ISSUE NO. 246 – THURSDAY 28TH MARCH 2013

ADM AUSTRALIAN DEFENCE MAGAZINE

DEFENCE WEEK

PREMIUM EDITION NEWS | INTELLIGENCE | BUSINESS OPPORTUNITIES | EVENTS

IN THIS ISSUE

NATIONAL NEWS

INTERNATIONAL NEWS

PUBLISHING CONTACTS:

EDITOR
Katherine Ziesing,
Tel: 02 6203 9535
Email: katherineziesing@yaffa.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,
Tel: 02 9213 8325
Toll Free 1800 807 760
Email: martinphillpott@yaffa.com.au

Articles by
Katherine Ziesing and Tom Muir

Army in 'great shape'

The Chief of Army, Lieutenant General David Morrison AO, has declared in no uncertain terms that "the Army is in great shape" but needs a return to "appropriate funding".

In an address to the Royal United Services Institute (NSW) in Sydney, LTGEN Morrison explained that under Plan *Beersheba*, the nation was well advanced in meeting its defence agenda.

He paid tribute to two of his predecessors who rationalised Australia's functional command structures to make Beersheba the next logical step by "enhancing the combat weight of the Army".

Today, the Army has three standard multi-role combat brigades, sustained by an aviation brigade, an intelligence/surveillance/target-acquisition brigade and a combat services support brigade, supplemented by six reserve brigades.

"It not only looks good - it is," LTGEN Morrison said. "Moreover, it extracts real value from scant resources. We can standardise our vehicle fleet and our infantry brigades.

"Our training systems and our career management systems no longer have to tailor our officer and soldier career plans to provide recurrent service in a single location such as Townsville, Darwin, Adelaide or Brisbane.

"So much of the narrow career profiles that our people had to follow are now a thing of the past. The cascading effects of this on improved family harmony, job satisfaction and career development, in my view, is encouraging."

He added: "Standardisation in place of specialisation will transform training.

"Indeed, the Plan Beersheba Army is already achieving considerable savings in every area of raising, training and sustaining land forces. And that has allowed us to weather what is a contemporary budget challenge."

"But without some return to an appropriate level of funding we will see a degradation in our existing military capability," LTGEN Morrison warned.

▶▶▶

New name for RGL

Repair Group Limited (RGL) have recently changed their name to Loop Technologies.

The business was founded on providing repair services for NZ's largest telecommunications company, their capabilities cover the full lifecycle care of technology hardware. They also provide a range of specialist services, including design, prototyping, training and decontamination. As a result, the business has grown through strategic partnerships with the major global technology brands.

For more information and to check out their new website click **here.**

Cyber threats for 2013

Newly arrived in Australia, BAE Systems' Detica has released its top five predictions for cyber security threats in 2013.

They are:

1. Further nation state cyber revelations - nation states gear up: An increasing number of nation states will have a credible level of cyber attack capability. For some this is a natural evolution of their military capability, for others it is part of the game of international espionage. Similarly, the actors behind these capabilities vary from the suited salesmen selling professionally developed toolkits like FinFisher, to hired hackers, complex networks of privateers and new cyber Armed Forces. The trail of digital breadcrumbs from cyber espionage has in the past revealed campaigns of ambition and scale which could only be conducted with nation state backing. Whilst it has been widely reported that Chinese and Russian threat actors regularly conduct cyber espionage against other nations' businesses, we believe 2013 will contain further revelations showing other nation state actors are also actively involved in this kind of international espionage and cyber warfare activity.

2. Professionalisation of a cyber attack industry: 2013 will also see the further maturing of a cyber attack industry, with clients paying cyber criminals for access to a company's secrets, rather than paying simply for the technology. We anticipate that a whole effective and efficient service industry will grow in this area offering tailored attack and information exfiltration services to those that wish to make use of them. Services will be engaged anonymously to order and the cyber goods delivered to the client's door, without the need to employ the technology themselves.

3. Increased attacks against the supply chain: As large organisations become aware of the threat they face, they consolidate and harden their defences forcing adversaries to seek alternative routes in. One method of entry is by exploiting

▶▶▶

trusted relationships with third-party organisations such as partners and suppliers. We have noticed an increase in this style of attack in recent months from sophisticated actors, and predict this trend will continue in 2013.

