Electromagnetic Mass: The Asymmetric Future of Electronic Warfare

Rhys Kissell
Founder, Panop

The Wake-Up Call

“We are f—.”[1]

This terse conclusion by an unnamed NATO commander came after Exercise Hedgehog 2025 in Estonia — an undertaking whose results revealed that the slow-moving bureaucratic machinery of the democratic world is now endangering the lives of those who have signed up to protect it.

Hedgehog, which simulated a Russian invasion across Estonia’s border, involved more than 16,000 troops from 12 NATO countries, supported by Challenger 2 tanks, Apache attack helicopters, and HIMARS rocket artillery. By any measure of conventional military power, the defending force was formidable.

It made no difference. A team of roughly 10 Ukrainian drone operators, acting as the opposing force and equipped with first-person-view (FPV) strike drones and bomber drones assembled from commercial off-the-shelf (COTS) components, conducted a simulated counterattack that destroyed 17 armoured vehicles and struck 30 additional targets in approximately half a day, rendering 2 NATO battalions — representing between 1,000 and 2,000 troops, along with their vehicles, weapons, and supporting elements — combat-ineffective.[2] The exercise coordinator described the results as “frightening.” NATO units did not detect a single Ukrainian drone team throughout the entire engagement.[3]

This occurred during a period when Russian GNSS jamming from Kaliningrad was active at record levels across the Baltic region,[4] meaning that NATO forces were operating in a genuinely contested electromagnetic environment — and still could not counter COTS drones costing between $980 and $12,000 AUD apiece.

---

[1] J. K. Melchior, ‘Ukraine’s Drones Are a Warning to NATO’, *The Wall Street Journal*, 12 February 2026.

[2] A. Hanniotti, cited in ERR News and *The Ukrainian Review*, May 2025.

[3] Lt. Col. A. Probal and A. Hanniotti, cited in Melchior, *The Wall Street Journal*, 12 February 2026; corroborated by Militaeraktuell.at and ERR News.

[4] Flightradar24 data and Baltic Ministries of Defence reporting confirmed Russian GNSS jamming from Kaliningrad at record levels during the weeks of Exercise Hedgehog. See also: Defence News, ‘Researchers home in on origins of Russia’s Baltic GPS jamming’, 2 July 2025.

Exercise Hedgehog was not a technology demonstration. It was a paradigm failure. And it revealed a truth that the electronic warfare community must now confront: the decisive asymmetric advantage in future near-peer operations will not come from building superior individual platforms. It will come from achieving *electromagnetic mass* — deploying cognitive, software-defined electronic warfare capability across an entire force structure, at a cost and scale that inverts the exchange ratio favouring authoritarian adversaries.

The Cost-Exchange Problem

The concept of cost-exchange — the ratio between the cost of achieving an effect and the cost of negating it — has always been central to asymmetric strategy. In electronic warfare, this ratio has shifted decisively against Western forces, and the shift operates at 3 distinct levels.

The first is the weapon-countermeasure exchange. In Ukraine, Russian electronic warfare systems have rendered some of the West's most expensive precision munitions ineffective. The 155mm Excalibur GPS-guided projectile, costing approximately $170,000 USD per round, saw its accuracy fall to below 10 per cent due to Russian GNSS jamming. JDAM-ER guided bombs performed worse than their unguided predecessors, and the M30/M31 rockets used by HIMARS — a system Australia has recently acquired — have been similarly degraded.[5] At Hedgehog, even the counter-drone EW systems that should have defeated COTS drones either were not present at the point of need or proved inadequate. In each case, the cost to *negate* the weapon was a fraction of the cost of the weapon itself.

The second is the force structure exchange. Western electronic warfare has historically optimised for capability per platform. At the lowest end, handheld counter-drone jammers cost between $50,000 and $150,000 AUD. Specialised electronic warfare ground vehicles routinely exceed $50 million AUD, and dedicated EW aircraft can surpass $100 million. These assets are fielded in small numbers by specialist units at brigade or division level. The vast majority of the force has no organic EW capability whatsoever. The more capable and expensive the platform, the worse the cost-exchange becomes — and as Hedgehog demonstrated, even when these assets are available to the force, they may not be adequate for the most basic combat task: surviving contact with one of the most common classes of munition on the modern battlefield.

