Cyber and Electromagnetic Activities (CEMA) in a Multi-domain Battlefield

Juha Kai Mattila
Aalto University, Helsinki, Finland

juhakaimattila24@gmail.com

Abstract: Contemporary adversaries aim to integrate lines of operations across information, cyber, electromagnetic, and kinetic domains. They take advantage of the digitalisation of the information realm, which opens avenues to deliver impact at the cognitive and social levels. Simultaneously, the demand for mobility and dispersion on the battlefield multiplies the need for transceivers and wireless communication. Naturally, this increases the targets for electronic attacks; for example, battlespace transceivers open new avenues for breaching isolated cyber domains. The military is gradually generating cyber and electromagnetic abilities into its capability portfolio, but often lacks appreciation for their combined impact on a modern multi-domain battlefield. Therefore, the paper uses design science methods to develop a model of CyberElectromagnetic Activities (CEMA) and Enterprise Architecture (EA) views, illustrating them in the context of a modern multi-domain battlefield. First, the paper aims to define modern CyberElectromagnetic battlespace and to derive its tenets from real-world cases. Secondly, the paper elaborates on the combined CEMA in the context of multidomain operations. Thirdly, the paper designs a CEMA model and illustrates it using views typical of enterprise architecture. Finally, the paper tests the feasibility of the abducted model with operational scenarios. The CEMA model is intended for Cyber and EW operational planners and orchestrators as a foundation for CEMA operations. The findings of this research provide insights and explanations to planners and researchers of operational art that: CEMA is always a part of multi-domain operations because of its omnipresence CEMA, being a composition of many abilities, needs collaborative planning and orchestration of execution, both in defensive and offensive operations Interrelationships among CEMA, information operations, and kinetic operations need to be understood to assess the combined system-of-systems impact, Asymmetric operational thinking opens a spectrum of means and ways to effect in a multidomain battlefield, Rapidly evolving technology opens both vulnerabilities and avenues of effect for defensive and offensive operations, and Advanced digital force will dominate a force with commercial or dual-use technologies in modern multi-domain operations.

Keywords: Cyber operations, Electronic warfare, CEMA, Multi-domain operations, Design sciences

1. Introduction

Contemporary adversaries aim to integrate lines of operations across the information, cyber, electromagnetic, and kinetic domains, as illustrated in Figure 1 (Mattila, Cyber Defence is more than Cybersecurity, 2025). They take advantage of the digitalisation of the information realm, which opens avenues into the cognitive and social realms. It becomes more cost-efficient to attack through the cyber domain, launch terrorising strikes, and create confusion and fear in these realms. (Clarke & Knake, 2020) Domain, in this context, refers to a dimension of the military theatre's area of operation.

Besides the expanding cyber environment (environment refers to a man-made digital infrastructure), the demand for mobility and dispersion on the battlefield increases the need for transceivers and wireless communication. Naturally, this increases the targets for electronic attacks, for example, suppressing the GPS signal increases the circular error probability. (Soren, 2025) Moreover, battlespace transceivers open new avenues for breaching logically isolated cyber domains. (Álvarez, 2025)

A kinetic line of operation may use the electromagnetic and cyber realms to multiply the system's effects, e.g., an adversary may destroy a central control hub with a gliding air-to-ground payload and simultaneously overload defender sensors with decoy targets while suppressing communications. (Gunn, 2025) The combined course of action (CoA) will suppress the surveillance system, prevent its repair, and make the adversary lose trust in any similar C5ISTAR[1] support system during that conflict. (Popli, 2025)

[1] C5ISTAR = Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, Target Acquisition and Reconnaissance support system of systems