4. Deployment of 'adaptive security architectures': Likely targets are starting to recognise the need to be able to alter their security stance in response to credible intelligence without crippling the business. Effectively building in a 'paranoia dial' into their systems that allows them to turn the dial up in circumstances of high threat to reduce attack surfaces, move to more secure but limited configurations, move transactional processing from real time to batch and increase monitoring/response team availability. They will also require the consequent ability to turn the dial back down when the threat passes to increase business agility and reduce costs. This is something starting to develop in a few very large systems likely to operate under high threat, but will start to trickle down as the concepts are defined and documented.

5. Cyber crime becomes mobile-enabled: Until recently there were only a handful of major cyber crime malware families, such as Zeus and SpyEye. Leaks of source-code from these highly effective data-stealers has led to mutant variants, each with their own features and customisations to make detection harder. This trend will likely continue in 2013, as budding authors learn from past examples, and then compete with each other to develop more advanced and resilient malware. Combined with this, instances of attacks on mobile devices are increasing rapidly – most apparently in regions which are hotbeds of other malicious cyber activity, such as Eastern Europe and the Far East. However, recent proof of concept attacks such as that against the Samsung Galaxy could quickly be turned into 'in-the-wild' attacks by incorporation into one of many cyber crime exploit kits. These exploit kits are becoming increasingly cross-platform and the leap to mobile devices could cause an avalanche of attacks in 2013.

Australian interest in multi-role NSM for F-35

Tom Muir

Norway and Australia are funding a program to adapt the Naval Strike Missile (NSM) to fit the internal bays of the F-35. This will be a multi-role version, named the Joint Strike Missile (JSM), and will be the only cruise missile to fit the internal bays. Studies have shown that the F-35 would be able to carry two of these internally, while four additional missiles could be carried externally. The missile has an expected range in excess of 278 km.

The multi-role JSM will feature an option for ground strike and a two-way communications line, so that the missile can communicate with the central control room or other missiles in the air. **Lockheed Martin** and **Kongsberg** have signed a joint-marketing agreement for this air-launched version of the NSM, as well as an agreement committing both parties to integrating the JSM on the F-35 platform. The project is funded by Norway and Australia.

Improved features for the Joint Strike Missile include:

- Shape changed to fit in F-35 internal bay.
- The ability to attack sea and land based targets.
- An aerial launch platform (F-35).
- Improved range over NSM to 280 km.
- Long-term, production start in 2013.

The JSM will have multicore computers running Integrity real-time operating system from **Green Hills Software**. Kongsberg is studying methods to deploy the JSM from Norway's submarines (and Australia's future submarine?).

Australia and US want C-GBAD emitters?

Tom Muir

The US Naval Surface Warfare Center, Crane Division, is seeking prospective sources for surrogate systems able to emulate man-portable air-defence systems (MANPADS). The proposed hardware will be used to test aircraft-mounted missile warning sensors and to train aircrews in proper tactics, techniques, and procedures to be used against MANPADS. It didn't take ADM's Defence Week long to discover just what the US Navy wants, viz: DRS's Joint Man-Portable Air Defense System (JMANPADS) Trainer.

This is a man-portable, fully integrated lightweight Electronic Warfare (EW) trainer for enhancing rotary and fixed wing aircrew combat proficiency while countering today's lethal InfraRed (IR) MANPADS. Easy to use with minimal maintenance or operator training required, JMANPADS cost-effectively meets the unique operational training and After Action Review (AAR) requirements for unit-level aircrew survivability training.

The ADF is also looking for a mobile electronic warfare threat emitter system under JP 3021 which seeks to provide aircrew with the ability to train and mission rehearse in a Ground Based Air Defence (GBAD) environment. Training is currently only available to the ADF through use of overseas EW ranges and on an ad-hoc basis during joint ADF-Allied exercises, eg the recently completed Red Flag exercise at the Nevada Test & Training Range at Nellis AFB involving eight F/A-18s from the RAAF's 77 Sqn and two E-7A Wedgetail aircraft from 2 Sqn.

The RAAF also participates in Red Flag exercises at the PACAF Range in Alaska as well as benefiting from visits by the Joint Deployable Electronic Warfare Range (JDEWR) which was developed to bring PACAF's training capabilities to a wider audience.

