
# Navigating the Digital Battlefield

## *Understanding Cyber Electromagnetic Activities in Warfare*

By Lieutenant Colonel Athanasios Sdrakas, GRC Air Force, JAPCC

### Introduction

On the modern battlefield, military forces face a complex environment where success depends on controlling geographic domains such as land, air, sea, and space while exploiting non-physical operational areas like cyberspace, the electromagnetic spectrum (EMS), and information operations (IO). As multi-domain integration advances, cyberspace and electronic warfare have become closely linked, and the fusing of the two operational areas is now commonly called Cyber-Electromagnetic Activities, or CEMA. CEMA is 'the synchronization and coordination of cyber and electromagnetic activities to deliver operational advantage, thereby enabling freedom of movement while simultaneously denying and degrading adversaries' use of the same.[1] Military leaders must be knowledgeable of CEMA and implement CEMA at all levels – strategic, operational, and tactical – to achieve success on the battlefield.

A recent exercise in March 2023 at Schofield Barracks, Hawaii, exemplifies this new operational reality. During an Operational Readiness Assessment, soldiers from the US Army's recently activated 11th Cyber Battalion demonstrated cutting-edge CEMA tactics. Operating under the 780th Military Intelligence Brigade and Army Cyber Command, the battalion delivered close-range cyber effects using radio-frequency (RF) weapons, electronic warfare (EW), and IO Tactics, Techniques, and Procedures (TTP).

During the exercise, the cyber battalion, comprised of four companies with over 300 personnel, divided into five Expeditionary CEMA Teams (ECTs) and demonstrated proficiency in using air- and ground-launched drones, stand-in jammers, and other cyber and EW tools to achieve effects against enemy positions. They gained access to enemy networks and communications, including tactical surface-to-air missile (SAM) systems, which were then infiltrated and disrupted using non-kinetic effects. This event marks a significant step forward in the Army's approach to integrating CEMA with traditional warfare tactics, and emphasises the importance of close-range, decentralized CEMA operations in future combat scenarios.[2]

## Origins of CEMA (2009 to Present)

The US Army formally introduced CEMA in 2009 as an organizational initiative to improve the planning and coordination of non-kinetic operations. By 2011, CEMA was incorporated into several Army Field Manuals, and by 2015, experimental units such as the CEMA Support for Corps and Below (CSCB) and the 915th Cyber Warfare Battalion were established.[3] In October 2022, the 11th Cyber Battalion was activated to further enhance the Army's ability to conduct defensive and offensive cyber operations, reflecting a continued commitment to advancing CEMA TTPs. These units were designed to improve the integration of battlefield cyber and EW capabilities.

The US Department of Defense (DOD) has long understood the importance of cyberspace and the EMS for the armed forces. Field Manual 3-38, published in 2014, provides the necessary information for the armed forces to conduct CEMA and model the operational environment. FM 3-38 was superseded in April 2017 with FM 3-12, titled 'Cyberspace and Electronic Warfare Operations'. This updated manual outlines tactics and procedures to enhance the coordination and integration of Army cyberspace and electronic warfare operations to support unified land and joint military operations.

## NATO's Role in CEMA Initiatives

Alongside the USA, NATO has integrated CEMA into its operational framework. NATO has been vigilant in the cyber domain since at least 2007, following an eye-opening cyber attack on Estonia that targeted government, financial, and media systems, leading NATO to outline its first Cyber Defence Policy in 2008. The 2010 NATO Summit in Lisbon acknowledged that cyber attacks could threaten Euro-Atlantic security, and in 2011, NATO codified its cyber defence policy. 2012 marked another milestone when the NATO Defence Planning Process (NDPP) first integrated cyber defence. In 2016, NATO declared cyberspace a domain of operations and executed a Cyber Defence Pledge. NATO has also established critical centres such as the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in 2018 in Estonia, which offers training and research to bolster cyber capabilities, the Joint Electronic Warfare Core Staff (JEWCS), which provides advanced EW training and equipment, and the Virtual Cyber Incident Support Capability in 2023. In 2024, NATO took a significant step forward by inaugurating the Integrated Cyber Defence Centre to centralize and enhance its cyber defence efforts. This centre fosters collaboration among Allies, streamlining threat detection and response and developing advanced cyber tools and techniques. These milestones reflect NATO's sustained commitment to evolving its cyber capabilities in response to emerging threats.[4]