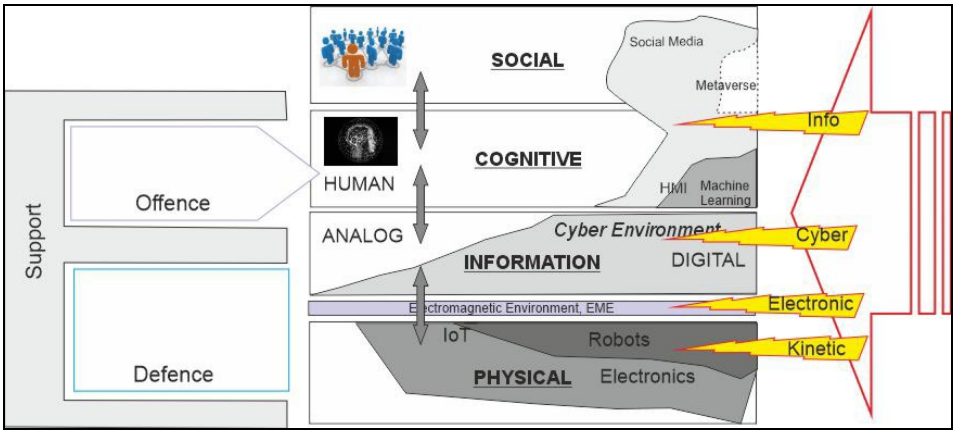

Figure 1: A View to Evolving Realms of Military Force Projection

A combination of operations on cyberspace and the electromagnetic spectrum is called Cyber and Electromagnetic Activities (CEMA) in the US Army (US Army, 2014) and the UK MoD (UK MoD, 2018). In the NATO multidomain operations model, the cyber domain fosters the electromagnetic spectrum (NATO, 2025), and missions planned in synchrony produce convergent effects within the System of Systems defence or offence. (Libicki, 2021) Hence, the definition in this paper states that CEMA are coordinated offensive or defensive courses of action that either improve BLUE's freedom of movement and survivability or degrade RED's use of the electromagnetic and cyber environment.

Since the CEMA environment predominantly comprises hardware nodes, transceivers that utilise electromagnetic propagation, and software-defined features that define cyberspace, it offers greater advantages as forces intensify their digitalisation and mobility. Therefore, the Western type of military force (4th-or 5th-generation) is more vulnerable to CEMA effects than a 3rd-generation industrial force optimised for attrition through kinetic effects. (Lind, 2004) (Abbot, 2010) On the other hand, when any force adopts dual-use consumer electronics, it may open unrecognised vulnerabilities to CEMA attacks. The rapid evolution of dual-use electronics during the Russia-Ukraine war proves this. Russia is enhancing its electronic warfare (EW) development and updating its existing equipment to counter Ukraine's rapidly evolving capabilities (Bronk, 2025).

Militaries worldwide are increasingly interested in the CEMA domain (Greenert, 2013), either to address vulnerabilities in their digital transformations or to create asymmetric, yet systems-level, effects against more digitised adversaries. The military is gradually generating cyber and electromagnetic abilities into its capability portfolio, but often lacks appreciation for their combined impact on a modern multi-domain battlefield. The paper develops a CEMA model for Cyber and EW operational planners and orchestrators, serving as a foundation for CEMA operations.

2. Illustrate CyberElectromagnetic Battlespace and Describe its Tenets

The Cyber and Electromagnetic environment continues to expand within military forces as they modernise and digitise their platforms, connecting them to a system-of-systems (SoS) of capabilities. (Dahmann, 2012) These systems of systems extend cyberspace and utilise the electromagnetic environment to support military affairs. The defenders' interest is to protect the BLUE system of systems and prevent the systemic effects (Beagle, 2001) of the Attackers (RED) that intend to suppress essential BLUE capabilities. The following literature review approaches the CEMA tenets from the perspectives of cyberspace, the electromagnetic spectrum, and a combined viewpoint. Finally, a technical system-of-systems model is developed to improve understanding of the CEMA system-of-systems in a confrontation.

2.1 Software-defined Cyberspace

As software-defined features replace mechanical functions, the amount of software code explodes. Unfortunately, the industry average for coding errors remains 15-50 defects per 1000 lines of code, and at best, the quality may reach 0.1 defects per 1000 lines. (McDonnell, 2004) The exponential growth of software code in armament, the integration of system-of-systems, and the rise of big data together increase the area of vulnerability within the technical layer of SoS.

Example: More than 30,000 public and private organisations were exposed to the SolarWinds hack between 2019 and 2020. Apparently, a Russian agent injected malicious code into SolarWinds Orion management software. When customers updated their management software, the malicious code created backdoors that hackers could use to access data. (Oladimeiji & Kerner, 2023)

On the other hand, the Armed Forces' evolving digital transformation requires competent military personnel to manage and leverage software-defined capabilities and processes. Otherwise, the growing number of people interacting with machines will provide lucrative avenues for attack. (Entrust Network, 2022)

Example: The Russian Ministry of Internal Affairs is advising residents and soldiers in areas near or within Ukrainian Forces' control not to use social media, dating apps, geotagging, geolocation links, or unsecured messaging applications. (Linder, 2024)

Software-defined, data-driven cyberspace is both more vulnerable and offers strategic advantages to the military. Hence, Information technology security, Cybersecurity, and Cyber defence operations are more critical as the military's digital transformation advances. (Whyte & Mazanex, 2023)

Example: Outdated technologies in enclaves expose the military to strategic vulnerability. An unpatched operating system in a fleet of main battle tanks may become a lucrative way to suppress the entire armoured capability. (Military Dispatches, 2024)

2.2 Electromagnetic Spectrum

Propagation in EME depends mainly on frequency, effective radiated power (ERP), antenna radiation patterns, atmospheric attenuation, and diffusion caused by elements along the propagation paths. This means that a significant concern in EME is the distance between the transmitter and receiver/reflector. Hence, both Electronic Support (ES) and Electronic Attack (EA) sensors and effectors need to be networked to select optimally located EW sites for intercepting or jamming. (Clark, Walton, Tourangeau, & Tourangeau, 2021) Any EW system, therefore, has cyberspace and needs to be protected against adversary electromagnetic and cyber effects.

