



Introduction to the U.S. 3rd Offset Strategy

By Mr. Ben Power

OUR VALUES

SERVICE

COURAGE

RESPECT

INTEGRITY

EXCELLENCE



Tac Talks

© Commonwealth of Australia 2021

This work is copyright. You may download, display, print, and reproduce this material in unaltered form only (retaining this notice and imagery metadata) for your personal, non-commercial use, or use within your organisation. This material cannot be used to imply an endorsement from, or an association with, the Department of Defence. Apart from any use as permitted under the Copyright Act 1968, all other rights are reserved.



OUR VALUES

SERVICE

COURAGE

RESPECT

INTEGRITY

EXCELLENCE



Introduction to the U.S. 3rd Offset Strategy

It would come as no surprise that the objective of any adversary is to deny the core mission of the RAN; to fight and win in the maritime environment as an element of a joint or combined force, assist in maintaining Australia's sovereignty and to contribute to the security of our region.

In the globalised corporate world, the ability of a company to exert its dominance and power over another is directly proportional to that company's competitive advantage. Suffice to say that the greater the advantage, the more likely a company will succeed in achieving its objectives over its competitors. The US Department of Defence coins this as an Offset Strategy; those long-term peacetime measures taken to generate and sustain decisive operational advantage and deterrence.

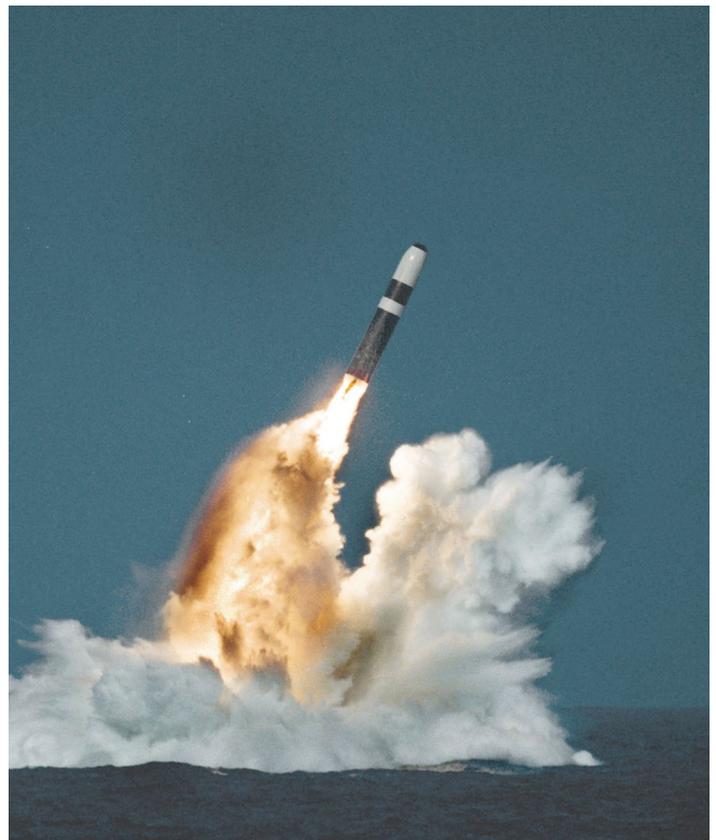
The announcement of the US 3rd Offset strategy welcomes a new era of technological competition aimed not only at countering the emerging advances of China and Russia, but also the asymmetrical and non-state actors who would seek to threaten the US superpower, including major developments in cyber and electronic warfare. There are several technological imperatives of the strategy; deep-learning systems, human-machine collaboration, human-machine combat teaming, assisted human operations and network-enabled, cyber hardened weapons. This essay will briefly discuss a history of Offset strategies, as well as some of the imperatives that the RAN, and wider ADF, will contribute to and benefit from.

History of Offset Strategy

Post World-War II, the US identified early that Soviet influence was of concern to its interests. Particularly troubling was Soviet advantage over Western Europe which led to the 1st Offset strategy; the development and proliferation of tactical nuclear weapons.

A product of this era was the development of the LGM-30 *Minuteman*, a land-based inter-continental ballistic missile which became the first of its kind to incorporate the multiple independently targetable re-entry vehicle (MIRV) technology with each missile carrying up to three nuclear warheads.

As the Cold War continued into the mid-1970s and early 1980s, the Soviets had all but recovered and advantage gained by the US, and so the 2nd Offset sought to revolutionise conventional munitions with precision guidance systems employed in unison with network centric warfare.



