REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
10-05-2023	FINAL	N/A

4. TITLE AND SUBTITLE
Harnessing Chaos: Unleashing Electromagnetic Warfare for Enhanced Joint Operations

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Audrey Duke

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Writing & Teaching Excellence Center
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the curriculum. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT
Joint Force Commanders can utilize Electromagnetic Warfare (EW) in novel ways to establish conditions for an early and favorable outcome in conflict. By leveraging non-kinetic EW to disrupt, deny, degrade, and deceive adversarial systems, the United States can capitalize on opportunities from the created chaos in data flow and the Electromagnetic Spectrum (EMS) to enable joint operations. First, achieving and maintaining an advantage in modern warfare requires a range of non-kinetic EW solutions, which are more accessible and maintainable than kinetic solutions. Second, emerging threats require novel solutions that can target and overwhelm system vulnerabilities. Third, EW can significantly alter Military Deception (MILDEC) operations to enhance information operations and Joint All Domain Command and Control (JADC2). Superior MILDEC capabilities are vital for the joint force in modern warfare. Controlling the EMS and data are the key to winning the power competition, and EW will provide that control.

15. SUBJECT TERMS (Key words)
Electromagnetic Warfare; Electronic Warfare; Non-Kinetic Warfare; Emerging Threats; Countermeasures; JADC2; MILDEC; Military Deception

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Director, Writing Center
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	N/A		19b. TELEPHONE NUMBER *(include area code)* 401-841-6499

Standard Form 298 (Rev. 8-98)

Harnessing Chaos: Unleashing Electromagnetic Warfare for Enhanced Joint Operations

Date Submitted: 10 MAY 2023

Word Count: 3,615 words

INTRODUCTION

During this decisive decade of great power competition, emerging technologies are rapidly changing warfare. By leveraging Electromagnetic Warfare (EW) in novel ways, Joint Force Commanders can establish favorable conditions for meeting operational objectives. While the Department of Defense (DoD), Congress, and multiple administrations have focused in recent decades on developing emerging technologies, priority must also be placed on non-kinetic EW mechanisms. Emerging technologies, including artificial intelligence (AI), Lethal Autonomous Weapon Systems (LAWS), hypersonic weapons, Directed Energy (DE) systems, and quantum computing, all have one element in common; each relies on the Electromagnetic Spectrum (EMS), data and information to operate effectively. EW can disrupt data flow to these weapon systems and deceive their human-in-the-loop decision-makers. In the current environment, limitations in the defense industrial base, munitions manufacturing capabilities, and adversary numerical advantages further enforce the necessity to prioritize novel means of combatting emerging threats. Additionally, the United States and its allies are falling behind qualitatively and numerically in various force categories as adversaries are rapidly enhancing fleet and weapon system quantities and capabilities. For example, the DoD estimated in 2021 that China's fleet size had grown to over three hundred and fifty vessels, whereas the U.S. fleet remained under three hundred.[1]

Furthermore, the People's Republic of China (PRC) military advances have driven the DoD to pursue and prioritize complex, offensive systems while overlooking EW capabilities that

---

[1] Shelbourne, Mallory. "China Has World's Largest Navy with 355 Ships and Counting, says Pentagon." *USNI News*: 3 Nov. 2021, https://news.usni.org/2021/11/03/china-has-worlds-largest-navy-with-355-ships-and-counting-says-pentagon.

can exploit these systems.[2] By leveraging EW to disrupt, deny, degrade, and deceive adversarial systems, the United States can capitalize on opportunities from the created chaos in data flow and the EMS to enable joint operations. First, achieving and maintaining an advantage in modern warfare requires a range of EW solutions, which are more accessible and maintainable than kinetic solutions. Second, emerging threats require novel solutions that can target and overwhelm system vulnerabilities. Third, EW can significantly alter Military Deception (MILDEC) operations to enhance information operations and enable Joint All Domain Command and Control (JADC2). Superior MILDEC capabilities are vital for the joint force in modern warfare.

THE ELECTROMAGNETIC SPECTRUM AND WARFARE

Control of information has always been part of military operations, and the U.S. Strategic Command views information operations as a core military competency, with emphasis on the use of the EMS, cyber operations, and the use of psychological operations to manipulate an adversary's perceptions.[3] The DoD relies on the EMS for its Command and Control (C2) infrastructure, communications links, weapon systems, and supporting technologies. The EMS refers to the range of wavelengths or frequencies of electromagnetic radiation, and, as illustrated in Figure 1, it includes radio waves, microwaves, visible light, X-rays, and gamma rays.[4] Essential military systems rely on data for freedom of maneuver and action, and data travels

---

[2] Davidson, Philip. "STATEMENT OF ADMIRAL PHILIP S. DAVIDSON, U.S. NAVY COMMANDER, U.S. INDO-PACIFIC COMMAND BEFORE THE HOUSE ARMED SERVICES COMMITTEE ON U.S. INDO-PACIFIC COMMAND POSTURE." 10 March 2021, 7.

