

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 dead¹. 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”².

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*³. 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*⁴.

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 equivalents⁵. 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 useless⁶.

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 armies⁷.

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 BRAVE1⁸, 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 article⁹, 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 Accelerator¹⁰. 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 casualties¹¹. 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 Lind¹², 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”¹³, 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.

¹ https://infographics.economist.com/2023/ExternalContent/ZALUZHNYI_FULL_VERSION.pdf

² <https://www.economist.com/europe/2023/11/01/ukraines-commander-in-chief-on-the-breakthrough-he-needs-to-beat-russia>

³ <https://www.armyupress.army.mil/Portals/7/Hot-Spots/docs/Russia/Mitre-Thomas.pdf> pp. 54

⁴ *Military Thought*, No. 5, 2016 pp. 22-27.

⁵ <https://apps.dtic.mil/sti/trecms/pdf/AD1137511.pdf> pp. 7

⁶ <https://www.washingtonpost.com/world/2024/05/24/russia-jamming-us-weapons-ukraine/>

⁷ <https://apps.dtic.mil/sti/trecms/pdf/AD1137511.pdf> pp. 14

⁸ <https://breakingdefense.com/2024/06/inside-ukraine-startups-try-to-edge-russia-in-the-electronic-warfare-race/>

⁹ <https://breakingdefense.com/2024/06/inside-ukraine-startups-try-to-edge-russia-in-the-electronic-warfare-race/>

¹⁰ <https://mil-tech.gov.ua/en>

¹¹ <https://www.naa.gov.au/students-and-teachers/student-research-portal/learning-resource-themes/war/first-world-war>

¹² *Maneuver Warfare Handbook*, 1983

¹³ <https://digital-commons.usnwc.edu/nwc-review/vol68/iss2/4/>