AOC Australia
ABN: 86 623 646 012

AOC Australia Essay Competition:

Exploring the Future of Warfare

AOC Australia
ABN: 86 623 646 012

Letter of support from Head Joint Capabilities

Dear Colleagues and Participants,

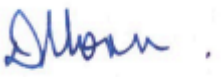
I would like to extend my sincere thanks to all who have taken the time and effort to contribute to this year's AOC Australia essay competition. Your participation reflects a deep commitment to advancing our understanding and capability in the fields of Electronic Warfare, Cyber Warfare, and Information Operations. The insights, solutions, and innovative thinking presented in these essays are invaluable as we continue to navigate the complexities of modern warfare.

These domains are at the heart of our joint capabilities, and the ideas explored in this competition are crucial to maintaining our operational advantage. The challenges we face are evolving rapidly, and it is through intellectual engagement and collaborative innovation that we will stay ahead of potential adversaries.

To those reading the essays, I urge you to consider the ideas and perspectives shared. Engage with the content, contribute to the discussion, and apply these insights to your own work. Together, we can drive progress and continue to enhance our collective defence posture.

Once again, my thanks and congratulations to all the participants. Your work is shaping the future of our defence forces.

Yours sincerely,



Rear Admiral David Mann CSC RAN
Head of Joint Capabilities
Joint Capabilities Group, Department of Defence

AOC Australia
ABN: 86 623 646 012

The AOC Australia's annual essay competition is a crucial platform for fostering thought leadership and innovation in the fields of Electronic Warfare (EW), Cyber Warfare, and Information Operations. It provides professionals and enthusiasts alike with the opportunity to showcase their knowledge, share insights, and propose groundbreaking ideas that could shape the future of these rapidly evolving domains. As the landscape of warfare continues to shift toward the digital and electromagnetic spectrums, it is essential that we cultivate new perspectives and encourage dialogue on emerging threats and strategies.

This competition serves as a forum where fresh voices can challenge conventional thinking, and industry experts can present forward-thinking solutions. By participating, individuals contribute to the growth and development of these critical fields, helping to secure and advance national defence capabilities. Moreover, it promotes a culture of collaboration and continuous learning, essential for staying ahead in an ever-changing technological environment.

We extend our heartfelt thanks to everyone who submitted essays to this year's AOC Australia competition. Your contributions not only demonstrate your passion and expertise in Electronic Warfare, Cyber Warfare, and Information Operations but also play a vital role in advancing these crucial fields. Your innovative ideas and insights will help shape the future of defence technology and strategy.

For those reading the submitted essays, we encourage you to engage with the material, share your thoughts, and reflect on the challenges and solutions presented. These essays are more than just words on paper—they represent the cutting-edge thinking that will drive the next generation of defence advancements. We invite you to continue the conversation, challenge assumptions, and contribute to the ongoing evolution of these fields.

With thanks for all who contribute,

Lauren Hassall
CEO | AOC Australia

Essay Topic: The operational concepts for EW capabilities are evolving rapidly, with many lessons drawn from the ongoing conflict in Ukraine. Given Australia's relatively limited history in operational electronic warfare, we face the challenge of evaluating the relevance of these external concepts to our own use case. How should Australia adapt these concepts? How do we optimize our existing capabilities and identify new ones to remain competitive in the EW domain?

AOC Australia
ABN: 86 623 646 012

On the Russo-Ukrainian Electromagnetic Struggle for Superiority: Lessons for Australia

Rhys Kissell | rhys@canberradynamics.com

Introduction

"All warfare is based on deception," said the inimitable master of strategy, Sun Tzu. Electronic warfare (EW) first arose from the need to realise such deception. Among the other subsets of information warfare, EW enables many of the tenets of the Art of War to be realised in very practical ways – to appear weak when one is strong, or strong when one is weak, or even to subdue the enemy without fighting.

It is no surprise, then, that EW has become vital to modern militaries, and that the lengths to which we go in engineering and constructing machinery for it are nothing short of marvellous. EW systems are built with astonishing accuracy, precision, rigor, minimal error tolerances, and are built to perform operationally at the highest standards – and of course, they attract an appropriate price tag – after all, the specialists who command any mastery over the electromagnetic spectrum are a rarity, and the discipline itself is considered something of a dark art by the engineers, technicians and operators who work in the field.

It stands to reason then, that the importance of these tools really does mandate that we must spend such effort perfecting them thus. Or does it? In matters of war, Clausewitz would say: "The enemy of a good plan is the dream of a perfect plan". This essay will argue that Australia must take three lessons from Ukraine: taking steps to ensure electromagnetic superiority, preferencing 'good enough' over 'perfect', and adapting Russian electronic warfare tactics.

The Situation in Ukraine

For all our striving to perfect our tools of the trade in EW, the discipline itself had – until the Russian invasion of Ukraine in 2022 – not seen widespread use between peer or even near-peer forces on land since the 1973 Yom Kippur War. It was really anyone's guess as to what the most effective electronic warfare approaches might be – and to further complexify this, electromagnetic effects in Ukraine are turning out to be as much a deciding factor as kinetic ones among confrontations at both the strategic and tactical levels.