Example: Ukrainian forces are combining electronic attacks, attack drones, and advancing infantry to penetrate behind Russian lines and create confusion. First, Russian surveillance drones are jammed, then, attacking drones strike both aerial and ground targets, and finally, infantry advance and seize crucial ground points. (Álvarez, 2025)

As the vulnerability of any radiating site increases, the need is to distribute, for example, surveillance radars and create low-size, weight, and power (SWaP) radar networks (Knight, 2025). While improving system resilience, the distributed architecture also provides broader coverage, especially in complex terrain. With a distributed, more disposable radar architecture, the cognitive electronic warfare (CEW) attributes will enhance both offensive and defensive capabilities. (Vernhes, 2025)

Example: Artificial intelligence-driven electronic protection (EP) can adapt in real time to conventional radar configurations and avoid detection. (Knight, 2025)

2.3 Combined Cyber and Electromagnetic Domain from a C5ISTAR System of Systems Viewpoint

Figure 2 presents a technical view of the CEMA environment. It is a snapshot from the viewpoint of a Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, Target Acquisition, and Reconnaissance system-of-systems. Figure 2 illustrates both vulnerabilities to attacks and defensive measures. Cyberspace can be used to attack transceivers, causing systemic disruption to communications services.

Example: Russians used a strain of wiper malware, 'AcidRain', to remotely erase vulnerable modems and routers of the Viasat service, disrupting Ukrainian access to broadband space communications for up to a week. (CyberPeace Institute, 2022)

Electromagnetic attacks can jam wireless transceivers and cause denial-of-service attacks in cyberspace.

Example: Russians are reportedly jamming GPS and other satellite-based navigation systems in the vicinity of the Baltic Sea as part of their hybrid operation to create fear of flying by degrading flight safety. (Waterman, 2024)

Cyberspace data flows can be captured by intercepting the GSM signal with a software-defined transceiver and analysing the data flow of ongoing sessions. (Louwers, 2024) By rerouting GSM traffic through compromised switches and exchanges, adversaries can capture mobile data flows.

> *Example: The Russian FSB operates communications interception devices (SORM) in telecommunications exchanges to collect and analyse traffic. (Soldatov, 2014)*

A hacker can take over a router in cyberspace by accessing it via a wireless interface, exploiting outdated firmware, and using the hijacked router as part of a Denial-of-Service (DoS) botnet to distort routing protocols or capture IP packets. (Rau, 2023)

> *Example: Russia's APT28 hacking group appears to have remotely breached the Wi-Fi of an espionage target by hijacking a laptop in another building across the street. (Greenberg, 2024)*

A defender may create an additional layer of air defence against incoming missiles, drones, and aircraft using cyber intelligence, electronic support measures, and electronic attack, in addition to conventional kinetic measures.

> *Example: During the 12-day war between Israel and Iran in 2025, Iran launched more than 1,000 drones at Israel. Israel created an additional layer of CyberElectromagnetic capabilities to intercept incoming airborne objects, achieving a success rate of up to 90%. (Frantzman, 2025)*

A model for a system of systems may be illustrated, as in Figure 2, with layers of physical, electromagnetic and logical. Physical platforms, facilities, and auxiliary systems host hardware capacity for processing and transmission. Electromagnetic performance transfers effective radiated power (ERP) to propagation in an electromagnetic environment (EME). Logical software and data-defined features and flows enable processes for military affairs. The technical illustration may scale to a socio-technical SoS involving users and administrators. (Mattila, Modelling Military as an Open, Socio-technical System, 2023) Furthermore, it may extend to enterprise-wide system networks that support the main military functions of Operate, Generate and Support. (DANSE, 2025) These systems-of-systems open new domains and attack vectors for adversaries to penetrate, exploit, and suppress defenders' capabilities. Cyber warfare can be thought of as techniques for creating effects or gaining intelligence on hostile systems through digital code. (Bronk, 2025) Electronic warfare can be thought of as techniques for creating effects or gathering intelligence on hostile systems through electromagnetic energy pulses. (Bronk, 2025)

The existing CEMA-related publicly accessible doctrines in the US (US Army, 2014) and the UK (UK MoD, 2018) do not cover, for example:

- How do CEMA-related abilities contribute to each other for tactical or operational impacts?
- How do CEMA-related abilities cluster in the military structure for force utilisation?
- How can CEMA courses of action be planned and executed against an adversary system-of-systems?
- How do CEMA-related abilities support both information and conventional operations in other domains?

The CEMA operational model aims to fill the gaps in understanding reflected in current CEMA-related doctrines and policies.