To further promote CEMA, NATO collaborates with member nations to align strategies and integrate technologies that enhance military advantage. The UK set up its Land Cyber Electromagnetic Activity Programme in July 2020, which delivers defensive

| Year | Event/Milestone |
|---|---|
| 2007 | Russian hackers launched a cyber attack on Estonia, targeting government, financial, and media systems, highlighting cyber vulnerabilities. |
| 2008 | NATO outlines its first Cyber Defence Policy. |
| 2010 | Lisbon Summit acknowledges cyber attacks as a threat to Euro-Atlantic security. |
| 2011 | NATO formalizes its cyber defence policy. |
| 2012 | The NATO Defence Planning Process (NDPP) first integrates cyber defence. |
| 2016 | NATO declares cyberspace a domain of operations and enacts the Cyber Defence Pledge. |
| 2018 | NATO establishes the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estonia for training and research. |
| 2023 | NATO creates the Virtual Cyber Incident Support Capability to improve response to cyber incidents. |
| 2024 | NATO inaugurates the Integrated Cyber Defence Centre to centralize and enhance cyber defence efforts. |

*A brief overview of various cyber-related events pertaining to the Alliance.*

and offensive cyber and electromagnetic activity, electronic countermeasures, and EW and signals intelligence capabilities while integrating people within these CEMA capabilities.[5] Additionally, NATO conducts integrated exercises such as 'Cyber Coalition', held annually since 2008, which brings together NATO Allies and Partners to strengthen the Alliance's ability to deter, defend, and counter threats in and through cyberspace.[6] However, while NATO has been hard at work promoting CEMA within the Alliance, the case studies below highlight the rapid changes and advancements occurring globally in this critical domain.

## Case Study 1: Recent Crisis Between Israel and Hezbollah

The conflict between Israel and Hezbollah demonstrates the advanced integration of CEMA in modern hybrid warfare. Israel coordinated cyber attacks and electronic jamming to disrupt Hezbollah's radar and communication networks, creating tactical advantages for precision airstrikes. Leveraging AI-driven data analytics, Israel merged cyber intelligence and EMS surveillance to enable real-time decision-making, enhancing operational effectiveness. Additionally, Israeli Unmanned Aerial Vehicles (UAV) utilized secure communication links and frequency-hopping technologies to evade jamming attempts while conducting surveillance and delivering electronic payloads. A recent operation against Hezbollah in Lebanon involved Israel's secretive 'Unit 8200' which embedded explosives in 5,000 pagers, killing 12 and injuring thousands of operatives.[7]

Meanwhile, since its founding in 1982, Hezbollah has served as a critical tool for Iran to project power beyond traditional military means, especially in asymmetric and hybrid warfare. Hezbollah's cyber arm, acting as an extension of Iran's Revolutionary Guard Corps (IRGC), has evolved into a significant force capable of conducting information warfare campaigns. Platforms, such as Hezbollah's Al-Manar TV, amplify anti-Western and anti-Israeli narratives, while Hezbollah's cyber operations target adversaries and spread disinformation such as exaggerated casualty reports of Israeli forces designed to undermine


*US Army soldiers coordinate cyber and electronic warfare strategies during a field exercise, showcasing the critical role of integrated CEMA teams in modern combat operations.*

Israel's public confidence. The 2006 Lebanon War between Hezbollah and Israel marked a turning point, highlighting Hezbollah's success in psychological warfare and media manipulation. During this conflict, Hezbollah's information campaigns helped it secure symbolic victories, using platforms like Al-Manar to portray itself as a regional resistance leader. Iran's investment in cyber capabilities, particularly after the Stuxnet attack on its nuclear programme in 2010, accelerated Hezbollah's cyber development.