Valerii Zaluzhnyi, former commander-in-chief of the Ukrainian Armed Forces, explained with his November 2023 essay, *Modern Positional Warfare and How to Win In It*, that manoeuvre warfare is largely dead[i]. The essay further explains that a deadlock in positional warfare is assured for the foreseeable future thanks to "notional parity" in technological capabilities between Ukrainian and Russian forces.

Zaluzhnyi names a handful of significant factors driving this deadlock: an inability for either side to gain air superiority; an inability for either side to gain electronic warfare superiority; the management of military reserves; and breaching of deep landmine barriers. Viewing these

challenges from afar has shown the world's militaries just how ill-prepared they are for contemporary warfare, and doubly so for modern electronic warfare.

The use of the electromagnetic spectrum will forever be necessary in war moving forward, but in Ukraine, its use has proven to be as treacherous as it is vital. The contested nature of the electromagnetic environment means that employing it successfully requires accepting a devil's bargain: a sender's message can be encrypted and transmitted freely, but their location cannot be hidden from forward observers who use direction finding techniques. Observers immediately feed these transmitter positions to artillery assets lying in wait, who will open fire within minutes of a transmitter going loud.

Plainly stated, the electromagnetic situation in Ukraine has seen the spectre of the Great War rear its head – the frontlines move at the speed of tens of metres per day – if at all – and electronic warfare parity has become directly responsible for aiding in the return of the trenches. Menacingly, this may well be a foreshadowing of what more widespread conflict in the future may look like. Zaluzhnyi sums it up well in his interview with the Economist: "The simple fact is that we see everything the enemy is doing, and they see everything we are doing. In order for us to break this deadlock we need something new"[ii].

Russian Electronic Superiority

Russia's history of electronic warfare in the radiofrequency spectrum extends back further than any other country. In 1904, during the Siege of Port Arthur, Russian forces jammed Imperial Japanese Navy communications, preventing artillery corrections and causing numerous misses. This event is ingrained in Russia military thought and even led to an annual commemorative day in Russia: April 15th is Radio-Electronic Warfare Day. Though Russia lost that war, it instilled the usefulness of electronic warfare in Russian military thought far before any other nation.

In Russian military thought, one of the primary uses of EW (and information warfare more broadly) in various forms to diminish the organisational capabilities of their enemy's systems, a strategy referred to in Russia as *disorganisation*[iii]. This is likely a descendant strategy of *deep operation* or *deep battle*, an old Soviet approach to combined arms, and the first military theory in the world to conceive of a level between tactical and strategic - operational.

This strategy of *disorganisation* focuses on the disruption and elimination of command and control (C2) systems and elements – especially those reliant on space elements – with state-of-the-art electronic warfare systems. It has apparently instilled great confidence in Russian military circles, with the Russian head of Radio-Electronic Warfare (REB) forces even stating, "electronic warfare will decide the fate of all military operations".

A specific tactic utilised by Russia to realise *disorganisation* is called *fragmentation*, wherein command decision-makers are tracked and are specifically targeted by electronic warfare effects. For example, if an enemy commander is known to have entered an area of operations

(AO), then electronic attack assets may well be dedicated to interfering with zonal C2 instruments while the commander remains in the AO. If the commander leaves the AO, directional electronic attack can be utilised to continue to interfere with C2 functions. Russia used this *fragmentation* implementation of *disorganisation* in Syria to great effect, according to the Russian military publication, *Military Thought*[iv].

While Russia frequently overstates the EW capabilities of its REB forces, Thomas explains in his September 2020 analysis that U.S. and NATO commanders have both noted that Russian EW capabilities are indeed superior to Western equivalents[v]. While Zaluzhnyi has described a situation where Ukraine and Russia are on par with one another in EW matters, it would be more accurate to describe Ukraine as being highly effective at developing ways to circumvent Russia's superior and continually evolving electronic attack systems.

More traditionally – at least by Western EW standards – Russian efforts in Ukraine have also been spent on jamming electro-optic (EO), global navigation satellite systems (GNSS), and position, navigation and timing (PNT) systems to great effect. Earlier this year, the Washington Post revealed that some of the United States' most advanced weapon systems have fallen victim to the dream of a perfect plan and have in some instances been completely removed from use by the Ukrainian Armed Forces due to Russian electronic warfare making the systems almost useless[vi].

These systems include the 155mm Excalibur projectile, touted as "a revolutionary, extended-range, precision munition", which saw its accuracy rates fall to less than 10% over a period of a few months, JDAM-ERs (which, even after patching by the manufacturer, have an accuracy rate lower than their unguided GBU-39 counterparts), and the M30/M31 rockets utilised by the M142 HIMARS (which Australia has recently acquired).

Russia can reliably achieve these effects – and likely more advanced ones that they have not had to utilise against Ukraine – because of the near ubiquitous proliferation of REB forces and equipment among the various branches of the Russian Armed Forces. They have brigades in all four theatre commands, they have companies in the armoured brigades, and they have divisions in the airborne forces. The Russian Navy also has REB elements in all four fleets, and the Aerospace Forces contain REB battalions for both the Air and Air Defence armies[vii].

Ukrainian Adaptation and Achieving Parity

Ukraine, not expecting an invasion, started out on extremely poor footing in the realm of electronic warfare. Beginning its defence with old Soviet electronic equipment, it has since rapidly innovated (a term victim to semantic bleaching in the West, but an accurate descriptor in Ukraine) and engaged over 50 manufacturers with over 100 electronic warfare projects through BRAVE1[viii], a multi-departmental Ukrainian government initiative to accelerate, acquire and deploy domestic and foreign military technology solutions to the frontlines.

