National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

# A GAP IN THE FOUNDATION: CANADIAN ARMY TRAINING IN DEGRADED ENVIRONMENTS

Major James Cressall

**JCSP 49**

**Service Paper**

**Disclaimer**

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.



**PCEMI n° 49**

**Étude militaire**

**Avertissement**

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.



Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 49 - PCEMI n° 49
2022 - 2023

Service Paper – Étude militaire

# A GAP IN THE FOUNDATION: CANADIAN ARMY TRAINING IN DEGRADED ENVIRONMENTS

Major James Cressall

# A GAP IN THE FOUNDATION:
# CANADIAN ARMY TRAINING IN DEGRADED ENVIRONMENTS

## AIM

1. Maintaining the ability to operate in degraded or austere systems and information environments is a requirement established in both the Canadian Army (CA) Modernization Strategy (CAMS) and the Canadian Land Operations Operating Concept, *Close Engagement*. Allies and competitors have incorporated this axiom into both force development and force generation in recent years, with the current war in Ukraine serving to underline the importance of it. Despite this, no current Canadian Army publication, doctrine manual, or order explicitly mandates training in such an environment. The aim of this service paper is to delineate this deficiency and provide actionable recommendations to the Army Training Authority (ATA) for the formalization of training in degraded or austere environments as an essential element of CA foundation training.

## INTRODUCTION

2. The rapid development of technology and the integration and increasing importance of the space, cyber, and information domains have characterized the security environment over the last two decades. The development, proliferation, and accessibility of formerly exquisite and expensive technologies between various state and non-state actors suggests that the technological superiority that Western militaries have grown accustomed to can no longer be relied upon.[1] In light of Russia's invasion of Ukraine, alongside other increasingly aggressive state actors, the Canadian Armed Forces (CAF) must be prepared to operate and compete across the spectrum of conflict in contested environments against peer and potentially technologically superior adversaries. For the CA, these environments will be characterized by degraded networks, communications, and satellite-enabled systems.[2] To preserve its ability to fight cohesively and win, the CA must explore and leverage new technology to gain and retain the advantage. However, technology cannot and will not fully mitigate this inevitable degradation. Equally important is the requirement to build resiliency through training in environments that replicate the contemporary and future threats. Recent CA publications reflect these realities, at least in rhetoric.

3. According to *Canada's Future Army*, the preservation of land combat capabilities that rely on cyber and electronic warfare systems "will require smarter capability development, including the ability to work within degraded systems and networks."[3] This ability is largely conceptualized through the lens of enhanced technology and defensive measures. The more recent CA Operating Concept, *Close Engagement*, appears to acknowledge the requirement for training by stating that the "Army must also carefully plan for and practise the ability to operate

---

1. Canada, Department of National Defence, A-PP-106-000/AF-001, *Advancing with Purpose: The Canadian Army Modernization Strategy* (Ottawa: Canadian Army Headquarters, 2020), 5.
2. Canada, Department of National Defence, B-GL-007-000/JP-009, Canada's Future Army, Volume 2: Force Employment Implications (Kingston: Canadian Army Land Warfare Centre, 2017), 63.
3. Department of National Defence, *Canada's Future Army, Volume 2*, 65.

in reversionary modes when its use of the network is degraded."[4] However, this statement is made in virtual isolation with no supporting concepts or guidance. This paper seeks to fill that gap. To do so, it will first provide brief examples of the potential threats to CA communications, networks, and systems which currently characterize the operating environment. It will then outline lessons that may be drawn from the American, Chinese, and Russia armed forces. The paper will subsequently describe the gap in the CA's current approach to training as well as opportunities for enhancement before concluding with recommendations for the CA ATA.