Between 2013 and 2015, Iranian cybersecurity spending increased significantly, leading to the creation of Hezbollah's Cyber Army (HCA). The HCA conducts cyberespionage, sabotage, and disinformation campaigns, with operations such as the *Volatile Cedar* campaign targeting Israeli and Western networks to undermine trust in the targeted institutions, degrade operational capabilities, and amplify psychological pressure on adversaries. By integrating local networks and expertise, Iran and Hezbollah jointly conduct cyber-influence operations, from disinformation campaigns to training regional proxies, demonstrating how nonstate actors can wield substantial soft power with state support. Their efforts included disrupting GPS signals, hacking civilian infrastructure, and spreading disinformation to create public anxiety.[8] Overall, Hezbollah employed cyber intrusions and EMS spoofing to undermine Israeli security and amplify psychological operations.

Both Israel and Hezbollah integrated CEMA to maximize tactical and strategic outcomes, with Israel achieving aerial and operational superiority and Hezbollah focusing on asymmetrical disruption. This conflict highlights the increasing importance of integrating cyber and EMS capabilities in warfare, where technology shapes battlefield dynamics and influences civilian perceptions and the psychological dimensions of conflict.

## Case Study 2: CEMA in the Russia-Ukraine Conflict

Russia has long embraced asymmetric warfare; its military doctrine prioritizes the initial preparation stages of a conflict, leveraging non-kinetic and asymmetric


*A soldier supports CEMA operations, utilizing electronic warfare systems for signal interception, jamming, and battlefield communication dominance*

capabilities to achieve early tactical advantages over its opponents.[9] This includes CEMA operations, as observed in the 2008 Georgia conflict and the 2014 annexation of Crimea, where cyber attacks and electronic jamming were employed to disrupt communications.

Additionally, Russia has made significant breakthroughs in CEMA in their ongoing war in Ukraine. At the onset of the conflict, a cyber attack attributed to Russian hackers targeted Viasat, a communications provider used by Ukrainian forces, disrupting command and control systems across Ukraine, creating difficulty for Ukraine's defence. Russia disrupts battlefield coordination, delays decision-making, and degrades Ukraine's ability to direct forces in real-time by targeting Ukraine's command and control (C2) systems through cyber attacks and EW. Furthermore, Russian artillery can exploit gaps, striking with greater precision the Ukrainian units. For instance, jamming communications and GPS signals hampers real-time targeting data, making it harder for Ukrainian units to direct counter-battery fire or reposition effectively. Despite initially lagging their Ukrainian target, Russian forces have demonstrated high integration between cyber capabilities and physical operations, particularly leveraging UAVs for real-time surveillance, identifying enemy positions and providing data to their artillery. By combining drone reconnaissance with cyber attacks, Russian units have improved their ability to strike targets quickly and accurately, reducing the time between detection and engagement. In one case, Russian forces reportedly employed advanced GPS jamming techniques in Donbas, disrupting Ukrainian drone operations and communications-impacting Ukraine's situational awareness and coordination.[10]

Close-range jammers, such as the Russian Krasukha-4 systems, designed to neutralize airborne electronics, have become a crucial asset in the Russian military's operations in Ukraine. This includes ground-based jamming of UAVs, radar-guided missiles, and other radar-dependent airborne platforms. These jammers have substantially degraded platforms like the M777 Howitzer's models, such as the Bayraktar TB2, resulting in missed targets and reduced strike effectiveness.[11]

Significant CEMA innovations have also been made on the Ukrainian side, where Ukraine has adapted to


*A US Army Soldier from the Expeditionary Firing Crew, Alpha Company, 11th Cyber Battalion, conducts field operations.*

its opponent by deploying agile, small-scale drones capable of conducting electronic reconnaissance and precision strikes. Ukrainian forces have also excelled in integrating commercial off-the-shelf technology into their operations. For instance, Ukraine's Sky Fortress systems uses smartphones to create mesh networks for audio drone detection, which exemplifies the effective repurposing of consumer technology for defence use. Additionally, Ukraine has utilized commercially available drones equipped with jamming modules to counter Russian UAV and disrupt Russian communications.[12] Similarly, the adoption of Starlink has provided resilient communication capabilities critical for command, control, and coordination, especially in regions with compromised infrastructure. Lastly, adaptations to electronic warfare and deployment of fibre-optics-guided drones resistant to radio frequency jamming highlight the dynamic response to contested electromagnetic environments.