It is often said that necessity is the mother of invention, but it is probably fairer to say that it is the mother of innovation. Though some former Soviet experts and many younger formally trained engineers participate, the drivers of Ukraine's electronic warfare industry are now largely craftsmen of various backgrounds from before the war – the types of people you'd expect to find in a *makerspace* or *hackerspace* (communal workshops available at many libraries and universities). This unique situation has led to immense competition in the Ukrainian domestic defence industry, and with the government funding and encouraging it, the results is that innovative new solutions are being created every week.

The prevailing design philosophy shuns the high-end sophistication that the West has historically preferred, and instead opts for a continually integrated military appreciation process as part of a rapid prototyping and iteration process for minimum viable capabilities. Breaking Defense describes some of these innovations in a June 2024 article[ix], some of which include homemade autonomous correlative interferometer (advanced direction finders) systems, or refitted consumer walkie talkies to provide mesh ad-hoc network (MANET) functionality and frequency hopping spread spectrum (FHSS) as an anti-jamming measure. There are also many drone startups in Kyiv who now have a focus on developing semi- or fully autonomous drones with watertight emanation security (EMSEC) to prevent their detection (and therefore pre-emptive jamming) before they can attack, and a handful of companies focusing on camouflage that focuses on fooling computer vision, rather than human eyes.

Most products are developed with commercial-off-the-shelf components, with custom-designed 3D printed components, and often with open-source software. They are not typically using $150,000/yr software licences to optimise microstrip antennas to near theoretically perfect S-Parameters, or developing a multi-model digital twin to determine the best way to make use of tuned mass dampers, or continuous uplinks to bespoke infrastructure in low Earth orbit.

Instead, Ukraine's approach represents the very best of the concept of 'good enough'. Although they remain reliant on a continuous supply of materials and munitions, they have come into their own in facing the Russians in the electromagnetic spectrum. Part of what enabled this is Ukraine's recent revamp of its own acquisition processes, through BRAVE1 and the Ministry of Defence's Mil-Tech Accelerator[x]. With these reforms, they have reduced the documentation required from over 100 forms and a timeline of more than 24 months to just 5 forms and 1 month, delivering effective materiel to the front as rapidly as it can be produced.

Lessons for Australia

Looking back home, there are lessons and ideas for Australia to consider, and to adapt.

First, Australia would do well to heed Zaluzhnyi's observations and to ensure that our adversaries cannot achieve electronic warfare parity. Like Ukraine, Australia is vulnerable to a strategy of attrition warfare. If Australia and its allies do not maintain electromagnetic superiority, it is likely that the Australian Army will find itself on a positional warfare footing, enabling the enemy to choose when, where, and how to fight. As the Army continues to explore what littoral manoeuvre

warfare might look like, it must remain cognisant of its vulnerability to being outmatched electronically.

Although warfare in all forms bears a terrible cost to society and to human life, positional warfare is its own special level of horrific – in the trenches of the First World War, two thirds of all Australians who left our shores would become casualties[xi]. Overmatching an adversary in the realm of electronic warfare must remain at the heart of Australian strategy moving forward, as it is one of the greatest assurances against this.

Second, Australia's tactics, techniques and procedures very often are adapted from the United States, thanks to their wider experience in warfare. American EW– and therefore Australian EW– differs substantially to its Russian equivalent, in that its focus is substantially on jamming missiles and aircraft, preventing munitions from reaching their targets.

While this aspect cannot be neglected, the Russian strategy of *disorganisation* should be considered for adaptation into Australian EW. The fundamental goal of manoeuvre warfare, according to Lind[xii], is to shatter the physical or mental cohesion of the enemy. By adopting *disorganisation* and continuously attacking command and control (C2) structures and organs, a situation can be brought about where the enemies' troops and equipment cannot effectively be allocated to tasks – in this way, despite Russia's historical preference for attrition warfare, *disorganisation* is very well aligned with Australian manoeuvre warfare, because it destroys the coherence of an adversary.

An Australian Defence Force (ADF) reimagining of *disorganisation* against a peer adversary would likely involve focusing electronic and cyberattacks against situational awareness systems and tactical data link networks, as well as enemy command elements. Through the electronic destruction of the C2 apparatus, an adversary can be re-enveloped in the fog of war that these systems seek to dissipate. This *disorganisation* approach allows a numerically or technologically inferior force to severely impact the speed and accuracy of the decision-making process for their adversary, which can act as a huge force multiplier for a military focused on manoeuvre warfare.

According to Milan, "Littoral Warfare requires the closest of cooperation amongst the services"[xiii], and thus is extremely reliant on robust, decentralised C2 structures. Given the increasing cooperation between Russia and China, the ADF should expect *disorganisation* and *fragmentation* to be used against it – and possibly to great effect. The ADF should therefore practice operating in scenarios where all electronic and/or ICT-based C2 systems are completely unavailable.

Finally, Ukraine's experiences in the defence industry arena should impress the Clausewitzian lesson upon Australia - while Defence has made some progress, much work remains. The consolidation among industry primes, the resultant lack of competition, and dogmatic adherence to ISO 24641 processes without nuance are all hinderances in providing effective tools to the Warfighter in an acceptable timeframe. Even with the government initiatives to bring about 'rapid innovation' with the introduction of the Advanced Strategic Capabilities Accelerator – the urgency is just not there.