## DISCUSSION

4. To frame the discussion that follows, it is necessary to define what is meant by a "degraded environment". Many different terms and interpretations of the concept exist across the Canadian and American militaries alone. The CA's *Close Engagement* uses the phrase "degraded or austere information environment" to describe the issue, with a primary focus on networks that are impacted by an adversary or by the environment.[5] The United States (U.S.) Navy uses D2E for "degraded or denied environment" while the U.S. Air Force uses "contested environment", both with a focus on the effects of adversarial action.[6] The United States (U.S.) Marine Corps (USMC) employs the more holistic acronym DDIL or "denied, degraded, intermittent and limited (bandwidth)".[7] This is used to describe conditions in which military communications, networks, and/or systems unintentionally malfunction, are degraded by the physical environment, or are deliberately interfered with or attacked by an adversary. Given that the antidote being proposed herein remains the same regardless of the cause, the more holistic term DDIL will be used henceforth.

### The Threat

5. While tactical communications have long served as a critical enabler of CA operations, current CA force employment also sees a near-ubiquitous reliance on the global positioning system (GPS) and satellite-enabled networks. The evolution of satellite-on-the-move and tactical data link technology, among other capabilities, and their integration at the lowest tactical levels will see this reliance on technology continue to grow. Though all militaries continually seek to improve and harden their capabilities against known threats, all communications, networks, and satellite-enabled capabilities remain vulnerable to the physical environment, technical failure, and adversary action. While these threats can each be significantly disruptive, the focus of this brief threat overview will be on the latter. Given the limited scope of this paper, electronic warfare (EW), cyber, and anti-satellite threats will be briefly examined with an example given for each.

6. Current electronic warfare (EW) capabilities are well known to possess the potential to interfere with and degrade tactical and satellite communications and networks as well as GPS.

---

4. Canada, Department of National Defence, B-GL-310-001/AG-001, *Close Engagement: Land Power in an Age of Uncertainty: Evolving Adaptive Dispersed Operations* (Kingston: Canadian Army Land Warfare Centre, 2019), 39.
5. Department of National Defence, *Close Engagement, 33.*
6. Travis Suggs, "Overcoming Degraded Communications under A2AD: A Doctrinal Solution," Joint Military Operations Department paper, Naval War College, 2014, https://apps.dtic.mil/sti/pdfs/ADA609300.pdf, 16.
7. Spencer Waters, "Training in The DDIL Environment: Building Nuanced Tactical Proficiency," Marine Corps Gazette (September 2022), https://mca-marines.org/wp-content/uploads/Training-in-the-DDIL-Environment.pdf, 26.

Most modern militaries field EW platforms for defensive and offensive purposes, with the CA being no different. To frame this potential threat, the Russian Army has long incorporated offensive EW or electronic attack (EA) into its doctrine and fields a variety of ground-based EW assets at a relatively low tactical level.[8] It has employed its EW capabilities against the Ukrainian Army in eastern Ukraine since its 2014 annexation of Crimea and as anticipated, during its 2022 invasion. While the Russian Army experienced unexpected difficulties in the employment of EW in the opening days of the war, there are increasing reports of its successful use. During the Battle of Kyiv, some reports suggest that it was highly effective in severely degrading Ukrainian tactical communications, with commanders "[falling] back to old fashioned runners when their communications went down."[9] As the battle lines have become more fixed, Russian use of EW has increased, with one Ukrainian official stating, "They are jamming everything their systems can reach…We can't say they dominate, but they hinder us greatly."[10] This hindrance is not just to tactical communications but to GPS and targeting systems as well. It can be expected that such impacts will characterize the future threat environment as well.

7. Army networks and satellite-enabled systems are equally vulnerable to anti-satellite and cyber attacks. The Canadian Defence Policy, *Strong, Secure, Engaged*, notes that various state and non-state actors "already have an ability to temporarily disrupt space-based services, such as the [GPS] or satellite communications, and a smaller number have the ability…to cause more permanent effects, including the destruction of satellites."[11] The U.S. Defense Intelligence Agency's 2019 report on China's military capabilities reflects this assessment. The report quotes a People's Liberation Army (PLA) publication that describes a means to "blind and deafen the enemy" by "destroying, damaging, and interfering with the enemy's reconnaissance…and communications satellites."[12] In the cyber realm, the PLA maintains a robust cyber attack capability under its Strategic Support Force. It is assessed as having the potential to target and degrade an adversary's network-based command and control (C2), logistics networks, and command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities, especially during the early stages of conflict.[13] While this paper does not suggest that the CA may one day have to contend with the PLA's space and cyber capabilities, a number of potential adversaries will possess similar capabilities in the future.

