22 October 2014, New Zealand**

In association with New Zealand Industry, Ministry of Defence and NZ Defence Forces. More details to come.

Land Forces 2014

DATE: **22 - 25 September, 2014, Brisbane**

The Land Forces 2014 conference is a major event for users, providers, academics, designers and manufacturers to meet, present, share and exchange new and visionary ideas on Land Systems. More details to come.

***ADM* will be in attendance**