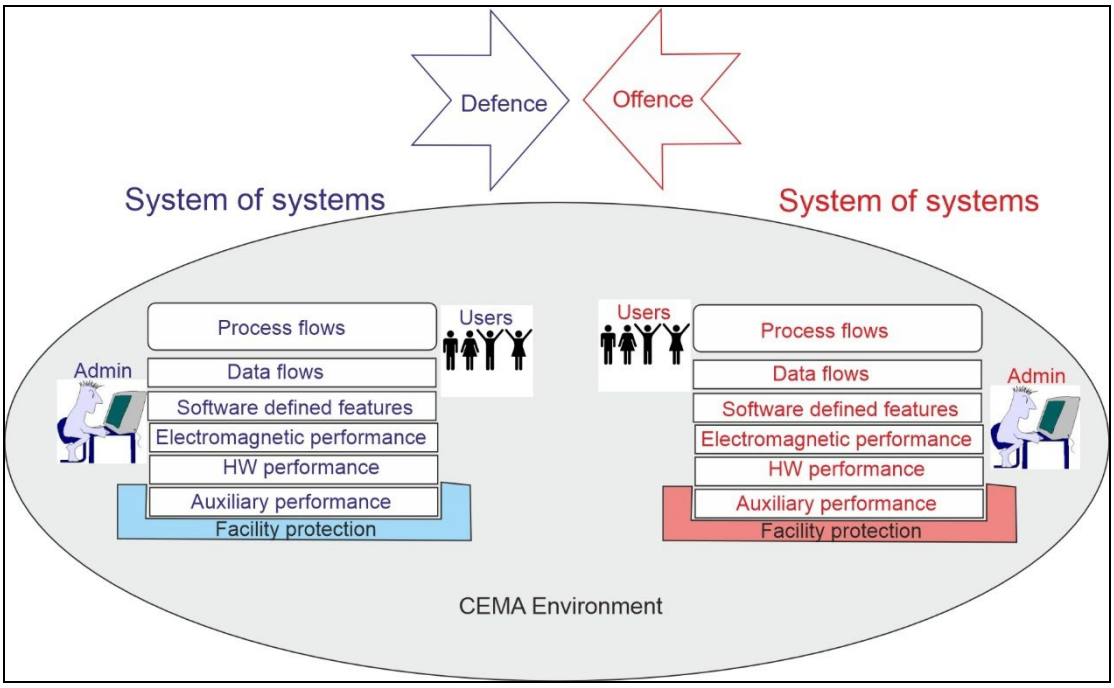

Figure 2: A System View of the CEMA Environment in Typical Forces Confrontation

3. CEMA in the Context of Multidomain Operations

Since the CEMA domain overlaps the cognitive and physical realms and encompasses most of the information realm, as illustrated in Figure 1, it provides an avenue to support both kinetic and information operations. Both Electronic and cyber-attacks can contribute to kinetic fires to achieve a joint systemic effect, as shown in Figure 3. The Russian Fancy Bear hacker group successfully infiltrated a Ukrainian artillery application used to control fires. Through the breach of 2014-2016, Russian artillery was able to locate both fire controllers and weapon sites on the Ukrainian side and destroy them more efficiently. (Crowdstrike, 2016)

Moreover, information operations benefit from Cyber or Electronic attacks that suppress official media sites or utilise hijacked cyberspace elements to disseminate influence messages. (Microsoft, 2023) Within the information realm, CEMA operations can also be employed independently as a covert arm, operating below the conventional threshold of war or providing an asymmetric advantage against modern forces (Russian Defence Policy, 2017). Russia has also used CEMA as part of a broader hybrid campaign to create terror, break the trust between the population and the government, and manipulate polarisation within a population. (NATO, 2024)

Since CEMA primarily focuses on the synchronisation and coordination of cyber and electromagnetic activities, the components and their combination in support of operations are more critical in various contexts. (UK MoD, 2018) The Electronic Warfare components are Electronic Attack, Electronic Support, and Electronic Protection, as shown in Figure 3.

- Electronic Attack (EA) broadly refers to the use of electromagnetic energy to degrade the performance of hostile systems for offensive purposes. It may independently contribute to kinetic, information, and CEMA operations.
- Electronic Support (ES or ESM) encompasses the exploitation of passively collected electromagnetic emissions to identify, track and possibly even target hostile systems. It directly supports EA, EP, and Network operations and provides essential awareness for force protection.
- Electronic Protection (EP or ECM) involves the use of electromagnetic energy by a platform to defend itself against enemy attacks, typically by degrading the signals received by enemy fire control radars, datalink connections, or missile seekers. (Bronk, 2025) EP support is used directly in kinetic operations, security, and survivability, but also contributes to Network operations and EA.

Cyberspace activities include network operations, cybersecurity, cyber defence, and cyber-attacks.

- Network operations (NO, NOC) encompass actions taken to design, build, configure, secure, operate, maintain, and sustain the C5ISTAR system of systems in a manner that ensures and preserves data

availability, integrity, confidentiality, as well as user and entity authentication and non-repudiation. (Senft, 2016) Network operations contribute directly to Cyber defence operations and also enable all military activities that use digital information. NO requires cybersecurity operations and other security measures to provide C5ISTAR support services.