---

8. United States, Defense Intelligence Agency, *Russia Military Power: Building a Military to Support Great Power Aspirations* (Washington, D.C.: Defense Intelligence Agency, 2017), https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/Russia_Military_Power_Report_2017.pdf, 42.
9. Dan Rice, "The Untold Story of the Battle for Kyiv," Small Wars Journal, May 31, 2022, https://smallwarsjournal.com/jrnl/art/untold-story-battle-kyiv.
10. Oleksandr Stashevskyi and Frank Bajak, "They're Jamming Everything: How Secretive Electronic Warfare Shapes War in Ukraine," The Times of Israel, June 3, 2022, https://www.timesofisrael.com/theyre-jamming-everything-secretive-electronic-warfare-shapes-war-in-ukraine/.
11. Canada, Department of National Defence, *Strong, Secure, Engaged: Canada's Defence Policy* (Ottawa: Department of National Defence, 2017), https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html, 57.
12. United States, Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win* (Washington, D.C.: Defense Intelligence Agency, 2019), https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/China_Military_Power_FINAL_5MB_20190103.pdf, 43.
13. Defense Intelligence Agency, *China Military Power*, 46.

**Lessons From Other Militaries**

8. In consideration of the threats described above and their potential impact on CA operations, it is worth examining the approaches to threat mitigation of Canada's closest ally and its main competitors. Within the last five years, the USMC and U.S. Army have both acknowledged the enhancement of anti-access, area denial capabilities of the U.S.'s strategic competitors and adversaries, which include EW, cyber, and anti-space capabilities, weapons and platforms as summarized above. Both services have begun to re-posture their forces accordingly. The USMC now incorporates GPS and satellite communications degradation as part of their large-scale training exercises.[14] While this does not simulate all potential threats, such as the effect of EA on tactical communication, it still serves the valuable purpose of training soldiers and leaders to recognize systems degradation, mitigate the deficiency or adapt, and fight through. Similarly, the commander of U.S. Army Forces Command has directed the design of training "that focus on units conducting operations in contested electronic warfare, cyber, and space environments."[15] Noting the practical and legal challenges to conducting live EA or offensive cyber in training, the U.S. Army and USMC are both also exploring simulation solutions to replicate the effects of such attacks.[16] Their progress should be followed with interest by the CA and the Canadian Manoeuvre Training Centre (CMTC) specifically as the national training centre and primary owner of the CA's weapons effects simulation.

9. There are also lessons to be taken from Russia's experience in Ukraine, as well as PLA Ground Force doctrine. As noted, the Russian Army's difficulties in employing EW in Ukraine surprised Western military observers and analysts based on the quantity and reported capabilities of their ground-based EW platforms. Reports indicate though that the Russian Army was forced to cease EW jamming due to its unforeseen effect on their own tactical communications.[17] One potential assessment of this critical failure is that Russian Army tactical units were poorly trained pre-conflict in operating in environments degraded by EA. As one retired senior U.S. Air Force Electronic Warfare Officer observed, "good militaries train their personnel to operate in a degraded electromagnetic spectrum…."[18] It appears the Russian Army may not have done so. Conversely, it appears that the PLA recognizes the importance of such training and has embraced it in doctrine and practice. A recently released U.S. Army Technical Publication notes that current PLA Ground Force doctrine requires that their units train in "communications blackout