Australia must get proactive. It can improve its own preparedness by looking to where Ukraine has succeeded in developing its own defence industry. This could be as simple as providing less conditional stimulus to the domestic defence small-medium enterprise (SME) community to stimulate the development of domestically owned capability, or discarding long-winded bureaucratic processes that do not deliver fit-for-purpose or cost-effective solutions, or even by developing new provisions to make testing defence equipment more affordable. By adopting similar improvements, and fostering a competitive environment, Australia can enjoy meaningful innovation, ensure that its plans remain realistic and adaptable, and that its dreams of a perfect plan do not begin to contort into a living nightmare.

References

i. https://infographics.economist.com/2023/ExternalContent/ZALUZHNYI_FULL_VERSION.pdf
ii. https://www.economist.com/europe/2023/11/01/ukraines-commander-in-chief-on-the-breakthrough-he-needs-to-beat-russia
iii. https://www.armyupress.army.mil/Portals/7/Hot-Spots/docs/Russia/Mitre-Thomas.pdf pp. 54
iv. *Military Thought*, No. 5, 2016 pp. 22-27.
v. https://apps.dtic.mil/sti/trecms/pdf/AD1137511.pdf pp. 7
vi. https://www.washingtonpost.com/world/2024/05/24/russia-jamming-us-weapons-ukraine/
vii. https://apps.dtic.mil/sti/trecms/pdf/AD1137511.pdf pp. 14
viii. https://breakingdefense.com/2024/06/inside-ukraine-startups-try-to-edge-russia-in-the-electronic-warfare-race/
ix. https://breakingdefense.com/2024/06/inside-ukraine-startups-try-to-edge-russia-in-the-electronic-warfare-race/
x. https://mil-tech.gov.ua/en
xi. https://www.naa.gov.au/students-and-teachers/student-research-portal/learning-resource-themes/war/first-world-war
xii. *Maneuver Warfare Handbook,* 1983
xiii. https://digital-commons.usnwc.edu/nwc-review/vol68/iss2/4/

What's the difference? Lessons from EW in Ukraine

David Enchelmaier | david.enchelmaier@aus.l3harris.com

At first glance, you might think the differences between Ukraine and Australia leave few lessons worth adapting to an Australian context. They are in a land war; conflict in the Indo-Pacific will likely be maritime and air focused. Distances are vastly different: the front line in Ukraine is around 1,000 km; across Australia's northern coastline there's some 2,000 km just from Exmouth to Darwin, and it's 2,500 km as the crow flies from Darwin to the Philippine Sea. They are fighting to preserve both independence and territory; we are unlikely to face invasion and the more likely fight for us rather will be to maintain Sea Lines of Communication (SLOCs) or help our friends and neighbours defend their territory.

Despite these significant differences, Ukrainian experience is highly relevant and there is a lot to be learned. Going back to first principles, the purpose of EW remains unchanged: to protect the EM spectrum and use it to our advantage while denying it to our adversaries. And in the larger context, it is even simpler: EW, like every other tool, exists to support the commander in achieving their mission objectives. In the rest of this essay, we will look at operational EW examples from the war in Ukraine, parallels in a potential Indo-Pacific conflict, and some of the cultural and organisational actions needed to help commanders fulfil their missions and keep the ADF on a competitive footing.

It wasn't long after Russia's 2022 invasion before media reports started appearing on EW. Russia's EW units were ill-equipped and caught off-guard some said. Other reports spoke of simple yet innovative tactics like a mobile phone "prank" call to geolocate a target for artillery strikes. Several months later and Russia was thought to have the upper hand, at least as far as EW was concerned.

Fast forward to August 2024 and it is clear neither side has a decisive, dominant advantage in the electromagnetic spectrum: like a pair of chess players it is a constant battle of move and counter-move, both sides having wins and losses, both adapting rapidly to the changing landscape. Most of the recent focus has been on drone warfare, broader communications EW, and navigation warfare. Reporting on drone warfare has highlighted the impact of successful jamming when operators lose control of their aircraft[1], and the potentially deadly outcome if jamming is turned off or ineffective[2]. In the navigation warfare space, Russia's success with GNSS degradation has been profound: Excalibur precision guided artillery falling from 70% accuracy to only 6% after 6 weeks[3]. The Guided Multiple Launch Rocket System (GMLRS) is

[1] https://breakingdefense.com/2024/06/inside-ukraine-startups-try-to-edge-russia-in-the-electronic-warfare-race, accessed 17 August 2024
[2] https://www.nationaldefensemagazine.org/articles/2024/3/8/daily-fight-for-ukraine-spectrum-superiority-puts-electronic-warfare-front-center, accessed 17 August 2024
[3] Dr. Dan Patt, Congressional HASC Testimony, 13 March 2024, https://www.hudson.org/information-technology/too-critical-fail-getting-software-right-age-rapid-innovation-dan-patt, accessed 17 August 2024

similarly affected[4], and a ground-launched version of an air-to-ground munition, thought to be the Ground-Launched Small Diameter Bomb (GLSDB),[5] is also failing to hit targets, causing Ukrainian soldiers to lose trust in it as a weapon system according to Dr Bill LaPlante, US Under Secretary of Defense for Acquisition and Sustainment (USD(A&S))[6].