[3] Theohary, Catherine. "Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues." (Congressional Research Service, 17 March 2009) 2.

[4] Hoehn, John. "Overview of Department of Defense Use of the Electromagnetic Spectrum." (Congressional Research Service, 14 November 2022)1-3.

through the EMS. The Joint Publication for EMS Operations defines the spectrum as a maneuver space essential for facilitating control within the Operational Environment (OE) and one that impacts all portions of the OE and military operations.[5]

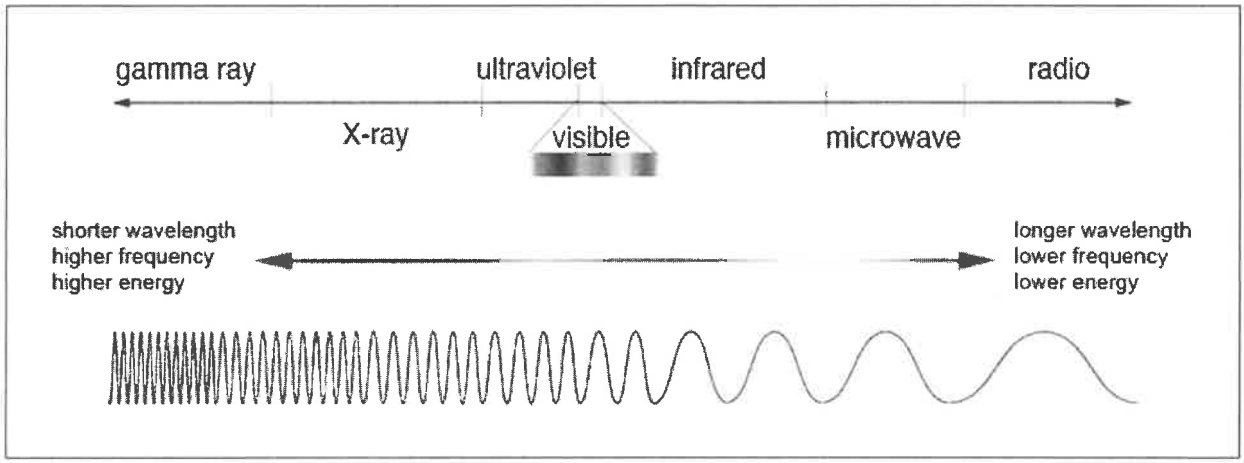

Figure 1. The Electromagnetic Spectrum[6]

A key solution for controlling the EMS is in the non-kinetic realm of EW. EW refers to using electronic means in the EMS to disrupt, deny, degrade, or deceive an adversary's information or communication systems without causing physical damage.[7] This type of warfare encompasses a range of techniques and tactics, including jamming, spoofing, Directed Energy (DE), Cyber Electronic Warfare (CEW), and electronic deception. Jamming is the deliberate radiation, reradiation, or reflection of EM energy to prevent or reduce an enemy's effective use of the EMS, intending to degrade the enemy's combat capability.[8] Spoofing involves transmitting false information to an adversary's sensors or communication systems, causing confusion and

---

[5] Joint Chiefs of Staff. *Joint Publication 3-85, Joint Electromagnetic Spectrum Operations*. 22 May 2020, PDF, 5. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf?ver=2020-04-09-140128-347.

[6] "The Electromagnetic Spectrum." National Aeronautics and Space Administration: Goddard Flight Center, March 2013. https://imagine.gsfc.nasa.gov/science/toolbox/emspectrum1.html.

[7] Joint Chiefs of Staff. *Joint Doctrine for Military Deception, Joint Pub 3-58*. 31 May 1996, I-5. https://irp.fas.org/doddir/dod/jp3_58.pdf. Online.

[8] Joint Chiefs of Staff. *Joint Publication 3-13.1, Electronic Warfare*. 25 Jan 2007, PDF, I-10.

potentially leading them to make incorrect decisions.[9] CEW merges cyberspace capabilities with traditional EW methods and involves infiltrating an adversary's computer or communication systems to steal or manipulate information and disrupt their operations.[10] Electronic deception involves using electronic means to mislead an adversary into believing something untrue. This can involve techniques such as creating false targets on radar screens, utilizing Electro-Optical (EO), Infrared (IR), or Radio Frequency (RF) countermeasures (CMs), and transmitting false signals to confuse an adversary's sensors. [11] EW is meant to exploit opportunities and vulnerabilities in the OE by leveraging the physics of EMS energy.[12]

In today's battlespace, achieving and maintaining an advantage in modern warfare requires a range of EW solutions. Non-kinetic EW technologies are more accessible and maintainable than kinetic measures. Although prioritization and funding for domestic manufacturing capabilities of propellants, energetics, and other components in munitions have increased with the past three administrations, the U.S. still relies heavily on other countries for munitions. Along with manufacturing capabilities, the U.S. also depends on international partners for natural resources in munitions. For example, the U.S. relies almost entirely on China

---

[9] Joint Chiefs of Staff. *Joint Publication 3-13.1, Electronic Warfare*, I-10.

