AIR WAR COLLEGE

AIR UNIVERSITY

Future Operating Concept for Employing Electronic Warfare in the Cyberspace Domain

by

David C. Van Brunt, CDR, USN

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

17 February 2010

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
17 FEB 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Future Operating Concept for Employing Electronic Warfare in the Cyberspace Domain	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air War College,Air University,325 Chennault Circle,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**33**	

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Illustrations

Page

Biography

CDR David Van Brunt is an active duty Navy Information Warfare Officer. A graduate of the United States Naval Academy, he has served at sea and ashore providing critical cryptologic and electronic warfare indications and warning. Tours have included Cryptologic Resource Coordinator and a Command and Control Warfare Officer for the Peleliu Amphibious Ready Group; the Outboard and Electronic Warfare Officer onboard USS Merrill; Officer in Charge of an Information Warfare detachment; IO Requirements officer at Naval Network Warfare Command, and Deputy IO Chief at Naval Forces Europe/Africa/Sixth Fleet. He has served as the JTF's Deputy IO Chief during exercise Austere Challenge 2008.

CDR Van Brunt has earned a Bachelor's Degree from USNA and a Masters Degree in Information Systems Technology from the Naval Postgraduate School. He earned JMPE phase 1 from the Naval War College. He is working towards a Masters Degree in National Strategic Studies from the Air War College.

Introduction

The Cyberspace domain is a military domain, like air and space, which changes the opportunities and vulnerabilities of conducting the mission essential functions of electronic warfare. An understanding of the advantages, constraints and limitations within the Cyberspace domain is critical in developing a future operating concept for Electronic Warfare (EW) forces and capabilities, and more importantly, to apply these functions effectively in the Cyberspace domain to support the Joint Force Commander (JFC).

1. General

a. Historical Evolution of Electronic Warfare

i. EW Warfare Theory; Strategists; Importance

Electronic Warfare adheres to fundamental warfare theories. From Clausewitz, Sun Tzu and Boyd, the basic warfare principles define the JFC's EW employment. Appendix A examines warfare theory as applicable to EW.

EW is one of five core competencies of Information Operations (IO) as defined by Joint Publication 3-13. Beyond the definition, IO is not just a group of capabilities comprising information, but a grouping of capabilities affecting information.[1]

It is important to understand how this applies to the JFC. EW has been an important warfighting force capability since man has manipulated the electromagnetic (EM) spectrum. EW operations refer specifically to the capabilities defined by Joint doctrine (JP 3-13, Information Operations). Thus, EW is "any military action involving the use of EM or directed energy to control the EM spectrum or to attack the enemy."[2] Specifically, it includes three major subdivisions: electronic attack (EA), electronic protect (EP), and electronic warfare support (ES).