Some of the most significant observations are summed up in Dr Dan Patt's recent testimony to the US House Armed Services Committee (emphasis added):

> *Once a conflict begins, adaptability and scaling drive outcomes. We must seize the current moment to prepare. For examples about how conflict drives adaptation, consider that the* ***lifecycle of a radio in Ukraine is only about 3 months*** *before it needs to be reprogrammed or swapped out as the Russians optimize their electronic warfare against it. The peak efficiency of a new weapon system is only about* ***2 weeks before countermeasures emerge****. As another example of superior weapons systems handicapped by lack of software adaptability, consider that Excalibur precision artillery rounds initially had a 70% efficiency rate hitting targets when first used in Ukraine. However****, after 6 weeks, efficiency declined*** *to only 6% as the Russians adapted their electronic warfare systems to counter it.* ***This shows how quickly adversaries can adapt*** *to new technologies.*[7]

How do these experiences and observations from Ukraine apply to Australia and potential Indo-Pacific conflicts?

The operational security risks of smartphones and other networked devices are well known. Although not strictly EW, one of the most public examples was in 2007 when Iraqi insurgents destroyed four AH-64 Apache helicopters in a mortar attack, thanks to targeting coordinates gleaned from photos uploaded to social media[8]. A year earlier, Iranian SIGINT specialists had identified Israeli army assembly points based on signals from personal phones[9]. Clearly, awareness of your personal footprint is applicable in any theatre, and not just the online footprint of Facebook and Instagram posts, but even the EM footprint of when and where your phone connects to the internet.

---

[4] https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-ukraines-offensive-operations-2022-23, accessed 17 August 2024
[5] https://www.c4isrnet.com/electronic-warfare/2024/05/06/electronic-warfare-in-ukraine-has-lessons-for-us-weapons-navigation/, accessed 17 August 2024
[6] https://www.defenseone.com/threats/2024/04/another-us-precision-guided-weapon-falls-prey-russian-electronic-warfare-us-says/396141/, accessed 17 August 2024
[7] Dr. Dan Patt, Congressional HASC Testimony, 13 March 2024, https://www.hudson.org/information-technology/too-critical-fail-getting-software-right-age-rapid-innovation-dan-patt, accessed 17 August 2024
[8] https://www.military.com/defensetech/2012/03/15/insurgents-used-cell-phone-geotags-to-destroy-ah-64s-in-iraq, accessed 17 August 2024
[9] Ibid.

When it comes to drone warfare, applicability is mixed. Australia's maritime approaches and sparse north-west region form a natural barrier against all but the highest capability military UAVs. But it is conceivable that Australian forces could be on the ground in support of another country and face large scale deployment of short range consumer drones similar to Ukraine's experience. Against consumer drones, what we see in Ukraine is that preparation and adaptability is essential: The time between deploying a countermeasure and an adversary reprogramming to circumvent will be at most 3 months, and could be as little as two weeks. While most Western EW discussion around drones focuses on development of Counter-Unmanned Aerial Systems (C-UAS) for protection of ground assets such as airports and other Critical National Infrastructure (CNI), the corollary is true for protecting our access to the spectrum: we may have at best a few months before effective countermeasures are brought to bear, and our reprogramming cycles and the logistics to push out updates need to be much faster if drones are to be a useful asset.

In the realm of high-end military UAVs, across the board Australia is reliant on a small number of very capable aircraft, and we are likely to face a severe overmatch situation when considering the quantity of long range UAVs in operational use with other countries in the region. Here, the applicable lesson is that we should expect to lose a portion of our UAVs, and face regular periods where they are unavailable because of the effectiveness of adversary countermeasures and the time needed to reprogram. For Australia to neutralise opposing UAVs, the sort of short range barrage jammers used in Ukraine aren't up to the task. We will need persistent systems with a combination of techniques of varying sophistication that will be effective against targets at extended ranges with hardened data links. Terms like Artificial Intelligence and Machine Learning (AI/ML) are overused; it would be better to say those systems need well-designed algorithms to recognize target emissions from non-target adversary and grey-force/blue-force emissions and respond accordingly, and carefully constructed rules of engagement to minimize the chance of spectral fratricide or civilian interference. In all likelihood, any persistent stand-in countermeasure systems will have to operate for extended periods cut off from communications with rear echelons and the human decision-makers based there.

In navigation warfare, the last of our examples, there are again both offensive and defensive lessons. The open source reporting quoted earlier does not detail how far outside the advertised Circular Error Probable (CEP) rounds are hitting, but it seems prudent to assume that with only 6% efficiency, most are a long way off target. The lesson is clear: Precision-guided weapons are vulnerable to GNSS denial, perhaps more than we want to admit. On the offensive side, if we are to prevent the same loss of confidence in weapons systems from our forces that Ukraine experienced, this needs urgent thought at multiple levels. Those of us who are engineers and technologists need to identify fixes, preferably of a sort that is low cost and quick to deploy, and ideally capable of long term prevention, not just a reactive patch. For military planners, it begs the question: do our expected consumption rates and targeting priorities reflect the reality seen in Ukraine the last few years, and if not, what needs to change? At the national level, do our political leaders appreciate the impact this has on the defence budget?