[10] Nurgul Yasar, Fatih Mustafa Yasar, and Yucel Topcu "Operational Advantages of Using Cyber Electronic Warfare (CEW) in the Battlefield," Proc. SPIE 8408, Cyber Sensing 2012, 84080G (7 May 2012); https://doi.org/10.1117/12.919454.

[11] For additional information on electronic warfare, see *EW 101: A First Course in Electronic Warfare – 1st Edition*, by David Adamy.

[12] For additional information on EW mechanisms, including CMs, EM compatibility and deception; EM hardening, interference, and intrusion; electronic masking, probing, reconnaissance, and intelligence; electronics security; EW reprogramming; emission control; and spectrum management, see *Joint Publication 3-13.1, Electronic Warfare* by the Joint Chiefs of Staff.

— and, to a lesser extent, Russia — to procure antimony, a critical mineral in ammunition production.[13]

With kinetic solutions, wartime production and mobilization depend on the Defense Industrial Base (DIB). Progress has been made towards enhancing supply chains and increasing the domestic capacity to produce kinetic munitions, but it could be more than a decade before the DIB can meet sustainment requirements for war with a peer adversary.[14] For example, the war in Ukraine has triggered the U.S. to rev up the munitions industrial base to rebuild the domestic inventory to pre-conflict levels, but even with enhanced production rates, it is estimated to take over 6.5 to 12.5 years.[15] Simply put, the U.S. is not prepared to domestically maintain munition production for a prolonged conflict with a peer competitor.

While EW measures also rely on the DIB, commercial-off-the-shelf (COTS) components can be leveraged as part of the solution. Securing the supply chain and resourcing for the energetic materials in kinetic solutions is more complex than building up inventories of COTS components. Given the growth in capabilities and force quantities by peer adversaries over the past decade, most specifically the PRC, EW is necessary for balancing the force deposit. Utilizing low-cost COTS, non-kinetic EW solutions to saturate the operational environment will yield significant advantages. Plus, if a COTS EW solution is compromised or seized by the

---

[13] Harris, Bryant. "The US is Heavily Reliant on China and Russia for its Ammo Supply Chain." *DefenseNews*: 8 June 2022. https://www.defensenews.com/congress/budget/2022/06/08/the-us-is-heavily-reliant-on-china-and-russia-for-its-ammo-supply-chain-congress-wants-to-fix-that/

[14] Gould, Joe, et. all. "Pentagon budget aims to max munitions production, make multiyear buys." *DefenseNews*: 13 Mar 2023, https://www.defensenews.com/pentagon/2023/03/13/pentagon-budget-aims-to-max-munitions-production-make-multiyear-buys/

[15] Cancian, Mark. "Rebuilding U.S. Inventories: Six Critical Systems." Center for Strategic and International Studies: 9 Jan 2023, https://www.csis.org/analysis/rebuilding-us-inventories-six-critical-systems.

adversary, no specific Intellectual Property (IP) or classified mechanism will be obtained as the components are already from the commercial sector.

The battlefield of the future will be characterized by advanced, intelligent threats operating across the EMS. Due to this environment, operational planners must consider the composition and balance of forces. Trading combat power for EW measures will become a necessity. EW is increasingly important in modern warfare, as information and communication systems are critical in military operations. By disrupting an adversary's ability to communicate or sense their environment, EW can provide a significant advantage on the battlefield. Hence, non-kinetic EW mechanisms can be leveraged to exploit critical vulnerabilities in emerging threats.

EMERGING THREATS AND VULNERABILITIES

"To know tactics, you must know weapons." – CAPT. Wayne P. Hughes Jr., USN[16]

Emerging threats require novel solutions across the EMS. As emerging technologies and offensive weapon systems continue to advance rapidly, spending time developing exquisite countermeasures aimed at defeating each weapon in its entirety is not an efficient path forward. Targeting various elements of each threat, including data flow, simplifies the problem set. Competing with peer adversaries requires freedom of thought and innovation. The emergence of AI, quantum computing, LAWS, hypersonic weapons, and DE systems require novel and often asymmetric solutions across the EMS. Through outlining emerging threats and their corresponding vulnerabilities, the necessity for leveraging EW is apparent.

---

[16] Hughes, Wayne, et. all. *Fleet Tactics and Naval Operations Third Edition* (Naval Institute Press: Annapolis, Maryland, 2018) 16.

While the U.S. government has not officially defined artificial intelligence (AI), the term is generally defined as a computing system capable of human-level or superior cognition.[17] A majority of current AI systems are classified as 'narrow AI,' or systems trained to perform specific tasks. Examples include applications focused on intelligence, surveillance, reconnaissance (ISR), and logistics.[18] Upcoming AI capabilities include general AI and artificial superintelligence. General AI computing systems are trained to perform a variety of tasks, even those outside the realm of their original scope or programming. Artificial superintelligence systems exceed the cognitive abilities of humans in all realms of operation.[19] Adversary artificial superintelligence systems may soon gather, analyze, and act on data at speeds that far exceed human cognition, shortening the computing timeline and introducing challenges to traditional operational planning methods.