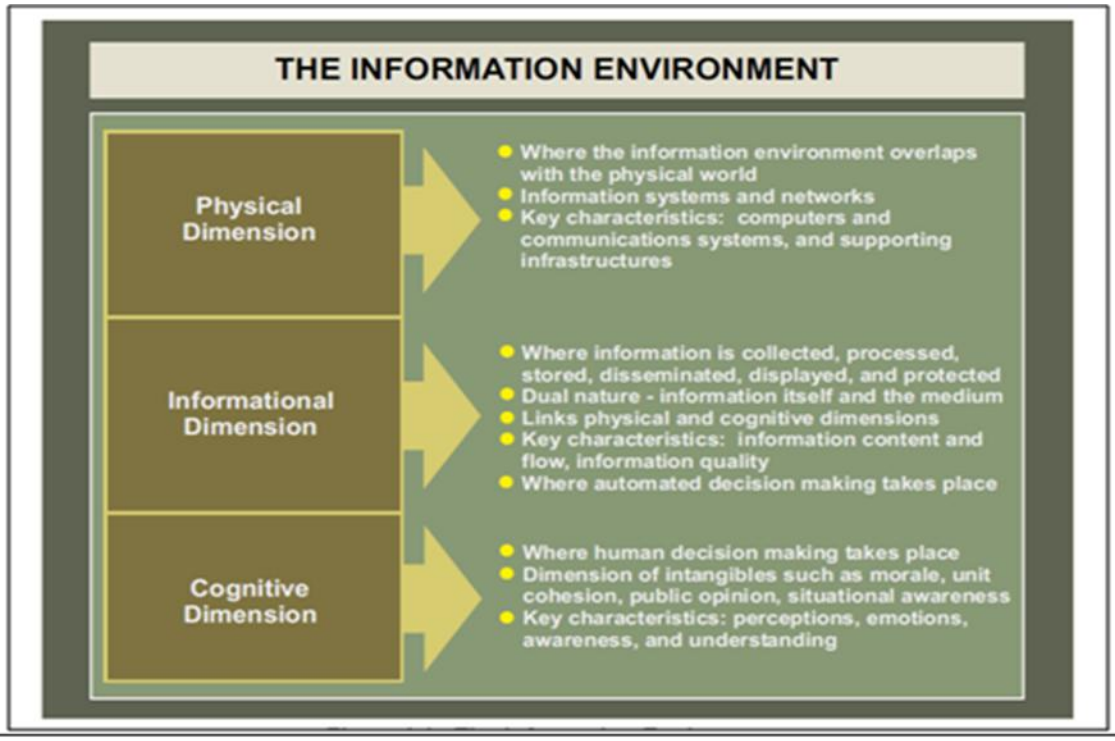


Figure 1: The Information Environment

EW, along with all elements of warfare, operates within the Information Environment (IE) (Figure 1).[3] In order for the JFC to achieve desired effects, he must understand this environment. It is a fundamental part of the operating environment, grounded in the physical domain.[4] It contains three dimensions. The first dimension, the physical dimension, is where computers, sensors and networks physically reside. The second dimension, informational, is where information is collected, processed, stored, disseminated, displayed and protected. This is also how the physical dimension connects to the cognitive dimension. Within the cognitive dimension, the value of collected, processed information becomes actionable. Human decision making occurs here. Therefore, although the cognitive dimension is EW's primary target, EW affects it through the physical and informational dimensions. While directly affecting the cognitive dimension may be prohibitive or too costly, it is possible to find weaker spots within the other dimensions to initiate the adversary's collapse. Thus, offensive EW "emphasizes the

manipulation of electronic information systems to influence an adversary's perceptions and behavior" and involves "disabling military and civilian telecommunication systems through computer viruses or electromagnetic pulse devices."[5] Fundamentally, EW impacts the physical and information dimensions by jamming, disrupting information paths, corrupting data, etc, affecting the cognitive domain, influencing the adversary and achieving desired effects.

ii. EW Methodology in Prior Conflicts.

All sides have utilized EW to gain strategic, operational and tactical advantages, from the rapidly transforming scientific battlefield applications during World War II to current wars in Iraq and Afghanistan. Appendix B describes historical operational EW employment.

b. Cyberspace Operational Advantages.

Cyberspace is characterized by electronics and the EM spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. Thus, it's a real physical domain consisting of hardware and networked systems utilizing EM energy existing across all other domains and connecting the physical domains with cognitive processes.[6] As Cyberspace's foundation resides on the IE's physical dimensions, then warfighting in cyberspace is necessarily about physical operations.[7]

Cyberspace's interconnected information technology infrastructure enables operational military advantages when operating effectively within it. It has also fundamentally altered the relationship between time, space, and distance and how capabilities are employed. EW operations both affect Cyberspace capabilities and support Cyberspace operations.[8] Based upon the IE framework, all of the capabilities developed supporting nation-states or individuals, are ultimately based upon the supporting physical and information dimensions. It is through these dimensions that military EW provides operational advantages.

The Cyberspace domain is a tremendous enabler for deception. Through Cyberspace a commander can rapidly understand the situation, or adversely affect his target. EW through Cyberspace can achieve strategic and operational level deception, affecting the adversary's cognitive domain preventing military actions. ES and Computer Network Exploitation (CNE) allow the commander to know adversarial capabilities, force distribution, and intentions.

EW does not simply equate to stand-off jamming. It is better defined as "anything that uses or prevents the use of any part of the broadcast spectrum [i.e., EM]."[9] Therefore, "just like the other four warfighting domains – air, land, sea and space – cyber relies on EW in order to achieve control of and enjoy free access to the electromagnetic spectrum."[10] Operating effectively within Cyberspace provides significant operational advantages. Utilized properly in an integrated operational approach with the other IO capabilities, EW in Cyberspace enables the ability to subdue the enemy "by attacking his ability to form a coherent strategy."[11]

2. Purpose

a. EW Mission Essential Functions

Several EW mission essential functions directly support the JFC. When conducted within Cyberspace, the JFC is provided with operational advantages. The current mission essential functions of EW are identified in Appendix C.