- Cyber defence operations (CDO) utilise both passive and active cyberspace capabilities to protect data, networks, net-centric capabilities, and other designated C5ISTAR System-of-systems. (FM 3-21, 2021) CDO supports Information, CEMA and kinetic operations, ensuring the survivability of C5ISTAR services.
- Cyberattack operations (CAO) are conducted in cyberspace, aiming to create noticeable destructive effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial-of-service impacts in physical domains. (JP 3-12, 2018) CAO supports Information, CEMA, and kinetic operations, opening opportunities to achieve systemic effects within an adversary's system of systems.

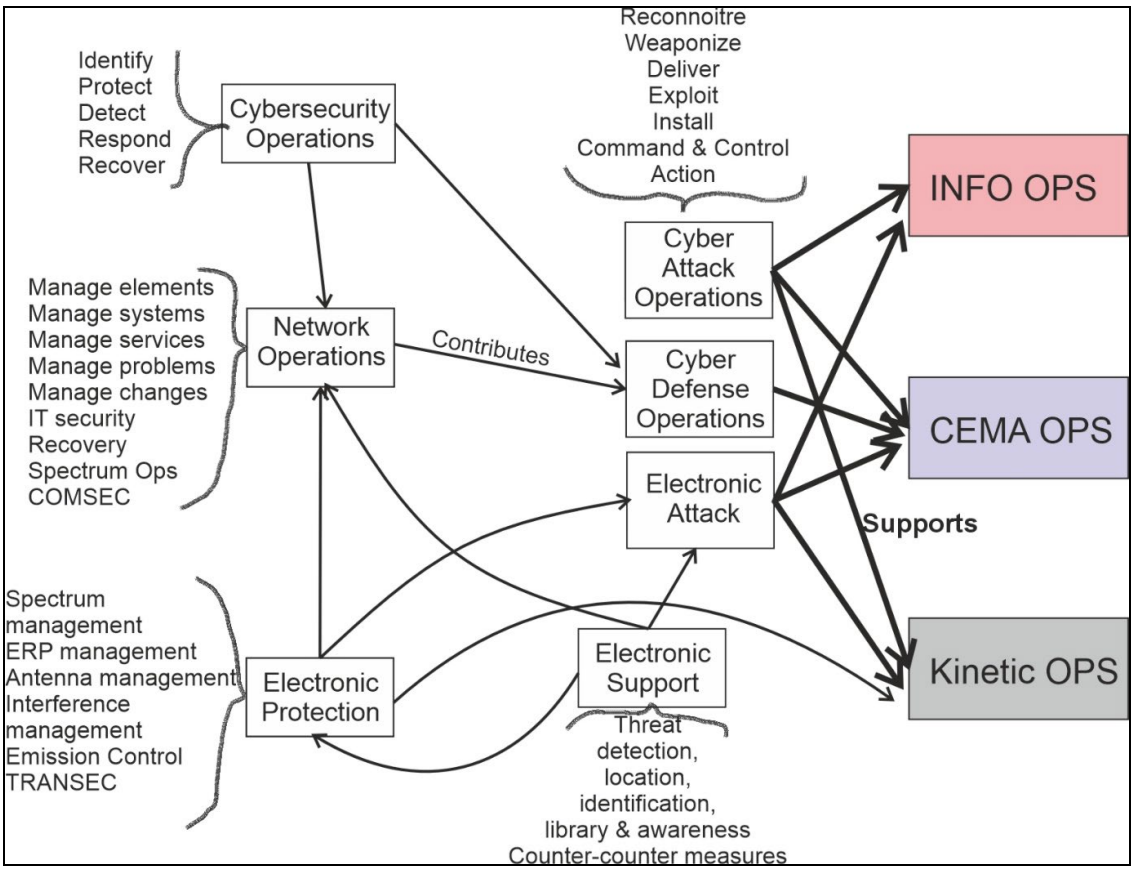

Figure 3: An operational view of the CEMA domain and its components, relationships, and architectural ontology

Understanding the interrelationships and dependencies within the CEMA in Figure 3 is crucial for effective operational planning and execution, given the complexity of both the targeting and effect. One instance of negligence renders the entire C5ISTAR system vulnerable to attacks. Naturally, this also applies to adversaries, hence, coordinated CEMA offensive activities, whether conducted alone or in support of other operations, may yield surprising victories.

4. Research Methodology

The research aims to develop a model and test its viability, the epistemological approach is knowing through making. Therefore, the research method follows the design science research process. (Gregor & Hevner, 2013) Firstly, the research recognises the problem, then surveys potential solutions, and thirdly, develops a solution. Finally, the feasibility testing of the created model follows the systems analysis methods (Mobus & Kalton, 2015). Feasibility testing uses two scenarios composed from the 2022 Russo-Ukraine war and the 2025 Israel-Iran war. The testing attributes are selected from the CEMA operational tenets of operational support, systemic impact, technology, dominance in the domain, and convergence.