---

14. Stew Magnuson, "U.S. Forces Prepare for a 'Day Without Space'," National Defense, February 1, 2014, https://www.nationaldefensemagazine.org/articles/2014/2/1/2014february-us-forces-prepare-for-a-day-without-space.
15. United States, Government Accountability Office, GAO-19-570, *Future Warfare: Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations* (Washington, D.C.: Government Accountability Office, 2019), https://www.gao.gov/assets/gao-19-570.pdf, 13.
16. Christopher Dupre, Nathan Watnabe, Alesya Paschal, and Steve Miskinis, "Training for Operations in a Contested Space Domain," Paper presented at the MODSIM World 2018 Conference, Norfolk, 24 April 2018, https://www.modsimworld.org/papers/2018/MODSIM_2018_Paper_not_required_for_a_44.pdf; Spencer Waters, "Training in The DDIL Environment," 28.
17. Thomas Withington, "Russia's Electronic Warfare Capabilities Have Had Mixed Results Against Ukraine," The War Zone, June 16, 2022, https://www.thedrive.com/the-war-zone/this-is-whats-happened-so-far-in-ukraines-electronic-warfare-battle.
18. Jeffrey Fischer, "A Key Reason for Russia's Colossal Electronic Warfare Failure in Ukraine," The Defense Post, April 13, 2002, https://www.thedefensepost.com/2022/04/13/russia-electronic-warfare-failure-ukraine/.

conditions, relying on ingenuity and tactical competency to overcome the effects of communications isolation, and wherever possible, use communications means that are not susceptible to enemy EW efforts."[19] While such practices may be occasionally observed in CA training, there is no similar mandate to do so.

**The Canadian Army Approach to Training**

10. Aside from the singular statement in *Close Engagement* that notes the requirement to train the CA's ability to operate in so-called "reversionary modes" – understood to mean analog methods or tactics, techniques, and procedures (TTPs) not reliant on technology – current CA training guidance makes no mention of this type of training. Canadian Army Order (CAO) 23-21, the CA Collective Training (CT) Policy for Foundation Training (FT), outlines the annual minimum requirement for collective training at various levels across the CA's combat arms, combat support, and combat service support elements. The CAO correctly notes that "a relevant and fit-for-purpose FT programme is vital to ensure the CA is investing appropriately in maintaining warfighting competencies."[20] As the framework document for FT, this order must be prioritized for review and revision as the operating and threat environments evolve. A review of the directed annual CT battle task standards (BTS) requirements for fiscal year 22/23, published in the CA operating plan, also identify a gap in training policy. No currently mandated BTS include a requirement to train in degraded environments.

11. As alluded to above, the absence of a formal requirement, guidance or doctrine for training in degraded environments does not prevent CA sub-units and units from training for it. Indeed, based on individual leaders' threat assessments of contemporary adversary capabilities and the perceived potential impact on their operations, sub-units and units do simulate and train in degraded environments. However, this approach is ad hoc and therefore not well resourced, not grounded in the most comprehensive threat picture, and not standardized across brigades, let alone the CA. As such, CA elements that try to simulate and train in degraded environments fail to realize the full potential of such training. On the other hand, if such training were CA-directed, standardized, and nested within doctrine, it would enhance resiliency across the force given the inherent challenges of operating under such conditions. In addition to promoting mastery of the basics, it would also encourage adaptability and innovation which will remain vital elements of the CA's ability to succeed in conflict. As a by-product, the requirement to operate with limited or no tactical communications would likely also go a long way to training and institutionalizing the elusive concept of mission command.

**CONCLUSION**

12. Clausewitz stated that "in war, while everything may be simple, even the simplest thing is difficult".[21] In the context of war, nowhere is this truer than in a degraded environment. The

---

19. United States, Department of the Army, ATP 7-100.3, *Chinese Tactics* (Washington, D.C.: Army Publishing Directorate, 2021), https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34236-ATP_7-100.3-001-WEB-3.pdf, 7-2.
20. Canadian Army, *CAO 23-21, Canadian Army Collective Training Policy – Foundation Training* (Kingston: Canadian Army Doctrine and Training Centre, 2021), 7.
21. Jeffrey Fischer, "A Key Reason for Russia's Colossal Electronic Warfare Failure in Ukraine".