JDEWR, a mobile Electronic Warfare oriented autonomous platform, is a system of systems that provide tactical-level training to participants in live training events around the world. Frequently, these events have limited or no range instrumentation or on-site training capabilities. JDEWR has been used to support multinational and joint exercises at weapon ranges in Thailand, Australia, and Canada, and unit-level training in South Korea.

Perfect storm for Defence?

In ASPI's latest Special Report, *Heavy weather: climate and the Australian Defence Force*, authors Anthony Press, Anthony Bergin, and Eliza Garnsey, argue that the downstream implications of climate change are forcing Defence to become involved in mitigation and response tasks. Defence's workload here will increase, so we need a new approach.

Heavy Weather makes a number of recommendations including:

- Defence should work with the Department of the Prime Minister and Cabinet and the Department of Climate Change and Energy Efficiency to establish an interagency working group on climate change and security. It would focus on addressing climate event scenarios for Australia and the Asia–Pacific to manage the risks those scenarios pose to national resilience and regional stability.
- Defence should appoint an adviser to the Chief of the Defence Force on climate issues to develop a Responding to Climate Change Plan that details how Defence will manage the effects of climate change on its operations and infrastructure.
- Defence should audit its environmental data to determine its relevance for climate scientists and systematically make that data publicly available. It should set up an energy audit team to see where energy efficiencies can be achieved in Defence.
- Australia should work with like-minded countries in the 'Five Eyes' community to share best practice and thinking on how military organisations should best respond to extreme weather events.

The recommendations aren't about Defence having a 'green' view of the world: they're about the ADF being well placed to deal with the potential disruptive forces of climate change-*ASPI*

Tarin Kot closure = Aussies home by end of year

The Prime Minister and the Defence Minister have welcomed the decision by the International Security Assistance Force (ISAF) to close Multi-National Base Tarin Kot in Uruzgan Province, Afghanistan at the end of this year, when the majority of Australia's troops will come home from Afghanistan.

The decision to drawdown and close the base at Tarin Kot was made after consultation with Australia, which leads Combined Team – Uruzgan, and Afghan authorities and is in line with the timetable to transition to full Afghan led security responsibility in Uruzgan Province by the end of 2013.

With the commencement of independent operations by the four Infantry Kandaks,

▶▶▶

Australian troops no longer conduct joint patrols with these ANA units. As well, Australia handed over control of forward operating bases and patrol bases to the 4th Brigade by the end of 2012. By the end of 2012, Australian troops had consolidated their presence at Tarin Kot and commenced planning for the complex task of redeploying Australian personnel and equipment and remediating buildings and facilities.

Australia will remediate the areas it has used and transfer the remaining infrastructure at the base to Afghanistan at the end of this year as transition occurs in Uruzgan and the Australian training and advisory mission in Uruzgan is completed.

Australian forces operate from two camps within the base at Tarin Kot, Camp Russell and Camp Holland. Camp Russell is where Australia's Special Operations Task Group in Uruzgan is located. Camp Holland is a much larger area where the remainder of Australia's military and civilian personnel in Uruzgan, including the Headquarters of Combined Team Uruzgan, live and work.

Planning has now commenced to transfer all of Camp Russell and a portion of Camp Holland to the Government of Afghanistan by the end of 2013.This is in accordance with the ISAF campaign plan and is being undertaken in consultation with ISAF and Afghan authorities. Australia has also contributed substantial funds toward the construction of permanent barracks for the Afghan 4th Brigade adjacent to the base at Tarin Kot.

The ADF role in Uruzgan will continue as at present until the end of this year:

- Australian troops will continue to train and advise at the Headquarters 4th Brigade level with the two Combat Support Kandaks and at the Afghan Operational Coordination Centre – Provincial in Uruzgan;
- The ADF Task Group will remain combat ready to assist Afghan Forces should the need arise;
- The Special Operations Task Group will continue to conduct partnered combat operations to disrupt the insurgency.

In 2014, the ADF will focus on a training role at the Afghan National Army Officer Academy in Kabul with British and NZ colleagues. In Kandahar, the ADF will continue to provide training assistance to the 205 Corps of the Afghan National Army.