5. Feasibility of the CEMA Model in Real-world Scenarios

The previous sections created the CEMA model from three viewpoints: 1. Environment and Confrontational in Figure 1, Systems view in Figure 2, and Operational view in Figure 3. This section tests the CEMA model's feasibility in two selected scenarios:

1. Scenario – Russian invasion of Ukraine 2022. The Ukrainian government and Microsoft identified 47 publicly attributed cyber incidents indicative of a campaign initiated by Russia between November 29, 2021, and May 9, 2022. Towards the end of the campaign, there was a 75 per cent increase in documented cyber intrusions—but a decline in the average severity of the attack. Only 29 per cent of the documented cyber incidents indicative of larger campaigns were degradations. Most Russian cyber operations were characterised by phishing attempts, distributed denial-of-service campaigns, propaganda or vandalism efforts, and single-network intrusions—all of which tend to have limited impact. (CSIS, 2023) Only the intrusion into the Viasat management system and the uploading of malicious software to the patching service, which then disseminated the malfunction to thousands of terminals in Ukraine and Europe, seem to have had a major impact. (CyberPeace Institute, 2022) Russian electronic warfare capabilities are countering precision-guided missiles and remotely controlled UAS. (Wattling & Reynolds, 2025)
2. Scenario – Iran-Israel 12-day war 2025 Iran-linked cyber actors execute a broad range of operations designed to exert psychological pressure, collect tactical intelligence, enforce deterrence against third countries, and maintain domestic control. Alongside disruptive cyberattacks, Iran intensified its psychological operations by using AI to generate and disseminate disinformation. Iranian operatives hijacked Israeli internet-connected closed-circuit television (CCTV) systems with the goal of exploiting them for real-time situational awareness, battle damage assessment, and adjustment of missile targets. (Khorrami, 2025) Iran intended to overwhelm Israel's Iron Dome air defence system with decoy drones and electronic attacks. (Croft, 2025)

Table 1: Testing the feasibility of the CEMA model against two selected scenarios

Attributes of the CEMA model	Scenario 1- Russian CEMA attack 2022	Scenario 2 – Iranian CEMA attack 2025
Support both Information, CEMA and kinetic operations	Ability to synchronise CAO as part of the main campaign. Ability to integrate EA with fires against airborne and ground targets.	Ability to integrate cyber and information operations for an influence campaign. Ability to integrate CAO and EA with missile and drone attacks.
Gaining a systemic impact using asymmetric means and ways	Ability to suppress Viasat terminals synchronised with air and ground forces attacks severed Ukrainian command and control functions.	Ability to retaliate against US air strikes with combined CAO and disinformation operations, creating impact in the US homeland.
Advantages or challenges of rapidly evolving technology	Russian cyber forces' ability to rely on only basic cyber-attack vectors while Ukraine builds up its coordinated cyber defence.	Iran's ability to use public CCTV networks in Israel for targeting and assessment.
Advanced digital force has dominance in the CEMA domain	Ukraine's ability to coordinate contributions from institutions, the IT Army, Cyber Troops, Technology companies, and coalition support for national cyber defence. (Kvartsiana, 2023)	The CEMA improved Iron Dome intercepted over 90% of incoming projectiles and drones.
CEMA integration for convergence and asymmetric impact	Russian tactical missions are mostly separate cyber and electronic attacks that may be synchronised under the campaign. No signs of operations in the CEMA domain.	Iranian CEMA efforts are coordinated through Information Operations and Missile/Drone Attacks. No signs of operations in the CEMA domain.

6. Conclusions

As militaries are gradually generating cyber and electromagnetic abilities as part of their capability portfolios, driven by lessons identified from the Russo-Ukrainian and Israel-Iranian wars, they often lack an appreciation of the combined cyber and electromagnetic impact on a modern multi-domain battlefield. The paper designs a model for CyberElectromagnetic Activities (CEMA) as part of the multi-domain operations in military

campaigns. The design illustrates the CEMA model from three viewpoints. An evolutionary view of the confrontation between two forces. A systems view of the opposing force system-of-systems. An operational view of the composition and value streams that contribute to CEMA operations. Following the methods of the design sciences, the paper tests the feasibility of the CEMA model in two recent scenarios.