Similar to AI systems, quantum technology is a data-reliant, emerging threat. Quantum technology translates the principles of quantum physics into technological applications.[20] While the technology has not yet matured, its threat poses significant implications for military operations. According to the Government Accountability Office, "Quantum communications could enable adversaries to develop secure communications that U.S. personnel could not intercept or decrypt. Quantum computing may allow adversaries to decrypt information, enabling

---

[17] Sayler, Kelley. " Emerging Military Technologies: Background and Issues for Congress." (*Congressional Research Service,* 1 November 2022) 2.

[18] Sayler, Kelley. " Emerging Military Technologies: Background and Issues for Congress." 2.

[19] Sayler, Kelley. " Emerging Military Technologies: Background and Issues for Congress." 2.

[20] For additional information on quantum computing, see CRS In Focus IF11836, Defense Primer: Quantum Technology, by Kelley M. Sayler.

them to target U.S. personnel and military operations."[21] Additionally, quantum computing and sensing threaten survivability and deterrence while providing additional mechanisms for guidance, targeting, and surveillance analysis.

Lethal Autonomous Weapon Systems (LAWS) can independently identify a target and employ an onboard weapon to engage and destroy it without manual human control.[22] These systems aim to remove human decision-makers from the targeting process. The presence of sensors and data flow in the battlefield is continuously increasing, pushing for reliance on autonomous systems in targeting and engagement operations for optimized decision-making. Although there are no completely autonomous weapon systems fielded by the U.S. yet, despite ethical concerns, this emerging technology is on the horizon. Currently, there are semi-autonomous weapon systems, or "human in the loop," weapon systems that only engage individual targets or specific target groups that a human operator has selected.[23] The next step towards fully autonomous systems is "human on the loop" weapon systems that are human-supervised and can be monitored and halted in their weapon's target engagement.[24] Similar to AI technologies, LAWS rely on algorithms and sensors in their decision-making process.

Finally, the use of hypersonic and Directed Energy (DE) weapons will characterize future conflict. Hypersonic weapons can travel at or above five times the speed of sound (Mach 5).[25]

---

[21] Government Accountability Office, National Security: Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies, December 2018, at https://www.gao.gov/assets/700/695981.pdf.

[22] Sayler, Kelley. " Emerging Military Technologies: Background and Issues for Congress." 8-9.

[23] Hicks, Kathleen. *Department of Defense Directive 3000.09: Autonomy in Weapon Systems*. (Department of Defense, 25 January 2023) 5.

[24] For additional information on LAWS, see CRS Report R44466, Lethal Autonomous Weapon Systems: Issues for Congress, by Nathan J. Lucas.

[25] For additional information on hypersonic weapons, see CRS Report R45811, Hypersonic Weapons: Background and Issues for Congress, by Kelley M. Sayler.

Although concepts of hypersonic technologies have existed for decades, the fielding of these capabilities has only recently been achieved by China and Russia. The U.S. has yet to field a hypersonic weapon or defensive capabilities to combat these threats, although the Army is targeting the end of 2023 for fielding an offensive system.[26] Meanwhile, the DoD defines DE weapons as those using concentrated Electromagnetic (EM) energy, rather than kinetic energy, to incapacitate, damage, disable, or destroy enemy equipment, facilities, and personnel.[27] While hypersonic weapons rely on kinetic energy, DE systems use EM energy to cause destruction.[28] Although both weapon systems leverage differing mechanisms to deliver damage, both weapons have the capacity to become LAWS and incorporate AI and quantum computing methods.

Today, all operating environments are sensor-rich and dense in data and information. Traditional human cognition and computing systems struggle to keep pace with the increasing rate of data exchange, making AI, quantum, and LAWS robust solutions, if not necessities. Although these systems are becoming common in military operations and society is shifting to rely on them, there are vulnerabilities. The greater challenge now is how to process all the information that is being collected.[29] AI, quantum, and LAWS rely on data; good data results in good analysis and information out, and vice versa. Additionally, these systems are vulnerable to biases from the baseline algorithms and coding chosen in their initial programming. EW can exploit both of these vulnerabilities. Repetitively injecting misleading, invalid data that surpasses system discriminants has the potential to render these systems useless. Jamming, spoofing, CEW,

---

[26] Judson, Jen. "US Army begins equipping first unit with hypersonic capability." *DefenseNews*: 9 Feb 2021, https://www.defensenews.com/land/2021/02/09/us-army-begins-equipping-first-unit-with-hypersonic-capability/.

[27] Joint Chiefs of Staff. *Joint Publication 3-85, Joint Electromagnetic Spectrum Operations*. GL-6.

[28] For additional information on directed energy weapons, see CRS Report R46925, Department of Defense Directed Energy Weapons: Background and Issues for Congress, by Kelley M. Sayler.