The directional jammer crystallises this failure. These handheld devices disrupt a single drone's control link by aiming a focused RF beam at it. Many members of the Armed Forces of Ukraine now consider them obsolete: experienced drone pilots know techniques for manoeuvring out of the beam, and the act of jamming itself alerts the pilot that a target is nearby. Rather than neutralising the threat, the jammer identifies the defender. Against a swarm approaching from

[5] The Washington Post, 'Russia turns to jamming to degrade U.S. weapons in Ukraine', 24 May 2024. Systems affected included the Excalibur GPS-guided projectile, JDAM-ER, and M30/M31 GMLRS rockets.

multiple vectors, it addresses one drone while the remaining 9 complete their attack. And yet, directional jammers remain what many Western governments procure as their primary counter-UAS EW solution, often exceeding $50,000 AUD per unit. The procurement system is optimised for the war we imagined, not the war being fought.

The third is the adaptation exchange. Legacy EW systems often operate on pre-programmed threat libraries: catalogues of known signal characteristics paired with pre-determined responses. When an adversary changes a waveform, modulation scheme, or control protocol, the defending system requires a manual update cycle — engineering analysis, software development, testing, certification, and distribution. This cycle is measured in months. On the Ukrainian frontline, drone control protocols evolve weekly. The cost of *adaptation* for the library-based defender is enormous and perpetual. For the adversary, it is trivial — a firmware update pushed to COTS hardware overnight.

Taken together, these 3 layers describe a systemic inversion. Western EW doctrine was built for the Cold War: high-end platforms engaging high-end threats in a relatively stable electromagnetic environment. For 2 decades, Western militaries focused on counter-terrorism and counter-insurgency operations that demanded little of their electronic warfare capabilities. During that same period, as a 2019 U.S. Department of Defense report acknowledged, adversary nations invested heavily in advancing theirs.[6] The consequence is that democratic forces are now structurally disadvantaged in precisely the domain that modern warfare depends upon most.

From Makerspaces to Cognitive Electronic Warfare

If the problem is structural, the solution must be too. Ukraine has demonstrated the first half of that solution under fire.

When Russia invaded in 2022, Ukraine's electronic warfare capabilities were largely based on ageing Soviet equipment. Within 2 years, Ukraine had engaged over 50 manufacturers and launched more than 100 electronic warfare projects through BRAVE1, a government initiative to rapidly develop and field domestic defence technology.[7] The engineers driving this effort were not drawn exclusively from the traditional defence industry. Many came from makerspaces, hackerspaces, and civilian electronics backgrounds — people who understood COTS hardware, open-source software, and rapid iteration.

---

[6] Department of Defense, Report on FY 2019 NDAA Section 1053, *Guidance on the Electronic Warfare Mission Area and Joint Electromagnetic Spectrum Operations*, September 2019.

[7] Breaking Defense, 'Inside Ukraine, startups try to edge Russia in the electronic warfare race', June 2024.

Ukraine achieved what former Commander-in-Chief Valerii Zaluzhnyi described as operational EW parity with Russia[8] — a force that U.S. and NATO commanders have repeatedly acknowledged possesses EW capabilities superior to Western equivalents.[9] Ukraine achieved this not by matching Russia's investment in bespoke platforms, but by embracing a fundamentally different design philosophy: COTS components, 3D-printed enclosures, open-source software, and a continuous cycle of rapid prototyping informed directly by frontline feedback. Ukrainian EW devices that perform comparably to Western equivalents costing $50,000–$150,000 AUD are being manufactured for $2,000–$3,000 AUD.

This approach proved a critical principle: *good enough at mass beats perfect in small numbers*. But it also revealed the ceiling of the current paradigm. COTS hardware and clever engineering can close the gap, but they cannot, alone, create a *compounding* advantage. That requires the second half of the solution: systems that learn.

The concept of cognitive radio, first articulated by Joseph Mitola III,[10] described a radio system capable of perceiving its electromagnetic environment and adapting its behaviour accordingly. This foundational idea has since been extended into electronic warfare, where the stakes are higher and the adaptation speeds more demanding. A cognitive EW system does not rely solely on pre-loaded threat libraries. Instead, it observes the electromagnetic environment in real time, classifies what it detects, identifies patterns, selects an optimal response, and executes — autonomously. Critically, it improves with every encounter. Each signal it classifies, each engagement it conducts, and each environment it operates in generates data that makes the system more effective.

This maps directly to John Boyd's Observe-Orient-Decide-Act (OODA) loop,[11] but executed at machine speed rather than human speed. A cognitive EW system cycles through Boyd's loop faster than any adversary can change waveforms or protocols, collapsing the temporal cost-exchange to near zero. The adversary must continuously invest in new techniques; the cognitive system absorbs each change as training data and improves.