CA's assessment of the future operating environment, its modernization strategy, and its operating concept all appear to acknowledge the high probability of conducting operations in such environments in the years to come. Nevertheless, the current lack of formal direction to train for it, let alone supporting doctrine or TTPs, creates a cognitive dissonance and potentially significant capability gap. The current ad hoc approach being taken by tactical-level leaders and units is grounded in necessity, based on a legitimate threat, and well-intended. However, it exacerbates the existing lack of standardization across the CA and encourages the development of unit-level standard operating procedures rather than TTPs nested in doctrine. The CA must therefore draw on lessons from its allies, competitors, and contemporary conflict to enhance its FT and doctrine to address the threats and build resilience and adaptability across the force. The following recommendations to the CA ATA, listed in order of priority, offer both immediately actionable and longer-term measures to close the existing gap and set conditions for the CA to continue to fight and win regardless of technological superiority.

## RECOMMENDATIONS

13. Communicate the Problem. In coordination with the broader CAF, the CA should adopt and promulgate a single term to describe a degraded communications, networks, and/or systems environment. As the most holistic term in current use, and given its applicability across the joint force, "DDIL" is recommended. This will establish a common vernacular, socialize the threat, and start the conversation around training.

14. High Readiness Forces First. It is recommended that the CA ATA explicitly mandate the requirement to train in DDIL environments as part of training design guidance under the Enhanced Warfighting Proficiency Training Direction Annex to the CA Operating Plan, as well as in ATA's High Readiness Forces Enhanced Warfighting Proficiency Training Directive. For 2024, the ATA should direct CMTC to incorporate a GPS and/or communications-degraded scenario as part of the EWP exercise, MAPLE RESOLVE. This will ensure that CA elements slated for contingency operations are adequately prepared for full spectrum operations.

15. Update the Policy. To ensure that this direction is subsequently communicated and applied across the CA, it is recommended that CAO 23-21 be updated accordingly. Noting that CA brigades and units are already challenged to meet individual and collective task requirements given ubiquitous personnel and resource constraints, training to operate in DDIL environments should be assigned priority as CA "key terrain" with other training requirements to be correspondingly reduced.[22] Army Common BTS as well as trade specific BTS should be updated to include a new BTS that directs the achievement of specific tasks in a DDIL environment. Examples could include "Establish and Maintain Command and Control in a DDIL Environment" as Army Common BTS and "Company – Execute an Attack in DDIL Environment" as Infantry-specific BTS. Alternatively, conditions could be added to specific BTS to complete requirements denied GPS or communications. Upon completion, Annex A to CAO 23-21, Annual CT BTS requirements, should also be updated.

---

22. Jesse van Eijk, "Doing Too Much with Too Little, All of the Time: The Effects of Tempo on Canadian Infantry Battalions," Joint Command and Staff Programme Directed Research Paper, Canadian Forces College, 2018.

16. Update the Doctrine. In coordination with allied armies, the CA's Land Warfare Centre should consider the requirement for a doctrine manual specific to tactical operations in DDIL environments. This publication could take a form similar to those of other unique or complex environments such as Arctic, Jungle, and Urban operations. Alternatively, considerations for operations in a DDIL environment could be incorporated in CA common and trade-specific operations manuals as they are due for renewal.

**BIBLIOGRAPHY**


Canada. Department of National Defence. A-PP-106-000/AF-001. *Advancing with Purpose: The Canadian Army Modernization Strategy*. Ottawa: Canadian Army Headquarters, 2020.

Canada. Department of National Defence. B-GL-007-000/JP-009. *Canada's Future Army, Volume 2: Force Employment Implications*. Kingston, Canadian Army Land Warfare Centre, 2017.

Canada. Department of National Defence. B-GL-300-001/FP-001. *Land Operations*. Ottawa: Chief of the Land Staff, 2008.

Canada. Department of National Defence. B-GL-300-008/FP-001. *Training for Land Operations*. Ottawa: Commander Canadian Army, 2014.

Canada. Department of National Defence. B-GL-310-001/AG-001. *Close Engagement: Land Power in an Age of Uncertainty: Evolving Adaptive Dispersed Operations*. Kingston: Canadian Army Land Warfare Centre, 2019.

Canada. Department of National Defence. B-GL-383-002/FP-002. *Battle Task Standards, Volume 2*. Kingston: Army Publishing Office, 2012.