[29] Hughes. *Fleet Tactics and Naval Operations Third Edition,* 132.

electronic deception, and other EW support measures offer a plethora of low-cost, available solutions. Since kinetic munitions are limited by quantity, data injection through non-kinetic means offers solutions capable of supplying data at the rates necessary to successfully deceive, disrupt and deny AI systems.[30]

While emerging threats and technologies rely on data, they also leverage the operational factor of time. AI, quantum computing, and LAWS seek to optimize data computation, analysis, and decision-making timelines. Meanwhile, kinetic emerging threats, such as hypersonic and DE weapons, employ decisive damage rapidly, focusing on decreasing the second half of the targeting and engagement timeline, the time from launch to strike. With threats leveraging the operational factor of time, countermeasures and solutions must focus on exploiting time. EW fills the necessity to influence time with its capacity to deceive, disrupt, and deny adversary systems and decision-makers.

PRIORITIZING JADC2 AND MILITARY DECEPTION OPERATIONS

Electromagnetic warfare can significantly alter Military Deception (MILDEC) operations to enhance joint operations and C2 warfare. Superior MILDEC capabilities are vital in modern warfare. Key strategic competitors identified in the 2022 National Defense Strategy (NDS), such as China and Russia, have observed U.S. military operations for the past 30 years, noting that disrupting C2 systems could be one cost-effective solution to diminishing U.S. military

[30] For additional information on AI systems, see CRS Report R46795, Artificial Intelligence: Background, Selected Issues, and Policy Considerations, by Laurie A. Harris.

advantages.[31] As a result, adversaries have developed systems to reduce the effectiveness of U.S. C2 systems. EW must be leveraged to combat these capabilities.

The previous Vice Chairman of the Joint Chiefs of Staff, Gen. John E. Hyten, noted in 2021 that over the last 30 years, the U.S. had built its warfighting concepts on the assumption that it would enjoy unparalleled information dominance.[32] China and Russia have invested heavily in building electronic, cyber, and space warfare capabilities to severely inhibit the U.S.'s C2 capabilities.[33] In 2021, China publicly released a new operational concept called Multidomain Precision Warfare.[34] The concept has been linked as a response to the United States Joint All Domain Command and Control (JADC2) operational concept. The U.S. concept aims to "sense," "make sense," and "act" on information across the battlespace quickly by utilizing automation, AI, predictive analytics, and machine learning (ML) to deliver informed solutions via a resilient and robust joint network environment.[35] Meanwhile, the PRC's Multidomain Precision Warfare concept, while similar to the U.S. strategy, places more emphasis on identifying adversary vulnerabilities through the use of AI. Multidomain Precision Warfare aims to identify and target

---

[31] Hoehn, John. "Defense Primer: What Is Command and Control?" (Congressional Research Service, IF11805, 8 April 2021) 1.

[32] Copp, Tara. "It Failed Miserably: After Wargaming Loss, Joint Chiefs Are Overhauling How the US Military Will Fight." *DefenseNews*: 26 July 2021, https://www.defenseone.com/policy/2021/07/it-failed-miserably-after-wargaming-loss-joint-chiefs-are-overhauling-how-us-military-will-fight/184050/

[33] Carmack, Dustin. "Assessing the Non-Kinetic Battlespace." *The Heritage Foundation*, 31 October 2022.

[34] Insinna, Valerie. "China Could Obtain 1,500 Nuclear Warheads by 2035, Pentagon Estimates." *Breaking Defense*, 29 November 2022. https://breakingdefense.com/2022/11/china-to-obtain-1500-nuclear-warheads-by-2035-pentagon-estimates/

[35] Department of Defense. "DoD Announces Release of JADC2 Implementation Plan." 17 March 2022. https://www.defense.gov/News/Releases/Release/Article/2970094/dod-announces-release-of-jadc2-implementation-plan/

weak points in systems to employ kinetic and non-kinetic measures.[36] The U.S. perspective, focused on optimizing its joint operations and decision-making, is beneficial for the unity of effort but neglects the additional emphasis on adversarial systems. China's operational concept illustrates its recognition that emerging threats and technologies have targetable vulnerabilities, and the U.S. must be prepared to protect its C2 structure.

General Mark Milley, Chairman of the Joint Chiefs of Staff, stated the following when discussing JADC2, "this is about dramatically increasing the speed of information sharing and decision making in a contested environment to ensure we can quickly bring to bear all our capabilities to address specific threats."[37] EW is the *sine qua non* of successful JADC2 implementation. More specifically, the information provided through JADC2 needs explicit protective measures, which is likely best served by complicating PRC targeting and interference of that information. Utilizing EW in military deception (MILDEC) operations is critical to enabling JADC2 and ensuring the adversary does not compromise information sharing. While prioritizing the JADC2 infrastructure, its enabling components and systems must also be given the same precedence. EW mechanisms can inject overwhelming amounts of signals and data to overwhelm adversary AI systems that are targeting U.S. C2 processes.