Do they understand that against heavy countermeasures our exquisite precision weapons may perform only marginally better than dumb weapons and what that may mean for civilian casualties? Do they appreciate the sheer quantity of weapons required to fight through those conditions?

Defensively, the picture improves somewhat. Just as the proliferation of consumer drones and the subsequent uses and abuses led to C-UAS EW systems for protecting CNI, there is an opportunity to add a distributed GNSS denial electronic countermeasures layer to existing Integrated Air and Missile Defence systems – reducing incoming salvos at a far lower equivalent cost per shot than surface to air missiles, and using more mature technology than the high energy laser systems currently in development. "The speed of relevance" is a term that comes up with increasing frequency and emphasis, and is another lesson reiterated through all aspects of the war in Ukraine. It sums up the view that a lower cost, less capable solution that covers part of the gap and is available today is better than a cutting edge solution that will defeat everything but won't be operationally ready for a decade and needs a budget to match.

In summary, the key examples and lessons from Ukraine from an EW perspective should come as no surprise: emissions control needs to be part of the holistic OPSEC posture; SIGINT professionals can and will use any stray emissions to their advantage. Unmanned systems and precision weapons are vulnerable to denial and spoofing of their command and control links and external navigation aids, with knock-on effects for reliability, availability, and effectiveness. This cuts both ways, and the impact depends on the type of system, where and how you want to use it, and what you're facing.

So how do we adapt? How do we, both here in Australia and the west more generally, optimize our existing capabilities and identify new ones to remain competitive in the EW domain? What cultural and organisational actions do we need?

Firstly, the whole EW community needs to draw closer together. The AOC is a great asset in this, but to make it effective all parties need to make an effort: academia, industry, government acquisition and S&T, and each of the services. What this looks like is different for each party: Government and the services must continue to build a tent of trusted partners with whom they can share their current and emerging challenges. Industry and academia must continue to show trustworthiness: staying focused on the task at hand, openness and honesty about capability and limitations, and transparency on progress.

Secondly, and building on the trust of a close-knit community, is a culture of understanding and communicating risk. The 2023 Defence Strategic Review[10] acknowledged the loss of the 10-year strategic warning period that has been the foundation of Australia's acquisition and sustainment policies; we are now more than half way through the three year period 2023-2025, and the following five year period to 2030 will soon be upon us. Which means there is an

[10] https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review, accessed 17 August 2024

elevated chance that at some point in the coming years, ADF Responsible Engineering Officers will need to decide on the risk of proceeding into conflict with EW systems or upgrades that offer attractive new capability but may be only partially proven, versus leaving them behind. Industry owes it to our services to provide whatever inputs it can as clearly and promptly as possible, to inform that decision. The services can foster this with an attitude of teamwork and partnership – this will be far more effective at drawing out risks and limitations than a combative checklist-driven approach.

These first two stages are underway, at least in pockets of the Australian EW community, which is good. Because the third stage, which is only possible in a trusted community where risk is well understood and clearly shared, is vital for surviving the electromagnetic battle: How we manage upgrades, particularly software upgrades and reprogramming. In his HASC testimony, Dr Patt quoted timeframes of two weeks to the emergence of countermeasures, and in the case of Excalibur six weeks until Russia's countermeasures had virtually nullified its effectiveness as a precision weapon. In that context, he also observed:

> *This shows how quickly adversaries can adapt to new technologies. This lack of adaptability is not an inherent property of software but rather a consequence of how we choose to manage it. After all, Ukrainian units with organic programming capability to rapidly adapt their UAV software have about 50% efficiency, while those reliant on companies and longer supply chains to make changes struggle to hit 20% efficiency. Keeping software in a pliant, fluid state is the only way to maintain tactical innovation.*[11]

It would be hard to find something more critical to remaining competitive in the EW domain than the ability to deliver rapid upgrades, especially software. And not just to reprogram emitter libraries but to address underlying software bugs and vulnerabilities, to add new countermeasure techniques, or to repurpose available hardware to a different application. At the height of a conflict, these updates will need to be turned around in days or weeks, and the best way for this to happen is when the community is working together in a trusted partnership.

This is not cheap, and again the actions to optimise existing capability and remain competitive require trust and coordination across the community. Government needs access to interfaces and source code. Industry needs to maintain up to date development environments, in most cases accredited for classified work, with automated regression testing tools and other DevOps practices that can help reduce the risk of introducing new software updates. For many systems, this will also include a copy or copies of the system hardware to verify updates before pushing to the customer. But even more importantly, industry needs to maintain the people – the experienced engineering teams who can take the problem from the user, adapt and update the product quickly, and give our defence personnel the best chance in the challenges to come.

[11] Dr. Dan Patt, Congressional HASC Testimony, 13 March 2024, https://www.hudson.org/information-technology/too-critical-fail-getting-software-right-age-rapid-innovation-dan-patt, accessed 17 August 2024

No-one has ever claimed that EW won the war. But without it, we can easily lose the war. Trust, understanding risk, and rapid turnaround that solves today's problem first. None of these are showy or exciting, but they make a difference, and that might just be what it takes.