The implications for the cost-exchange are transformative. Where a library-based system imposes a recurring engineering cost every time the threat evolves, a cognitive system's

[8] V. Zaluzhnyi, 'Modern Positional Warfare and How to Win In It', November 2023; interview with *The Economist*, 1 November 2023.

[9] T. Thomas, 'Russian Electronic Warfare Capabilities to 2025', MITRE/DTIC, September 2020, p. 7.

[10] J. Mitola III, 'Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio', PhD Dissertation, KTH Royal Institute of Technology, 2000. Mitola described cognitive radio; the extension of these principles to electronic warfare has since been developed by multiple researchers and defence organisations.

[11] J. Boyd, 'Destruction and Creation', 1976; 'Patterns of Conflict', 1986. Boyd's Observe-Orient-Decide-Act loop remains foundational to Western manoeuvre warfare doctrine.

marginal cost of adaptation approaches zero relative to a legacy library-centric approach. The more encounters it has, the smarter it becomes. The more units deployed, the more data generated. This is a compounding advantage, and it is extraordinarily difficult for an adversary to replicate without the same volume of real-world electromagnetic data.

Electromagnetic Mass

The convergence of COTS hardware and cognitive software produces a capability that has no precedent in electronic warfare: the ability to deploy EW to every node in a force structure, at a cost that makes mass deployment economically viable for the first time.

Consider the arithmetic. If a legacy EW system costs $100,000 AUD per unit, a force with a $5 million EW budget deploys 50 systems. These are distributed among specialist units at brigade level, leaving the vast majority of platoons, vehicles, and positions electromagnetically blind. If a software-defined, COTS-based EW node costs $5,000 AUD per unit, the same budget deploys 1,000. If the cost is driven below $3,000 AUD, the number approaches 2,000. At this scale, every platoon, every vehicle, every fixed position, and every uncrewed platform becomes an EW node — sensing, reporting, and when authorised, acting.

This is *electromagnetic mass*, and its asymmetric effects are qualitatively different from simply having more jammers.

First, electromagnetic mass creates an *intractable targeting problem* for the adversary. When a force operates 50 EW nodes, an adversary's intelligence, surveillance, and reconnaissance apparatus can feasibly locate, classify, and target each one. When that force operates 5,000 nodes — many of which are generating jamming, deception, and decoy emissions — the adversary can no longer easily distinguish high-value emitters from hundreds or thousands of low-value nodes, each contributing to a blanket of electromagnetic effects. Every resource they dedicate to finding and neutralising EW nodes is a resource diverted from other tasks, and even successful targeting of individual nodes does not meaningfully degrade the network. The system is resilient through redundancy, not through hardening.

Second, electromagnetic mass generates a *compounding intelligence advantage*. Every node deployed is a sensor. Every sensor collects data on the adversary's electromagnetic emissions, waveforms, protocols, and behaviour. When aggregated and fed into cognitive AI models, the entire network becomes smarter with every mission. The force that achieves electromagnetic mass first accumulates a dataset of real-world adversary signals that cannot be synthesised or purchased — it can only be generated through operational deployment at scale. This creates a self-reinforcing cycle that is extraordinarily difficult for an adversary to replicate.

Third, electromagnetic mass enables *electromagnetic deception at scale*. When thousands of low-cost nodes are capable of generating authentic electromagnetic signatures — mimicking the emissions of command posts, armoured vehicles, air defence radars, or communications hubs — the adversary's confidence in their targeting and intelligence picture is systematically degraded. They must dedicate scarce reconnaissance assets to determine which emitters are real and which are decoys, and the answer may change in seconds. The cognitive layer makes this deception adaptive: the system learns which deception techniques the adversary responds to and adjusts accordingly. The net effect is a thick fog of war that cannot easily be lifted — degrading the adversary's ability to act while preserving one's own freedom of manoeuvre.

A natural objection is that coordinating thousands of EW nodes creates its own problems — fratricide, interference, and command-and-control complexity. In practice, a well-architected distributed network improves rather than compounds these challenges. More connected nodes mean richer situational awareness, making electromagnetic fratricide a product of negligence rather than inevitability. Specialised C2 architectures for cognitive EW may be necessary, but the engineering problem is tractable. The alternative — continuing to field a small number of nodes that the adversary can locate and destroy — is not.