Canada. Department of National Defence. B-GL-383-003/FP-001. *Individual Battle Task Standards for Land Operations*. Kingston: Army Publishing Office, 2012.

Canada. Department of National Defence. *Strong, Secure, Engaged: Canada's Defence Policy*. Ottawa: Department of National Defence, 2017. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html.

Canadian Army. *CAO 23-21, Canadian Army Collective Training Policy – Foundation Training*. Kingston: Canadian Army Doctrine and Training Centre, 2021.

Dupre, Christopher, Nathan Watnabe, Alesya Paschal, and Steve Miskinis. "Training for Operations in a Contested Space Domain." Paper presented at the MODSIM World 2018 Conference, Norfolk, 24 April 2018. https://www.modsimworld.org/papers/2018/MODSIM_2018_Paper_not_required_for_a_44.pdf.

Fischer, Jeffrey. "A Key Reason for Russia's Colossal Electronic Warfare Failure in Ukraine." *The Defense Post*. April 13, 2002. https://www.thedefensepost.com/2022/04/13/russia-electronic-warfare-failure-ukraine/.

Magnuson, Stew. "U.S. Forces Prepare for a 'Day Without Space'." *National Defense*, February 1, 2014. https://www.nationaldefensemagazine.org/articles/2014/2/1/2014february-us-forces-prepare-for-a-day-without-space.

Rice, Dan. "The Untold Story of the Battle for Kyiv." *Small Wars Journal*. May 31, 2022. https://smallwarsjournal.com/jrnl/art/untold-story-battle-kyiv.

Turunen, Andreas. "The Broader Challenge of Russian Electronic Warfare Capabilities." In *Improvisation and Adaptability in the Russian Military*. Washington, D.C.: Center for Strategic and International Studies, 2020. https://www.jstor.org/stable/resrep24241.

Waters, Spencer. "Training in The DDIL Environment: Building Nuanced Tactical Proficiency." *Marine Corps Gazette* (September 2022): 26-29. https://mca-marines.org/wp-content/uploads/Training-in-the-DDIL-Environment.pdf.

Stashevskyi, Oleksandr and Frank Bajak. "They're Jamming Everything: How Secretive Electronic Warfare Shapes War in Ukraine." The Times of Israel. June 3, 2022. https://www.timesofisrael.com/theyre-jamming-everything-secretive-electronic-warfare-shapes-war-in-ukraine/.

Suggs, Travis. "Overcoming Degraded Communications under A2AD: A Doctrinal Solution." Joint Military Operations Department paper, Naval War College, 2014. https://apps.dtic.mil/sti/pdfs/ADA609300.pdf.

United States. Defense Intelligence Agency. *China Military Power: Modernizing a Force to Fight and Win*. Washington, D.C.: Defense Intelligence Agency, 2019. https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/China_Military_Power_FINAL_5MB_20190103.pdf

United States. Defense Intelligence Agency. *Russia Military Power: Building a Military to Support Great Power Aspirations*. Washington, D.C.: Defense Intelligence Agency, 2017. https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/Russia_Military_Power_Report_2017.pdf.

United States. Department of the Army. ATP 7-100.3. *Chinese Tactics*. Washington, D.C.: Army Publishing Directorate, 2021. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34236-ATP_7-100.3-001-WEB-3.pdf.

United States. Government Accountability Office. GAO-19-570. *Future Warfare: Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations*. Washington, D.C.: Government Accountability Office, 2019. https://www.gao.gov/assets/gao-19-570.pdf.

van Eijk, J. "Doing Too Much with Too Little, All of the Time: The Effects of Tempo on Canadian Infantry Battalions." Joint Command and Staff Programme Directed Research Paper, Canadian Forces College, 2018.

Withington, Thomas. “Russia’s Electronic Warfare Capabilities Have Had Mixed Results Against Ukraine.” *The War Zone*. June 16, 2022. https://www.thedrive.com/the-war-zone/this-is-whats-happened-so-far-in-ukraines-electronic-warfare-battle.