The CEMA model proved its feasibility in two scenarios of the 2022 Russian invasion and the 2025 Israel-Iranian war in five tested features:

- Interrelationships between CEMA, information operations, and kinetic operations need to be understood for the combined system-of-systems impact. The CEMA is hard to identify in the Russo-Ukrainian war, as the parties are locked in tactical-level attrition and the fast evolution of UAS on the battlefield. On the contrary, the Israel-Iranian 12-day war was more operational in nature, and CEMA integration, both in influence operations and conventional missile strikes, followed the model.
- Asymmetric operational art opens a spectrum of means and ways for effect in a multidomain battlefield. Russian ability to take down Viasat connections synchronised with their invasion attack, and Iranian ability to counter US air strikes with influence operations in the US homeland, prove that CEMA provides major systemic impacts.
- Rapidly evolving technology opens both vulnerabilities and effects for defensive and offensive operations. Adversary digital infrastructure opens new avenues to support CEMA operations, as Iranians were able to fuse data from their ES sensors and hacked CCTV to assess the impact of missile/drone strikes in Israel, and Israeli's were using the Iranian GSM network to guide their UAS.
- Advanced digital force dominates force with commercial or dual-use technologies. Israel's CEMA-enhanced Iron Dome air defence system was able to intercept 90% of incoming ballistic or cruise missiles and drones during the 12-Day war.
- CEMA integration for convergence and asymmetric impact remains in its infancy. CEMA components are used as supporting roles for either information or conventional operations, rather than as a third line of operation. The evolution of technology or lessons identified alone does not provide sufficient leverage for transformation when existing military cultures and competencies oppose the change.

The designed CEMA model is intended to support military enterprise architects in creating multi-domain operational and systems views, military capability portfolio managers in anticipating the evolution of confrontation in military strategies, and Cyber and EW operational planners in preparing for future campaigns.

The CEMA model presented in this paper is still in its early concept. For maturity, it needs more scenario testing and simulation before it is translated into doctrine and utilised to generate military capabilities.

Ethics Declaration: This research did not require any ethical clearance.

AI Declaration: An AI tool (Grammarly) was used during the proofreading of this paper.

References

Abbot, D. H. (2010). *The Handbook of 5GW.* Nimble Books LLC.

Álvarez, S. (2025, April). *Electronic warfare: the silent battlefield of the future*. Retrieved from Oesia grupo: https://grupooesia.com/en/insight/electronic-warfare-the-silent-battlefield-of-the-future/

Beagle, T. (2001). *Effects-Based Targeting.* Maxwell AFB: Air University Press.

Bronk, J. (2025). *Airborne Electromagnetic Warfare in NATO: A Critical European Capability Gap.* London: RUSI.

Clark, B., Walton, T. A., Tourangeau, M., & Tourangeau, S. (2021). *The Invisible Battlefield: A Technology Strategy for US Electromagnetic Spectrum Superiority.* Washington DC: Hudson Institute.

Clarke, R. A., & Knake, R. K. (2020). *The fifth domain.* New York: Penguin Random House.

Croft, A. (2025). How has Iran managed to breach Israel's Iron Dome air defence system? *Independent*. Retrieved from https://www.independent.co.uk/news/world/middle-east/iron-dome-israel-iran-missiles-failing-tel-aviv-b2773584.html

Crowdstrike. (2016). *Use of FANCY BEAR android malware in tracking of Ukrainian field artillery units.* Crowdstrike.

CSIS. (2023). Cyber Operations during the Russo-Ukrainian War. *Center for strategic & international studies*. Retrieved from https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war#h2-russian-cyber-operations

CyberPeace Institute. (2022, June). *Case Study - Viasat*. Retrieved from CyberPeace Institute: https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat

Dahmann, J. S. (2012). *Systems of Systems Characterization and Types* . McLean: MITRE Corporation.

DANSE. (2025, March). *Designing for Adaptability and evolutioN in System of systems Engineering*. Retrieved from HiPEAC Network: https://www.hipeac.net/network/projects/6797/danse

Entrust Network. (2022, August). *Top 5 Ways End Users Compromise Security and Cause Data Breach*. Retrieved from Entrust Network: https://www.entrustnetwork.com/top-5-ways-end-users-compromise-security-and-cause-data-breach/

FM 3-21. (2021). *Cyberspace operations and electromagnetic warfare.* US Army FM 3-21.

Frantzman, S. J. (2025). New missile defenses, EW tactics aided Israel during 12-day Iran conflict. *Braking Defense*. Retrieved from https://breakingdefense.com/2025/07/new-missile-defenses-ew-tactics-aided-israel-during-12-day-iran-conflict/

Greenberg, A. (2024). Russian Spies Jumped From One Network to Another Via Wi-Fi in an Unprecedented Hack. *Wired*.

Greenert, J. (2013). Adm. Greenert: Wireless Cyberwar, The EM Spectrum, And The Changing Navy. *Braking Defense*. Retrieved from https://breakingdefense.com/2013/04/adm-greenert-wireless-cyber-em-spectrum-changing-navy/

Gunn, K. (2025). How Iran's air defense systems were defeated so quickly. *Task & Purpose*. Retrieved from https://taskandpurpose.com/news/iran-israel-air-defense-rising-lion/

JP 3-12. (2018). *Cyberspace operations.* Washington DC: US DoD Joint Publication 3-12.