In practice, this transforms the character of engagement. Consider a force element moving through contested littoral terrain, every vehicle and dismounted position carrying a cognitive EW node. When an adversary drone swarm launches, dozens of nodes detect the control signals simultaneously, classify them in milliseconds, and begin coordinated disruption — not from a single directional beam, but from overlapping fields across the area of operations. The swarm's control links degrade from multiple directions. Its navigation references are spoofed. Every signal it emits is catalogued, feeding the network's model of the adversary's next iteration. The force has not fired a shot, but the attack has failed — and the next attack will be harder to execute, because the network has learned.

Exercise Hedgehog demonstrated what happens to a force that lacks electromagnetic mass. NATO formations were detected immediately by cheap aerial sensors and struck before they could respond — 10 operators with several dozen drones.[12] In a near-peer conflict, the electromagnetic equivalent of this scenario would see a force without distributed EW capability blinded, jammed, deceived, and stripped of its communications, navigation, and targeting systems — not by a single exquisite adversary platform, but by thousands of small, cheap, intelligent nodes that are everywhere at once.

[12] I. Raag, analysis published following Exercise Hedgehog 2025, cited in multiple outlets including DroneXL and ERR News. Ukrainian drone pilots estimated Estonia alone would require approximately 200,000 drones per month during wartime.

Implications for Australia

These dynamics carry particular weight for Australia. The electronic warfare capabilities of the world's major authoritarian military powers have advanced rapidly while Western attention was elsewhere. The People's Liberation Army has been described as "an electronic warfare juggernaut" in testimony to the U.S. Government,[13] and Russia's electronic warfare forces are assessed as world-class by the U.S. Defense Intelligence Agency.[14] Admiral Philip Davidson's 2021 assessment that the window of greatest risk for conflict over Taiwan could arrive as early as 2027 — the "Davidson Window" — remains a central planning assumption across Western defence establishments.[15] Critically, these capabilities are not developing in isolation. PLA observers embedded with Russian armed forces are absorbing electronic warfare lessons from Ukraine in real time, meaning that the threat facing Australian forces is continuously improving.

The Australian Defence Force is a small, technologically capable force. In any future near-peer scenario, it will need to operate in an electromagnetic environment contested by adversaries with decades of dedicated investment in electronic warfare. Australia cannot outspend those adversaries on platforms. Nor should it try. The asymmetric path is to outscale — to achieve electromagnetic mass through software-defined, AI-enabled systems built on COTS hardware, deployed to every element of the joint force. This approach plays to Australia's strengths: a technically skilled workforce, strong partnerships through AUKUS and the Five Eyes, and a defence innovation ecosystem that has demonstrated the capacity to produce world-class capability in niche domains.

The challenge is institutional, not technological. The technology to build distributed, cognitive, software-defined EW exists today. What is required is the willingness to break from legacy procurement — to stop purchasing refinements of concepts that Ukraine's frontline has already rendered obsolete, and to invest in the architecture that Hedgehog proved is needed. This means EW capability at the platoon level, not the brigade level. It means software that updates in hours, not hardware that updates in years. It means the Department of Defence and the Australian Communications and Media Authority enabling Australian electronic warfare ventures to iterate and test at speed — a conversation that is overdue, because the question is no longer how to avoid falling behind, but how to recover from a position that is already behind.

---

[13] J. M. Dahm, Testimony before the U.S.-China Economic and Security Review Commission, Hearing on China's Evolving Counter Intervention Capabilities, March 2024.

[14] U.S. Defense Intelligence Agency, *Russia Military Power: Building a Military to Support Great Power Aspirations*, 2017; updated assessments in DIA annual threat briefings through 2024.

[15] Admiral P. Davidson, Testimony before the U.S. Senate Armed Services Committee, March 2021.

Most importantly, it means revisiting the compliance architecture applied to electronic warfare development. Currently, an EW system destined for service may have up to 5 separate safety margins applied during test and evaluation: one derived from ARPANSA standards, one from the Defence Radiation Safety Authority, one from the Capability Acquisition and Sustainment Group, one at the discretion of the individual test officer, and the manufacturer's own margin embedded in the design. Each of these is individually reasonable. Stacked together, they can reduce an operationally effective system to one that is compliant on paper but ineffective in the field — precisely the outcome that Hedgehog exposed. If Australia is serious about fielding asymmetric electromagnetic capability, it must empower the operators and engineers closest to the problem, and design a regulatory framework that enables speed without abandoning safety.