The LGM-30 Minuteman.

This continues as a key theme of modern technologies like the GBU-39 *Small Diameter Bomb* and Link-16. With this revolution came the proliferation of microprocessor technologies surging forward the digital age and the coming of the internet as we know it today. But as with the previous generations of strategies, the competitive advantages once realised is no longer and the US think tanks are in the process of developing the 3rd Offset strategy to ensure US military dominance for years to come.

OUR VALUES

SERVICE

COURAGE

RESPECT

INTEGRITY

EXCELLENCE

Deep-learning Systems

Technological networking, research and development firm CISCO anticipate that global IP traffic will pass the zettabyte (ZB). Internet video surveillance traffic alone nearly almost doubled in 2015, peaking at 516 petabytes per month. The sheer volume of data in this single transmission medium alone is enough to inundate contemporary national security initiatives, necessitating a need for more efficient and effective analysis. One of the earliest recognitions of the growing need for automation was in the US National Security Agency's widely publicised communication interception, collection and analysis network, codenamed ECHELON.

But with the continued development of hardware, particularly in processing power and storage capacity, systems are becoming more and more capable of executing advanced, dynamic procedures akin to, and in some cases surpassing that of human intellectual capability. These systems are not only able to perform multiple extremely complex tasks at once, but are able to learn from their environment and make decisions about what actions should be taken for optimal outcomes.



Deep learning systems are already being used in Augmented Reality applications where a computer must recommend decisions to the host by learning from the visual environment. Subaru has fielded its first generation of adaptive electro-optical cruise control titled EyeSight.

The high-performance PC hardware developer, NVIDIA have already produced one of the first commercial off-the-shelf applications of the technology with the DGX-1 system prototype. US Defence Advanced Research Projects Agency (DARPA) are well ahead in development for applications in the electronic warfare domain with programs such as Adaptive Radar Countermeasures (ARC) and Behavioural Learning for Adaptive Electronic Warfare (BLADE). Australia has recently bought into the aged but proven Aegis weapons system installed on the Hobart Class DDG which commences first of class trials in mid-2016.

The reality is that these systems process enormous volumes of information, far beyond the capacity of a human, and either makes informed recommendations to the user or acts autonomously in self-defence situations where timely action is a must. While legacy systems like Aegis will look to optimise decision-making and processing power based on intensive operator setup, future systems will optimise parameters by learning directly from the environment using real-time data. How a technology collaborates with the human counterpart is another key technological imperative of the US 3rd Offset strategy.

Human-machine collaboration and combat teaming

As US Deputy Defence Secretary Robert Work identified in one of many media engagements with NATO partners, "... nothing can match the lethality and destruction of high-end conventional

OUR VALUES

SERVICE

COURAGE

RESPECT

INTEGRITY

EXCELLENCE



Tac Talks

warfare, and we must do everything in our power to prevent it from happening". Specifically, Work referenced two problems in defeating future adversaries; winning the emergent guided munitions salvo competition and dominating the highly lethal battlefield with next generation follow-on forces attack and manoeuvre. Some of the earliest and most successful advances in this arena are evident in modern 4th and 5th generation fighter aircraft.

The inclusion of Hands on Throttle and Stick (HOTAS) in the F/A-18A *Hornet* allows the pilot to continue to fly the aircraft while simultaneously operating weapon and sensor systems. Coupling the Joint Helmet Mounted Cueing System (JHMCS), the pilot now has information displayed directly to the helmet visor, enabling the pilot to fly, fight and maintain visual awareness outside the cockpit. The F/A-35A *Lightning II* takes these technologies further by fully integrating the pilot into the operation of the aircraft weapons and sensors, allowing the operator a tactical advantage in a shooting match with a near-peer adversary.



BrahMos is a supersonic anti-ship missile developed and fielded by India. Seen here being fired from INS Rajput, the proliferation of supersonic weapons brings with it a reduced reaction time to an already complex ASMD problem, supporting the case for better Human-Machine collaboration.