"In the midst of chaos, there is also opportunity." – Sun Tzu[38]

EW has been viewed traditionally as a solution at the tactical level but utilizing it at the operational level will give the side that harnesses it a decisive advantage. Operational planners

---

[36] Insinna, Valerie. "China Could Obtain 1,500 Nuclear Warheads by 2035, Pentagon Estimates." *Breaking Defense*, 29 November 2022.

[37] Department of Defense. "DoD Announces Release of JADC2 Implementation Plan." 17 March 2022.

[38] Sun Tzu. *The Art of War.* (Oxford University Press, USA: September 1971).

must balance the operational factors of time, space, and force to optimize missions and meet objectives. Leveraging EW for MILDEC operations has the potential to influence all three operational factors. Overwhelming and deceiving adversarial systems create time delays. Projecting power through deception can deceive adversaries of accurate force capability and quantity estimates. In terms of space, MILDEC operations can make it appear as though offensive and defensive actions are occurring across numerous locations. Successful MILDEC operations are capable of buying time while projecting space and force, influencing adversarial decision-making.

Current DoD guidance defines MILDEC as actions executed to deliberately mislead adversary decision-makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to accomplishing the friendly mission.[39] MILDEC has four main deceptive techniques; feints, demonstrations, ruses, and displays. Feints are offensive actions involving contact with the adversary aiming to deceive them of the locations and timing of the actual offensive.[40] Although the term contact in the definition of a feint implies kinetic actions, non-kinetic EW can mimic the signatures of joint forces to accomplish deception. Mechanisms of which include decoys actively transmitting similar radar-cross-sections (RCS) of the fleet. Alternatively, a demonstration is power projection and a show of force intended to cause the adversary to select a course of action (COA) favorable to U.S. goals.[41] Although force projection is typically associated with physical assets and kinetic capabilities, demonstrating the effectiveness of non-kinetic mechanisms can also coax adversaries toward desired decisions.

---

[39] Joint Chiefs of Staff. *Joint Doctrine for Military Deception, Joint Pub 3-58.* I-8.

[40] Joint Chiefs of Staff. *Joint Doctrine for Military Deception, Joint Pub 3-58.* I-9.

[41] Joint Chiefs of Staff. *Joint Doctrine for Military Deception, Joint Pub 3-58.* I-9.

Ruses are designed to gain a friendly advantage by deliberately exposing false or confusing information for the adversary to collect and interpret. Ruses are similar to feints, except they are utilized during friendly operations before an offensive.[42] Non-kinetic mechanisms, such as CEW and spoofing, can be utilized operationally to spread disinformation and inject deceptive signals and data to accomplish a ruse.[43] Finally, displays are the simulation, disguising, and portrayal of friendly objects, units, or capabilities projecting the MILDEC objective.[44] Displays may depict capabilities that do not exist.

By pairing EW mechanisms with MILDEC operations, the U.S. can create chaos for adversarial systems by injecting overwhelming amounts of signals and data. In the current international ecosystem, defined by rapidly advancing technologies and emerging threats, leveraging deception innovatively will create opportunities. Some might argue that creating additional chaos on the battlefield with non-kinetic EW mechanisms will introduce unnecessary confusion for friendly forces, given the increase in noise, signal, and data processing. Although these mechanisms will further complicate the battlefield, by establishing a clear C2 structure for joint operations, the U.S. can navigate the environment. Controlled chaos is the solution for deceiving high-fidelity, advanced, emerging threats.

REDEFINING SUCCESS METRICS: UNDERSTANDING THE EFFECTS OF KINETIC AND NON-KINETIC WARFARE

Although non-kinetic EW mechanisms can secure decisive advantages in operational planning, kinetic solutions have traditionally been preferred. Kinetic options, such as guided

---

[42] Joint Chiefs of Staff. *Joint Doctrine for Military Deception, Joint Pub 3-58.* I-9.

[43] Joint Chiefs of Staff. *Joint Doctrine for Military Deception, Joint Pub 3-58.* I-9.

[44] Joint Chiefs of Staff. *Joint Doctrine for Military Deception, Joint Pub 3-58.* I-9.

munitions and missiles, yield physical, quantifiable damage, whereas the effectiveness of non-kinetic mechanisms is more challenging to assess. The unknowability of the success of non-kinetic EW has made it a less attractive option in operational planning. When considering quantifiable Battle Damage Assessments (BDAs), target sets must be kept in mind. For kinetic solutions, the target sets are physical and locatable, i.e., buildings, ships, and airfields. Performance for kinetic measures is based on accuracy and physical damage achieved. Conversely, non-kinetic solutions target the decision-making process and data. Target sets include cyberinfrastructure, data flow, signal processors, and AI computing systems. The performance of non-kinetic solutions should not be based strictly on physical damage; but also on the output of adversary decisions and chosen COAs. Operational planners must broaden their perspectives to include the understanding that non-kinetic target sets and their corresponding damage assessment metrics are different from those associated with kinetic solutions.