Khorrami, N. (2025, August 4). *Digital frontlines: What the 12-day war revealed about the evolution of Iran's cyber strategy*. Retrieved from MIddle East Institute: https://mei.edu/publication/digital-frontlines-what-12-day-war-revealed-about-evolution-irans-cyber-strategy/

Knight, N. (2025, February). *The evolving battlefield: How radar technology is advancing in the age of advanced electronic warfare and C-UAS*. Retrieved from Military Embedded Systems: https://militaryembedded.com/radar-ew/rf-and-microwave/the-evolving-battlefield-how-radar-technology-is-advancing-in-the-age-of-advanced-electronic-warfare-and-c-uas

Kvartsiana, K. (2023). *Ukraine's Cyber Defense: Lessons in Resilience.* Berlin: George Marshall Fund.

Libicki, M. C. (2021). *Cyberspace in peace and war.* Annapolis: Naval Institute Press.

Lind, W. S. (2004). Understanding Fourth Generation War. *Antiwar*.

Linder, E. (2024). Russian government warns soldiers and residents of Ukrainian-threatened regions to avoid dating apps and social media. *ABC News*.

Louwers, J. (2024). GSM/5G basic radio signal interception. *Medium*. Retrieved from https://louwersj.medium.com/gsm-5g-basic-radio-signal-interception-1364ec7f395e

Mattila, J. K. (2023, August). *Modelling Military as an Open, Socio-technical System*. Retrieved from Thoughts about C4I systems: https://c4isys.blogspot.com/2023/08/modelling-military-as-open-socio.html

Mattila, J. K. (2025). Cyber Defence is more than Cybersecurity. *Proceedings of the 24th European Conference on Cyber Warfare and Security · Jun 27, 2025.* Kaiserslautern: ACI. Retrieved from https://papers.academic-conferences.org/index.php/eccws

McDonnell, S. (2004). *Code Complete, 2nd Edition.* Redmond: Microsoft Press.

Microsoft. (2023). *7 emerging hybrid warfare trends from Russia's cyber war.* Microsoft Threat Intelligence.

Military Dispatches. (2024). Cyber Vulnerabilities in Military Systems: A Critical Analysis. *Military Dispacthes*. Retrieved from https://militarydispatches.com/cyber-vulnerabilities-in-military-systems/

NATO. (2024, May). *Statement by the North Atlantic Council on recent Russian hybrid activities*. Retrieved from North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/official_texts_225230.htm

NATO. (2025). *Multi-Domain Operations*. Retrieved from NATO: https://www.act.nato.int/activities/multi-domain-operations/

Oladimeiji, S., & Kerner, S. M. (2023). SolarWinds hack explained: Everything you need to know. *TechTarget*. Retrieved from https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Popli, N. (2025). Air Supremacy Over Tehran Gives Israel a Decisive Edge—And Raises New Risks. *Time*. Retrieved from https://time.com/7294919/israel-air-supremacy-tehran-iran/

Rau, T. (2023). The 5 most dangerous Wi-Fi attacks, and how to fight them. *PCWorld*.

Russian Defense Policy. (2017, May). *Electronic Warfare Chief Interviewed*. Retrieved from Russian Defense Policy: https://russiandefpolicy.com/2017/05/30/electronic-warfare-chief-interviewed-2/

Senft, M. (2016, January). Convergence of Cyberspace Operations and Electronic Warfare Effects. *Research Gate*.

Soldatov, A. (2014, January). *Russia's communications interception practices (SORM).* Retrieved from Europarliament: https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/soldatov_presentation_/soldatov_presentation_en.pdf

Soren, M. (2025). The Precision Mirage: What Happens When GPS-Guided Weapons Meet Systematic Jamming. *Trajectory*. Retrieved from https://www.readtrajectory.com/the-precision-mirage-what-happens-when-gps-guided-weapons-meet-systematic-jamming/

UK MoD. (2018). *Cyber and Electromagnetic Activities.* London: UK MoD JDN 1/18.

US Army. (2014). *FM 3-38 Cyberelectromagnetic activities.* Washington: Department of the Army.

Vernhes, C. (2025, March). *AI and cognitive electronic warfare are shaping the future battlefield*. Retrieved from 59hardware: https://www.59hardware.net/en/ai-and-cognitive-electronic-warfare-are-shaping-the-future-battlefield/

Waterman, S. (2024). Russian Jamming Is Wreaking Havoc on GPS in Eastern Europe. But Is It Hybrid Warfare? *Air & Space Forces Magazine*.

Wattling, J., & Reynolds, N. (2025). *Tactical Developments During the third year of the Russo-Ukranian war.* London: RUSI.

Whyte, C., & Mazanex, B. M. (2023). *Understanding cyber warfare.* Abingdon: Routledge.