## Case Study 3: China's CEMA Development

China's CEMA strategy focuses on *'systems confrontation'* and *'systems destruction warfare'*. This involves coordinating kinetic and non-kinetic operations to degrade an adversary's communication and information systems. China leverages cyberspace and the EMS to disrupt and fragment adversaries' system-of-systems, aiming to gain informational and decision-making superiority. The People's Liberation Army (PLA) views CEMA as essential to integrating and enabling kinetic operations in physical domains while also serving as a key platform for influence operations within the broader scope of information warfare. Central to this approach is China's 'integrated network electronic warfare' strategy, which combines cyber attacks, EW, and precision kinetic strikes on critical nodes within the command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) networks.[13]

The PLA plays a key role in cyber espionage, exemplified by campaigns like Advanced Persistent Threat (APT) 10, which has targeted multinational corporations and government entities to steal intellectual property and sensitive data, providing strategic and technological advantages to China.[14] Additionally, through offensive cyber operations (OCO), the PLA breached the US Office of Personnel Management (OPM) in 2015, compromising the personal data of millions of federal employees, enabling potential exploitation and psychological operations.[15] Both efforts highlight China's integrated approach to leveraging cyber capabilities for strategic gain and to disrup adversaries.

## Recommendations

NATO must modernize frameworks to increase its CEMA capabilities in the evolving operational environment. Advancements in simulation technologies, realistic testing environments, and updated doctrinal guidance must be incorporated by NATO. These initiatives must align with the rapid technological evolution and the complexities of contemporary warfare, ensuring that military personnel remain proficient and adaptable.

A critical component of this strategy involves enhancing simulation platforms and the integrating artificial intelligence (AI) and machine learning tools. Existing systems, such as One Semi-Automated Force (OneSAF), should be upgraded to include dynamic Electronic Targeting Folders (ETFs), real-time adversary network modelling, and simulations replicating modern intelligence-gathering environments, including social media and network mapping. Incorporating AI-driven tools can simulate adaptive adversarial behaviours, increasing the realism and rigour of training exercises. Furthermore, interactive decision-making tools can improve operators' ability to perform under time-sensitive conditions, fostering effective decision-making in high-pressure scenarios.

Realistic testing and training environments are urgently needed to complement advancements in simulation. Establishing dedicated physical and/or virtual CEMA ranges for NATO and Allied forces is essential. These ranges should replicate modern EW and cyber operational systems, allowing personnel to test offensive and defensive capabilities under realistic conditions. These ranges can facilitate comprehensive assessments of force readiness while uncovering gaps in interoperability and capability.

Military doctrine and TTPs must be updated frequently to reflect emerging technologies and lessons learned from current conflicts, such as the one in Ukraine. The rapid evolution of technology necessitates an agile approach to doctrinal and procedural development, with accelerated revision cycles to ensure alignment with contemporary threats and opportunities. Furthermore, a sustained emphasis on interoperability is essential for synchronizing across joint and Allied forces during multinational operations. Interoperability should extend beyond technical compatibility to include procedural and operational coherence, ensuring seamless collaboration in complex operational environments.

Collaboration with private industry, academic institutions, and research organizations is another vital element of CEMA capability development. Such partnerships can provide access to cutting-edge innovations, enhance training methodologies, and enable military organizations to stay at the forefront of technological advancements. Insights from real-world conflicts, such as integrating cyber and electromagnetic tactics observed in Ukraine, should inform training and capability development efforts. By leveraging these partnerships and lessons learned, military organizations can remain agile and adaptive in the face of evolving threats.