David Enchelmaier (SMIEEE, FIEAust, CPEng, NER, RPEQ)
Future Solutions Architect
L3Harris Space and Airborne Systems Australia Pty Ltd

Exploring the Future of Electronic Warfare

Hope Sneddon | hope.sneddon@outlook.com

The essence of the Electronic Warfare essay topic proposed by the AOC can be captured by rephrasing the topic into the following two key questions: How should Australia adapt modern EW concepts highlighted by recent conflicts? And how do we optimize our existing capabilities and identify new ones to remain competitive in the EW domain?

Electronic Warfare has seen unparalleled levels of innovation and development when compared to other warfare capability fields. It is reasonable to expect that this will continue in the form of more powerful signal modulation techniques and effective employable ranges to anticipate battlefield participants and obstacles. So how then, can Australia specifically keep pace and competitively contribute to the advancement of Electronic Warfare technology where we struggle to match the testing facilities and level of investment in EW as compared to countries like the United States and China? The answer could simply be, we focus on the integration and application of Electronic Warfare rather than the technology bound for perpetual optimisation from the traditional development leaders. Integration and fused applications of Electronic Warfare technology will be crucial in maintaining leading edge EW capabilities on air, land and sea assets alike as we enter the age of data fusion and autonomy led warfare.

In order to discuss EW data fusion concepts that will sustain existing and emerging Electronic Warfare capabilities for Australia, it is imperative to preface this discussion with the identification of key themes and concepts that bound the problem space. From this, the essay will discuss the evolving context in which EW capabilities operate. It will then go on to propose that a key pillar of EW advancement moving forward should be the development of EW capability that integrates autonomous consideration of civilian battlespace contexts in key killchain decisions. This is used as a key example of how fusion of EW data with other battlespace modelling data streams can provide entirely new insights that can inform better high-stakes decision making.

Electronic warfare capabilities fundamentally function to sense, identify and disrupt in the kill chain. Common Electronic Warfare capabilities that are most related to a typical killchain are: EW signal disruption to enemy Radio Frequency (RF) guided munitions, RF guided weapons for enemy counter-attacks/ neutralisation, infra-red imaging, Synthetic Aperture Radar (SAR) and Airborne Warning and Control (AWAC) targeting as part of broader Intelligence, Surveillance and Reconnaissance (ISR) and Suppression of Enemy Air Defences (SEAD) and other mission types/ objectives. Electronic Warfare capabilities fundamentally operate via the active emission or passive sensing of static or modulated electromagnetic signals.

One aspect of EW sensor data integration and application that is specifically lacking, as a prime example of the advantages to be gained from this developmental approach, is the fusion of Electronic Warfare sensor data with civilian battlespace context. While this exemplar application may not be front of mind to defence industry, who often prioritise kill chain efficiency and early enemy detection, it would significantly decrease the collateral damage experienced in populated warzones. Integrating EW sensor data with higher fidelity geographical and urbanisation data would arguably revolutionize the political acceptability and social acceptance of tactical strikes

and counter-strikes in defence of the free world. That is because, lethal defensive action could be proven to incorporate better consideration, and maximal avoidance of, unintended destructive consequences.

To elaborate, in recent years, the fallout resulting from contention and conflict in densely populated parts of the world such as Ukraine, Gaza and Taiwan has highlighted the collateral price of warfare. The unprecedented visibility we - as a global society - have to the communal consequences of conflict, thanks to the use of personal electronic devices (PEDs) and social media, has emphasized that precision warfare can often be deprioritised in the name of effective target neutralisation. Electronic Warfare is arguably becoming the defining capability of next-generation warfighter platforms, with EW sensors, EW guided weapons and signal jamming determining the survivability and lethality of our modern assets.

At the point of employing EW-guided lethal weapons or EW jamming with lethal intent, it is assumed that a reasonable attempt to mitigate collateral damages via diplomacy and non-lethal measures has been made. But in the case where lethal conflict cannot be mitigated, Electronic Warfare capabilities have a vital role to play in integrating ethical considerations into the killchain where they may otherwise be overlooked. In scenarios where EW guided weapons and jamming are used, any human operators on military platforms are under immense pressure to make split-second combat decisions. It is not reasonable to expect that they can always mentally comprehend the best target neutralisation tactics while also executing this in such a way that absolute minimal collateral damage is achieved. In this way, fusing EW sensing and targeting signals with urban and regional civilian related parameters will vastly improve the ability to minimise collateral damage.

It is proposed that collateral context be realised as a more important data input to battlespace representations. Specifically, collateral battlespace representation refers to the use of pre-collected mission data and real-time sensor data to fuse civilian population and building location/ density data with the location, velocity and target type of hostile targets as collected by EW functions on military platforms. While current EW capabilities have generally facilitated high levels of targeting accuracy, it is notable that accounting for warfare precision due to both weapons types and attack timing has anecdotally been a lower priority. Integrating these proposed additional battlespace data streams can improve warfare precision without compromising existing real-time mission objectives and tactical priorities.

While requiring additional computation, battlespace data fusion would mean that EW dependent weapons release or target jamming timing could be optimised to compromise and/or destroy the target while simultaneously influencing its terminal impact trajectory toward a local geographical collateral damage minima (i.e. least-populated or urbanised area). This would significantly contribute towards more precise and “collateral conscious” warfare. Importantly, it can also be implemented via autonomous data fusing and autonomous weapons release timing/ jamming schedule calculations. Given the aforementioned information load humans-in-the-loop experience when operating warfighter platforms, autonomous implementation ensures significant additional mental burden is not placed on any operators.