Post-2014, Australia is prepared to contribute to the train, advise and assist mission for the Afghan National Security Forces by continuing to provide embedded Headquarters staff, advisors at the Corps level and trainers at the ANA Officer Academy in Kabul. Under an appropriate mandate, Australia remains prepared to make a Special Forces contribution, either for training or for counter terrorism purposes.

Prime Minister Julia Gillard and Minister for Defence Stephen Smith announced that the Australian Army's Special Operations Command will receive the first Army Battle Honour since the end of the Vietnam War. The Battle Honour is for outstanding performance during the Shah Wali Kot Offensive in Afghanistan from May to June 2010.

The Battle Honour, titled Eastern Shah Wali Kot, has been awarded in recognition of the operational actions of the Special Air Service Regiment (SASR) and 2nd Commando Regiment (2 Cdo Regt) from the Australian Special Operations Task Group Rotation XII.

The efforts of the SASR and 2 Cdo Regt during the engagement were highly commended by the International Security Assistance Force (ISAF) command for the contribution it made to overall ISAF efforts to disrupt insurgent activities in the region around Eastern Shah Wali Kot, one of their traditional stronghold areas. The Battle Honour will be formally presented to the Regiments later this year.

COMINT to provide specialist communications support to defence

Award winning aerospace and defence writer and journalist, Andrew McLaughlin, has established a new communications consultancy to support the aerospace and defence sectors.

Communications Intelligence, or **COMINT**, can provide organisations with the support and expertise required to effectively communicate with their key internal and external stakeholders, and with the media.

COMINT will initially be based in Sydney, Canberra and Newcastle, and can draw upon like-minded specialist communications professionals to provide additional support in Melbourne, Adelaide, North Queensland, and Singapore.

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.

Making headlines this week, the **Royal Australian Navy**, supported by the Royal Australian Air Force, conducted a highly successful maritime exercise with the Royal Thai Navy, demonstrating yet again how well the two nations can operate effectively together.

Elbit Systems Electro-optics Elop was awarded an approximately $80 million contract to upgrade **AFV** of an Asian customer.

Two RAAF E-7A Wedgetail aircraft from No 2 Squadron, RAAF Base Williamtown, recently deployed to Nellis Air Force Base in Nevada for the first **Exercise Red Flag** of the year.

International

F-35 Steering Board discusses integrating foreign weapons

The Joint Strike Fighter Joint Executive Steering Board (JESB) met last week to discuss integrating foreign weapons as part of a follow-on effort, according to a joint program office official.

The board consists of a group of four-stars from each of the three services involved as

▶▶▶

well as partner nations that make decisions related to where the program will be in terms of its configuration in the future, USAF Lieutenant Colonel **Jeff Geraghty**, lead representative for the system development and demonstration phase in the JPO's air systems requirements division, said on March 20 at an industry conference in Springfield, VA, sponsored by the Precision Strike Association.

"All of the partners have great interest in the particular country's weapons," he told *Inside the Navy* in a brief interview after his presentation. "The JESB has to get together and decide what's going to satisfy everybody, kind of a big plan for integrating weapons."

Geraghty used the example of the Joint Strike Missile, a munition capable of being carried in the aircraft's internal weapons bay and specifically designed for anti-surface and anti-ship warfare. Norwegian defense contractor **Kongsberg** and the Norwegian government, which is one of JSF's international partners, continue to press the JPO to integrate the missile, *InsideDefense.com* has previously reported.

In fact, the Defense Department and Norway's Ministry of Defence awarded a contract last summer to Lockheed Martin to conduct risk-reduction activities on the missile. The board will discuss integrating weapons as part of a two-phase Block 4 follow-on effort. Each phase would last about two years, Geraghty stated. Block 4a would concentrate on integrating the common weapons, while Block 4b would concentrate on integrating those unique partially common weapons like the JSM- *Lee Hudson/Inside Defense*

President of CDA, Dave Schmitz

Cubic appoints new defence applications president

Cubic Corporation has appointed Dave Schmitz as president of Cubic Defense Applications (CDA).

Schmitz succeeds Brad Feldmann, who was recently promoted to president and chief operating officer of Cubic.

"As president of CDA, Dave brings a solid track record of experience in defense systems," Feldmann said. "His extensive experience and leadership skills make Dave well-suited to help grow CDA's efforts globally. Schmitz is a seasoned executive with a proven track record in strategic planning and business management."