Moreover, some might argue that the U.S. seems to prefer the legitimacy of kinetic attacks, as non-kinetic actions can be perceived as deceptive with negative connotations associated with their true intention.[45] The legitimacy associated with kinetic attacks is directly correlated to the ability to measure physical damage. However, the aftermath of kinetic measures is often neglected. Similar to non-kinetic actions, kinetic actions generate societal and psychological impacts that are difficult to assess. The bombings of Hiroshima and Nagasaki in World War II illustrate this viewpoint. While both bombs hit their targets, the long-lasting effects were not realized until years, even decades later. In addition to widespread physical damage, the bombings psychologically impacted the entire world and sparked widespread fear, and the

---

[45] Bilal, Arsalan. "Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote." NATO Review: 30 Nov 2021, https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

concept of nuclear deterrence was born.[46] Thus, kinetic measures yield similar, difficult-to-quantify results. While deception may be seen as less legitimate, it is necessary to secure an advantage in today's operational environment against emerging threats. Additionally, EW enables kinetic warfare by allowing the platforms that carry the kinetic weapons to get closer or within weapons engagement zones. Although the effectiveness of non-kinetic solutions is difficult to assess, the impact of their success is paramount as they enable JADC2 and kinetic attacks. Modern kinetic warfare is simply ineffective without EW.

CALL TO ACTION

Joint Forces must utilize EW in novel and innovative ways to overcome emerging threats in light of the PRC's rise and resurgent Russian aggression. To effectively communicate and operate jointly, EW must be leveraged. Building resilient systems, refining EW and counter-EW capabilities, and harnessing the EMS in favor of the U.S. will be crucial in any future conflict.[47] By leveraging EW to disrupt, deny, degrade, and deceive adversarial systems, the U.S. can capitalize on opportunities from the created chaos in data flow and the EMS to enable joint operations. As discussed, achieving and maintaining an advantage in modern warfare requires a range of non-kinetic EW solutions, which are more accessible and maintainable than kinetic solutions.

Additionally, emerging threats require novel EW solutions that can target and overwhelm system vulnerabilities. Repetitively injecting misleading, invalid data that surpasses system

---

[46] Freund, Norman et. all. *NUCLEAR DETERRENCE: THE RATIONALITY OF THE IRRATIONAL.* (International Journal on World Peace, Vol. 4, No. 3; Sept 1987) 74.

[47] Carmack, Dustin. "Assessing the Non-Kinetic Battlespace." The Heritage Foundation, 31 October 2022.

discriminants has the potential to render these systems useless. Controlled chaos is the solution for deceiving high-fidelity, advanced, emerging threats. Finally, EW can significantly alter MILDEC operations to enhance information operations and JADC2. Superior MILDEC capabilities are vital for the joint force in modern warfare. Vice Admiral Horatio Nelson once stated, "A ship's a fool to fight a fort," similarly, it would be illogical for the U.S. joint force to challenge peer adversaries' emerging technologies with traditional capabilities and defenses.[48] Controlling the EMS and data are the key to winning the power competition, and EW measures will provide that control.

[48] Wester, Tom et. all. "The End of Deception." U.S. Naval Institute: Nov. 2019, https://www.usni.org/magazines/proceedings/2019/november/end-deception.

Bibliography

Adamy, David. *EW 101: A First Course in Electronic Warfare, 1st Edition.* (Artech House, 2021) ISBN 9781580531696.

Bilal, Arsalan. "Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote." NATO Review: 30 Nov 2021, https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

Cancian, Mark. "Rebuilding U.S. Inventories: Six Critical Systems." *Center for Strategic and International Studies*: 9 Jan 2023, https://www.csis.org/analysis/rebuilding-us-inventories-six-critical-systems.

Carmack, Dustin. "Assessing the Non-Kinetic Battlespace." *The Heritage Foundation*, 31 October 2022.

Clarke, Arthur. "Superiority," *The Best Military Science Fiction of the 20th Century, eds. Harry Turtledove and Martin H. Greenberg (*New York: Del Rey, 2001), 129-138.

Copp, Tara. "It Failed Miserably: After Wargaming Loss, Joint Chiefs Are Overhauling How the US Military Will Fight." *DefenseNews*: 26 July 2021, https://www.defenseone.com/policy/2021/07/it-failed-miserably-after-wargaming-loss-joint-chiefs-are-overhauling-how-us-military-will-fight/184050/

Davidson, Philip. "STATEMENT OF ADMIRAL PHILIP S. DAVIDSON, U.S. NAVY COMMANDER, U.S. INDO-PACIFIC COMMAND BEFORE THE HOUSE ARMED SERVICES COMMITTEE ON U.S. INDO-PACIFIC COMMAND POSTURE." 10 March 2021.

Department of Defense. "DoD Announces Release of JADC2 Implementation Plan." 17 March 2022. https://www.defense.gov/News/Releases/Release/Article/2970094/dod-announces-release-of-jadc2-implementation-plan/

Edmund Burke, Kristen Gunness, Cortez A. Cooper III, Mark Cozad. "People's Liberation Army Operational Concepts" *Rand Corporation*, 2022. PDF.