Enhancing CEMA capabilities requires a holistic approach prioritizing upgraded training, realistic testing environments, agile doctrinal development, and collaborative partnerships. By integrating advanced simulation technologies, establishing CEMA testing ranges, and fostering joint interoperability, militaries can prepare their forces to navigate the dynamic challenges of modern warfare. These efforts must be underpinned by continuous investment in

personnel proficiency, leveraging innovative tools and iterative learning processes to maximize the strategic potential of CEMA.[16]

## Conclusion

As the modern battlefield advances, military forces must evolve by mastering physical and non-physical domains. The CEMA concept underscores the need to synchronize cyber and electromagnetic operations with the physical domains to gain strategic and tactical advantages while simultaneously mitigating vulnerabilities. This integration demands technical and procedural interoperability among various forces and agencies to ensure seamless information exchange and coordination. By implementing the recommendations in this paper, NATO can secure its collective defence across the full spectrum of modern warfare. ●


1. Joint Doctrine Note 1/18 (2018), Joint Doctrine Note 1/18 Cyber and Electromagnetic Activities, UK: MoD.
2. Dvids (2023), Soldiers innovating technology, refining tactical concepts, and strengthening partnerships.
3. Soesanto, S., (2021), 'A digital Army: Synergies on the Battlefield and the Development of Cyber-Electromagnetic Activities (CEMA)'.
4. NATO (2024), Cyber Defence.
5. MoD Gov. UK. (2021), Land Cyber Electromagnetic Activity (CEMA) Programme.
6. NATO ACT (2023), Cyber Coalition: NATO's Flagship Cyber Exercise.
7. Saul, J., Scheer, S., Rabinovitch, A., (2024). 'Hezbollah pager attack puts spotlight on Israel's cyber warfare Unit 8200', Reuters.
8. Pahlavi, P., (2022), 'Digital Hezbollah and Political Warfare in Cyberspace', The National Interest.
9. Bowen, A., (2020), Russian Armed Forces: Military Doctrine and Strategy.
10. Waterman, S., (2024). 'Russian Jamming Is Wreaking Havoc on GPS in Eastern Europe. But Is It Hybrid Warfare?', Air & Space Forces Magazine.
11. Global Defence News, (2024), Analysis: How Russia's Krasukha Electronic Warfare System Disrupts UAVs and Radars in Ukraine.
12. Australian Army Research Centre, (2024), Drones in Modern Warfare: Lessons Learnt from the War in Ukraine.
13. Black, J., & Lynch, A, (2020), 'Cyber Threats to NATO from a Multi-Domain Perspective'. In Cyber Threats and NATO 2030: Horizon Scanning and Analysis. NATO CCDCOE.
14. West, F., (2017), 'Warning: Hacking Group Based in China Targeting UK Business Data'.
15. The Wall Street Journal, (2015), 'U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say'.
16. Schneider, L., Jerald, A., Chick, N., Anderson, C., Mittal, V., Boyce, M., (2021), 'Identifying Simulation Requirements to Support CEMA Training'. United States Military Academy Departments of Systems Engineering and Army Cyber Institute.


ABOUT THE AUTHOR


**Lieutenant Colonel Athanasios Sdrakas**

GRC Air Force, JAPCC


Lieutenant Colonel Athanasios Sdrakas graduated from the Hellenic Air Force Academy with a Bachelor of Science in Aeronautics in 2000. He holds two Master of Science degrees: one in International Affairs from the University of Nicosia, Cyprus, and another in Environmental, Disaster, and Crises Management Strategies from the National and Kapodistrian University of Athens. He began his service in the 348 Tactical Reconnaissance Squadron as a fighter pilot from 2000 to 2009, accumulating over 1,000 flying hours on the RF-4E aircraft. Subsequently, he was an instructor pilot in the 364 Air Training Squadron from 2009 to 2022, accumulating nearly 3,000 flying hours on the T-6A aircraft and serving as a squadron commander. He graduated from the Fighter Weapons School and the Supreme Joint War College. Lieutenant Colonel Sdrakas is the Subject Matter Expert in Electronic Warfare (EW), including Suppression of Enemy Air Defence (SEAD) Operations at the JAPCC.