Ultimately, it means accepting that in a domain defined by adaptation speed, *good enough now* is worth infinitely more than *perfect eventually*.

As the Australian Defence Force continues to explore littoral manoeuvre warfare in Australia's immediate region, it must recognise that manoeuvre depends entirely on electromagnetic superiority. Zaluzhnyi's observation from Ukraine applies directly: without it, manoeuvre warfare collapses into positional, attrition warfare, and the enemy chooses when, where, and how to fight.[16] For a small force operating across vast maritime distances, positional warfare is not a stalemate — it is a defeat.

Conclusion

Retired General David Petraeus, reflecting on Hedgehog 2025, offered a warning: lessons are not learned when they are identified, but only when new concepts are developed, doctrine rewritten, organisational structures changed, training overhauled, and materiel requirements set out that drive the procurement process.[17]

The lesson of Hedgehog has been identified. 10 operators with FPV strike drones and bomber drones built from COTS components defeated 2 battalions of a modern Western force. The electronic warfare systems that should have protected those battalions were inadequate or obsolete. Russian jamming from Kaliningrad provided a contested electromagnetic environment that NATO was unprepared for.

The lesson that must now be *learned* is that the future of electronic warfare is not a better jammer, a faster library update, or a more expensive platform. It is electromagnetic mass: thousands of cognitive, software-defined, networked EW nodes deployed across the entire

[16] Zaluzhnyi, op. cit.

[17] Gen. D. Petraeus (Ret.), cited in Melchior, *The Wall Street Journal*, 12 February 2026.

force, learning in real time, adapting at machine speed, and creating an electromagnetic environment so distributed that no adversary can unpick it.

The bloc that achieves electromagnetic mass first — whether democratic or authoritarian — will define the outcome of the next great power conflict. Whichever does not will find itself in the precarious position NATO found itself in at Hedgehog — but the violence will not be simulated this time.

The Australian Army fields 7 infantry battalions. Just 35 trained drone pilots could take them out of the fight. To paraphrase Marcus Aurelius: Australia can waste no more time arguing what an effective fighting force looks like. It must build one.

Bibliography

[1] Melchior, J. K., ‘Ukraine’s Drones Are a Warning to NATO’, The Wall Street Journal, 12 February 2026.

[2] Hanniotti, A., cited in ERR News and The Ukrainian Review, May 2025.

[3] Probal, Lt. Col. A. and A. Hanniotti, cited in Melchior, The Wall Street Journal, 12 February 2026; corroborated by Militaeraktuell.at and ERR News.

[4] Flightradar24 data and Baltic Ministries of Defence reporting, May–June 2025. See also: Defence News, ‘Researchers home in on origins of Russia’s Baltic GPS jamming’, 2 July 2025.

[5] The Washington Post, ‘Russia turns to jamming to degrade U.S. weapons in Ukraine’, 24 May 2024.

[6] Department of Defense, Report on FY 2019 NDAA Section 1053, Guidance on the Electronic Warfare Mission Area and Joint Electromagnetic Spectrum Operations, September 2019.

[7] Breaking Defense, ‘Inside Ukraine, startups try to edge Russia in the electronic warfare race’, June 2024.

[8] Zaluzhnyi, V., ‘Modern Positional Warfare and How to Win In It’, November 2023; interview with The Economist, 1 November 2023.

[9] Thomas, T., ‘Russian Electronic Warfare Capabilities to 2025’, MITRE/DTIC, September 2020.

[10] Mitola, J. III, ‘Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio’, PhD Dissertation, KTH Royal Institute of Technology, 2000.

[11] Boyd, J., ‘Destruction and Creation’, 1976; ‘Patterns of Conflict’, 1986.

[12] Raag, I., analysis published following Exercise Hedgehog 2025, cited in DroneXL and ERR News.

[13] Dahm, J. M., Testimony before the U.S.-China Economic and Security Review Commission, Hearing on China’s Evolving Counter Intervention Capabilities, March 2024.

[14] U.S. Defense Intelligence Agency, Russia Military Power: Building a Military to Support Great Power Aspirations, 2017.

[15] Davidson, Admiral P., Testimony before the U.S. Senate Armed Services Committee, March 2021.

[16] Zaluzhnyi, V., op. cit.

[17] Petraeus, Gen. D. (Ret.), cited in Melchior, The Wall Street Journal, 12 February 2026.