Freund, Norman et. all. NUCLEAR DETERRENCE: THE RATIONALITY OF THE IRRATIONAL International Journal on World Peace, Vol. 4, No. 3; Sept 1987.

Gould, Joe, et al. "Pentagon budget aims to max munitions production, make multiyear buys." *DefenseNews*: 13 Mar 2023. https://www.defensenews.com/pentagon/2023/03/13/pentagon-budget-aims-to-max-munitions-production-make-multiyear-buys/.

Government Accountability Office. "National Security: Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies." December 2018, https://www.gao.gov/assets/700/695981.pdf.

Harris, Bryant. "The US is Heavily Reliant on China and Russia for its Ammo Supply Chain." *DefenseNews*: 8 June 2022. https://www.defensenews.com/congress/budget/2022/06/08/the-us-is-heavily-reliant-on-china-and-russia-for-its-ammo-supply-chain-congress-wants-to-fix-that/

Harris, Laurie. "Artificial Intelligence: Background, Selected Issues, and Policy Considerations." *Congressional Research Service*, R46795, 19 May 2021.

Hoehn, John. "Defense Primer: What Is Command and Control?" *Congressional Research Service*, IF11805, 8 April 2021.

Hoehn, John. "Overview of Department of Defense Use of the Electromagnetic Spectrum." *Congressional Research Service*, R46564, 14 November 2022.

Hughes, Wayne, et al. *Fleet Tactics and Naval Operations Third Edition* (Naval Institute Press: Annapolis, Maryland, 2018).

Insinna, Valerie. "China Could Obtain 1,500 Nuclear Warheads by 2035, Pentagon Estimates." *Breaking Defense*, 29 November 2022.

Joint Chiefs of Staff. *Electronic Warfare, Joint Publication 3-13.1.* 25 January 2007, file:///C:/Users/audre/Downloads/469779%20(1).pdf. Online.

Joint Chiefs of Staff. *Joint Doctrine for Military Deception, Joint Pub 3-13.4.* 26 January 2012, https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf. Online.

Joint Chiefs of Staff. *Joint Doctrine for Military Deception, Joint Pub 3-58.* 31 May 1996, https://irp.fas.org/doddir/dod/jp3-58.pdf. Online.

Joint Chiefs of Staff. *Joint Electromagnetic Spectrum Operations, Joint Publication 3-85.* 22 May 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf?ver=2020-04-09-140128-347. Online.

Judson, Jen. "US Army begins equipping first unit with hypersonic capability." *DefenseNews*: 9 Feb 2021, https://www.defensenews.com/land/2021/02/09/us-army-begins-equipping-first-unit-with-hypersonic-capability/.

Liang, Xiangsui. "Unrestricted Warfare" *Beijing: PLA Literature and Arts Publishing House*, February 1999.

Lucas, Nathan. "Lethal Autonomous Weapon Systems: Issues for Congress." *Congressional Research Service*, R44466, 14 April 2016.

National Aeronautics and Space Administration. "The Electromagnetic Spectrum." *NASA: Goddard Flight Center*, March 2013. https://imagine.gsfc.nasa.gov/science/toolbox/emspectrum1.html.

Nurgul Yasar, Fatih Mustafa Yasar, and Yucel Topcu "Operational Advantages of Using Cyber Electronic Warfare (CEW) in the Battlefield," Proc. SPIE 8408, Cyber Sensing 2012, 84080G (7 May 2012); https://doi.org/10.1117/12.919454.

Sayler, Kelley. "Defense Primer: Quantum Technology." *Congressional Research Service*, IF11836, 15 Nov 2022.

Sayler, Kelley. "Department of Defense Directed Energy Weapons: Background and Issues for Congress." *Congressional Research Service*, R46925, 13 Sept 2022.

Sayler, Kelley. "Emerging Military Technologies: Background and Issues for Congress." *Congressional Research Service,* 1 November 2022. PDF.

Sayler, Kelley. "Hypersonic Missile Defense: Issues for Congress." *Congressional Research Service,* 3 October 2022. PDF.

Sayler, Kelley. "Hypersonic Weapons: Background and Issues for Congress." *Congressional Research Service,* R45811, 13 Feb 2023.

Shelbourne, Mallory. "China Has World's Largest Navy with 355 Ships and Counting, says Pentagon." *USNI News*: 3 Nov. 2021, https://news.usni.org/2021/11/03/china-has-worlds-largest-navy-with-355-ships-and-counting-says-pentagon.

Sun Tzu. *The Art of War* (Oxford University Press, USA: September 1971).

Theohary, Catherine. "Defense Primer: Information Operations." *Congressional Research Service*, 9 March 2022. PDF.

Theohary, Catherine. "Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues." *Congressional Research Service*, 17 March 2009. PDF.

U.S. Department of Defense. *2022 National Defense Strategy of the United States of America.* 27 October 2022, media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF. Online.

Wester, Tom et al. "The End of Deception." U.S. Naval Institute: Nov. 2019, https://www.usni.org/magazines/proceedings/2019/november/end-deception.