So how far from a “collaterally conscious” battlespace representation are we? And are there any significant technical considerations to be worked through before integrating an improved battlespace model with Electronic Warfare computations?

In recent decades, Intelligence Preparation of the Battlespace (IPB) has evolved from a focus on geography, topology and climate, to an IPB that champions physical location and identification of military assets, both friend and foe. Notably, variation on target sensing priorities is observed between the Air Force, Navy and Army. For example, aircraft sensors are postured to prioritise collecting lethal capability information to inform the onboard battlespace model whereas Army are typically concerned more with the geographic positioning of an enemy target. Generally speaking, a modern battlespace representation can be thought of as the summation of four categories of data; air and space data, surface and land data, information systems and functions data and human dimensional data. The majority of the data streams that make up these categories rely on EW capabilities to collect, update and combine with pre-loaded battlespace data and it is important to highlight that these data streams are not necessarily independent from each other.

The Air Force IPB process is appropriate to use to demonstrate the integration of the above proposed new data stream, given its inherent reliance on EW capabilities and therefore collection of related data to inform participant battlespace models. Civilian context data would be considered as mostly human dimensional data with elements that could be categorised as surface and land related data too. Importantly, this data goes onto construct a battlespace visualisation to inform decision making via a four-step IPB process (once again this process will be given in an Air Force exemplary context): define the battlespace environment, describe battlespace effects, evaluate Adversaries and finally, determine adversary operational areas. In a computational sense, these IPB process steps are continually evaluated and updated both pre-mission, during mission and post-mission. Regarding the example of civilian battlespace context, this data stream would be incorporated as human dimensional and surface data in phase 1 of the IPB computational process.

"The purpose of step one is to bound the intelligence problem and identify for further analysis specific features in the environment, activities within it, and the space where they exist that may influence available [operational areas]s or the commander's decisions."- (Lt Col Mark T. Satterly, Lt Col Kevin D. Stubbs, Maj Geryl D. Gilbert, Ms Cathy L. Iler, & Capt Kevin B. Glenn, 1999)

Once the Operational Area (OA) and Area of Interest (AI) are defined (whereby AI will always be larger than OA), mission objectives and desired end-states can be defined which facilitates mission execution planning.

In general, once an IPB process has produced a relatively converged battlespace visualisation, some form of a Decision Support Matrix (DSM) can be used in combination with the IPB battlespace model to determine optimal mission phase objectives and priorities. The DSM largely reverse engineers the best decision that can be made based on assumed achievable outcomes which are directly linked to observed battlespace participants and observed capabilities. Once again, there is significant opportunity to integrate more consideration of the civilian battlespace context in the DSM which will then have a compounding positive effect on overall conflict collateral damage when combined with the IPB civilian-data informed battlespace model.

Evidently, if the first phase of the IPB process lacks data fidelity, the entire subsequent mission planning and IPB phases can be sub-optimal and misinformed. This can exacerbate potential collateral damage outcomes when civilian battlespace data is not associated with EW-sensed

information in the DSM. This consideration deficiency is arguably occurring on a regular basis in mission planning and at key decision-making mission points due to the deprioritisation of fusing perceived "benign" data streams with real-time EW sensor data.

The question of how Australia remains advantageously relevant in the complex field of Electronic Warfare, given the current unstable global political climate, is by no means a simple conversation. In improving warfare to be more civilian and collateral destruction conscious via EW technology, Australia can become a leader in life-saving, ethically developed EW capability whereby we truly champion lethality as an extreme that can be more ethically minded even when violent confrontation is unavoidable. Informing EW capabilities with more battlespace context to autonomously minimise unnecessary warfare destruction is also a much-needed stride toward justifiable ethical guardrails in weaponised artificial intelligence. In the ever-increasing age of autonomous, software-defined warfare, Electronic Warfare related data fusion is the key to humanising emerging combat technology.

Generally, Australia should consider emerging Electronic Warfare progress against how it can improve the battlespace picture by using EW outputs more effectively. Not only from a singular platform's internal battlespace model, but how this can contribute to the larger shared battlespace visualisation. While there is still inherent improvements to be made in the accuracy of EW for weapons guidance as the warfare is fought with ever-accelerating kinematic capabilities, the real tactical advantage to be gained from EW technologies is to use produced sensing data in more complex computation and modelling to enable better informed decisions in the battlefield. While this essay has explored this via the specific example of EW data fusion with collateral damage informing data streams, there are many more applications that are heavily interwoven with EW capabilities that will revolutionise the nature of warfare, and Australia should realise their potential role in this.

In addition to the Association of Old Crows for their ongoing support of the Defence Engineering community, special mention should go to the following sources in informing some of the EW concepts and battlespace modelling concepts mentioned in this essay:

References

Lt Col Mark T. Satterly, U., Lt Col Kevin D. Stubbs, U., Maj Geryl D. Gilbert, U., Ms Cathy L. Iler, G.-1. D., & Capt Kevin B. Glenn, U. (1999). Intelligence Preparation of the Battlespace — An Airman's Introduction. *AF/XO White Paper*.

Stimson, G. W. (1998). *Introduction to Airborne Radar, 2nd Edition*. Raleigh, NC: The Institution of Engineering and Technology.

2024 Winner: Rhys Kissell

2024 Runner up: David Enchelmaier

2024 Runner up: Hope Sneddon