Most recently, he was vice president and general manager of **Cobham Sensor Systems** involved in technology applications supporting a variety of critical military platforms and systems.

US DOD to demand network breaches reporting

Pentagon officials will likely jump through the hoops of a federal rulemaking process to satisfy a new legal requirement aimed at forcing defence contractors with access to secret government information to report network hacking incidents to the Defense Department.

At issue is how - and when - DOD will establish implementing guidelines for the new requirement, codified in section 941 of the fiscal year 2013 Defense Authorization Act

The law, enacted in early January, gives DOD 90 days to establish requisite procedures, which would then take effect immediately.

"DOD is analysing the Section 941 requirements for implementation and is in the process of designating a senior official to oversee implementation," department spokesman Lt. Col. **Damien Pickart** wrote in an email to *Inside the Pentagon*.

"The department will likely publish a new federal rule, or amend current rules, to implement Section 941, which is a lengthy process. However, industry will be provided the opportunity to formally comment on the department's approach during the public comment period-*Inside Defense*

Spongy armour?

Given that scientists are already looking to sea sponges as an inspiration for body armor, perhaps we shouldn't be surprised that foam is also being considered ... not just any foam, though.

Unlike regular foam, specially-designed nanofoams could someday not only be used in body armor, but also to protect buildings from explosions.

Led by professor of structural engineering Yu Qiao, a team at the **University of California**, San Diego has been creating the foams by mixing pairs of substances together at a molecular level, then removing one of those materials via acid etching or combustion. As a result, the spaces formerly occupied by the targeted material end up as tiny empty pores within the remaining material.

The size of those pores is crucial, however. It was observed that when regular foams are subjected to a sudden, intense impact, the energy is absorbed in one localized area – this can lead to structural failure. When the foam's pores are small enough (but not too small), that energy is harmlessly dispersed over a wider area.

The structure of the nanofoams is composed of 50 to 80 per cent pores, which have ranged in size from 10 nanometers to 10 microns each. Those different grades of nanofoam are tested in a lab-based gas gun, that subjects them to increasingly strong impacts. They're subsequently examined for damage, using a scanning electron microscope.

While the research is still ongoing, nanofoams with a pore size within the tens of nanometers have so far shown the best ability to absorb impacts and blasts-*UC San Diego Jacobs School of Engineering/Gizmag*

FORTHCOMING EVENTS.....page 10

FORTHCOMING EVENTS

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

SEWG

DATE: **17 April 2013, Russell Offices, Canberra**
ENQUIRIES: **Lori Catelli, Ph: 02 6265 7108; Email: lori.catelli@defence.gov.au**
The sixth meeting of the SEWG will take place from 10.00am to 1.00pm. Respond by email by Thursday 28 March with the names and email addresses of those attending the SEWG meeting.

International Maritime Security Conference

DATE: **14-16 May 2013, Changi, Signapore**
ENQUIRIES: **More details to be released closer to the date.**
IMDEX Asia Web: http://www.imdexasia.com/index.aspx
IMSC 2013 will bring together Navy Chiefs, Coast Guard Directors-General and academia around the world to discuss threats to maritime security and safety, as well as develop frameworks and solutions to deal with the security challenges that threaten and disrupt sea lines of communication.

ADM Cyber Security Conference

DATE: **12-13 June, 2013, Hotel Realm, Canberra**
ENQUIRIES: **ADM Events - Jamie Burrage, Ph: 02 9080 4321;**
Email: Jamie.burrage@informa.com.au Web: www.admevents.com.au
ADM's 3rd Cyber Security Summit will see stakeholders from Australia's Defence and National Security agencies address the current and emerging cyber threats to Australia's security. More details to be released closer to the date.

DSEI

DATE: **10-13 September, 2013, ExCel, London**
ENQUIRIES: **Web: www.dsei.co.uk**
DSEI is the largest fully integrated defence and security show in the world, feautring Air, Naval, Land and Security show content. Based in ExCeL, London every two years, the event provides unrivalled access to key markets across the globe.

SimTecT

DATE: **16 Sep - 19 Sep, 2013, Brisbane Convention and Exhibition Centre, Queensland**
ENQUIRIES: **Web: 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.