In a comprehensive DARPA study, humans and machines competed against one another in a game of chess. As the study progressed, machine became far better than the human, but interestingly a human-machine hybrid was able to defeat the machine in almost 70 percent of cases. The same is expected to hold true in combat, and the US DoD is making the shift to integrated human-machine combat teaming. Unmanned combat vehicles, for example, are limited in agility only by the physical strength of the materials with which they are made from whereas the average human is limited to forces not greater than 9G (that is, 9 times the normal gravitational force). Unmanned underwater vehicles are able to sustain prolonged surveillance

OUR VALUES

SERVICE

COURAGE

RESPECT

INTEGRITY

EXCELLENCE



Tac Talks

operations under water without the critical life supporting systems typical of submarines like oxygen, food, water and heat. This integration is already being realised on Australian platforms like the P-8A *Poseidon* which is designed to be operated in tandem with the MQ-4C *Triton*.

Traditional data-link networks will not be unable to handle the volume of information analysed by these platforms, posing a communications compatibility risk with the contemporary RAN systems. While the need for bespoke tactical data-link systems continues to challenge naval warfighters, collaboration and combat teaming is identified as a key initiative in enabling allied forces to defeat and survive the guided munitions salvo competition, and position well against subsequent tiers of an Anti-Access and Area Denial (A2/AD) system.

Network-enabled, Cyber-hardened Weapons and Systems

Cyber and electronic warfare are rapidly becoming a common theme in adversary tactics to degrade and exploit the contemporary technological advantage. Not only are these types of systems comparatively cheap, they are effective. As the US progressed into a precision guided lethality strategy of the 2nd Offset strategy, weapons and sensor systems become heavily dependent on GPS for position, navigation and time, from data-links to cruise missiles. However, military operations are increasingly denied GPS reception by way of cheap and readily accessible jamming technology ranging from small-scale commercial devices to large military applications within an A2/AD network.

Microprocessors and electronics technology facilitated small aperture, portable radar systems for use in aircraft and missile systems, however just as quickly as these systems were proliferated, so too was the equipment to detect and localise, and even deny them.

In 2013, China completely inhibited the shortwave frequencies of all BBC broadcasting stations in the region in a deliberate and coordinated attack against its media services. Months later, the Chinese claimed to have developed the capability to deny the Link-16 anti-jam waveform.



E/A-18G Growler coupled with the AGM-88E Advanced Anti-Radiation Guided Missile and Next Generation Jammer represents a part of the solution to the growing complexity of modern Anti-Access and Area Denial (A2/AD) networks.

As the technological edge continues to sway between emitter and jammer, Australia remains well positioned to defeat and deny the future threat via the E/A-18G *Growler* armed with the AGM-88E next generation Advanced Anti-Radiation Missile. While lacking any kind of Electronic Attack suite for some years now, the RAN has taken a large leap towards an electronic warfare advantage

OUR VALUES

SERVICE

COURAGE

RESPECT

INTEGRITY

EXCELLENCE



Tac Talks

with acquisition of the ES-3701 Electronic Support suite on its surface combatants and with it the latest phase measurements technology for high precision direction finding and a very high probability of interception. But with a finite inventory of precision guided munitions, the US and her allies will continue their reliance and dependence on the ability of these weapons to overcome emergent denial technologies. And that includes the very real threat of cyber warfare. Preventing a ship from sailing through diversion of some urgently needed synthetic engine oils is just as effective as any other conventional kinetic effect, albeit achieved at a fraction of the cost, near-zero risk and with the benefit of anonymity.

Cyber-attacks are becoming increasingly prevalent in mainland US and Australia and are not limited to just military targets. Commercial enterprises are also being exploited for a much greater strategic affect; in 2012, Qatari liquefied natural gas producer RasGas was targeted with a malicious virus that memory-wiped its computer network, bringing production to a halt, raising LNG prices and temporarily destroying revenue for the US backed company. Future developments will focus on building immunity and exploiting vulnerabilities within the cyber warfare domain to secure freedom of action of friendly networks, systems and infrastructure.

Conclusion

The announcement of a US 3rd Offset strategy could not have come at a more opportune moment. Tensions are mounting in the South China Sea with a fortification effort and the construction of defensive infrastructure by Chinese in a dispute for ownership rights. The support for the US is continually challenged in the region as the lack of direct action to secure international sovereignty leads to a stand-off trending with similarities to the Cold-War.

Australia has sound interest in promoting regional stability, and has a significant part to play in a joint forces construct of any future US led task group with such a purpose. Our ability to remain in line with the US 3rd Offset strategy will ensure Australia continues to maintain its dominance in the region for decades to come while also committing to a valuable and meaningful contribution to global security.

OUR VALUES

SERVICE

COURAGE

RESPECT

INTEGRITY

EXCELLENCE