Disrupting, degrading and usurping databases, information flow and the physical 'wires and poles' of Cyberspace produce effects within the adversary's cognitive dimension. For instance, denying or disrupting the information, data or EW network connectivity destroys diminishes observation and orientation. Disrupting an adversary's information system pathways affects the ability to make, disseminate, and execute decisions, thus the ability to act. EW's functions in Cyberspace against an adversary's technical capability, impacts cognitive will.[12]

Additionally, EW within Cyberspace enables shaping of an adversary's cognitive dimension by targeting data interpretation. This can either force action or inaction, or cause information/system distrust. This increases stress, introducing randomness into decision making processes.[13] Additional stresses due to EW include deception via false or repeated information into the system.

Likewise, another essential EW function is defending the JFC's communications links and navigational aids. These are vital as strike execution is linked within the Cyberspace domain via these technical paths.[14]

Finally, essential ES functions within Cyberspace include locating, identifying, targeting, and timely collaboration enabling time-critical kinetic and non-kinetic strikes. Essential EA functions within Cyberspace include jamming, disabling, and disrupting EM signals; accessing and corrupting and/or usurping enemy EW system networks; injecting false signal data, corrupting data at rest, eliminating vital data, transmitting intermittent data; and physical destruction of sensors. Essential EP functions within Cyberspace include ensuring EW network data file integrity, and system information authentication.

The combat process must emphasize inputs to the adversary's decision making process. A goal is to provide partial information to the adversarial commander sufficiently influence him to take inappropriate actions.[15] Precise, limited deceptive data can achieve significant effects[16] on the adversary. Attacks on network architectures debilitate the adversary's decision making process.

Finally, essential EW functions within Cyberspace provide operational advantages to the JFC to shape the IE by destroying the adversary's view of information, influence probability of outcomes and create exploitation opportunities.

b. Challenges and Opportunities

This future operating concept aids the JFC coping with challenges of conducting EW in Cyberspace. It identifies necessary capabilities and operational functions required to exploit Cyberspace opportunities. As this environment is occupied and contested, simple calls for information superiority are impossible. However, conducting EW via Cyberspace assists the JFC achieve Information Control enabling the JFC to maintain initiative through the conflict and achieving victory.[17]

The JFC conducts EW operations within Cyberspace to defend his sensors, networks, and information paths, and influence his adversary's cognitive dimension through attacking the underlying physical and informational dimensions. As a "computer cannot be deceived by destroying its components,"[18] the cognitive dimension is influenced through informational and physical access. EW provides the JFC the ability to maneuver by protecting his IE and controlling the adversary's. Denying the adversary accurate battlespace situational awareness is crucial[19] to maneuver warfare.

3. Time Horizon, Assumptions, Risks

a. Time Horizon

This future operating concept describes Joint EW operations within Cyberspace for the 2009 – 2015 planning horizon. It builds upon and assumes capabilities described in section 6. It assumes full integrations with all IO capabilities and other non-kinetic and kinetic planning actions. This concept assumes operational control will be given to a JFC within a Regional Combatant Commander (COCOM)'s designated Joint Operating Area (JOA) with support from the functional commands, Strategic Command (STRATCOM) and Cyber Command (CYBERCOM).

i. Current (2009-2010) Implications

Current military implications of EW within Cyberspace have been demonstrated by Russia against Estonia and Georgia. Additionally, Operation Iraqi Freedom has seen an increase in EW operations via Cyberspace. Appendix D details these implications.

ii. Future (2015 and Beyond) Implications

Future implications include an occupied domain with increasingly robust capabilities and technological breakthroughs. These breakthroughs and new effects will occur exponentially due to infinite combinations enabled via increasing processing and networking. Increasing numbers of nodes and users will create precisely tailored capabilities.[20]

Cyberspace operations will transform JFC capabilities. Long-range detection and targeting will occur long before traditional capabilities can even identify threats.[21] Deterrence, degradation and defeating targets will occur at previously unthinkable distances.[22] JFC contingency plans will require swift counterterrorism operations against social networks in Cyberspace.[23]

There will be a ubiquitous use of technically sophisticated measures affecting the IE. There will be increased false telemetric signals misdirecting targeting computers, direction of high-powered microwave beams to disable missile computing circuitry; GPS jamming;[24] targeting other connected networks, such as domestic financial networks by adversarial states or non-state actors.[25] These threats will be integrated within all operational forces. New requirements will include maintaining social net monitoring tools to keep pace with the rapidly changing IE.[26]

b. Assumptions

This operating concept assumes full integration of EW with all IO capabilities and other non-kinetic and kinetic actions. Cyberspace will continue to be occupied and contested; the domain will be ubiquitous and essential to perform JFC functions. The time and space dimensions will be more compressed due to the domain's near-instantaneous nature. It assumes OPCON will be given to a JFC within a Regional COCOM's designated JOA.

Further assumptions include the development of CYBERCOM as a fully functioning Combat Support command. The 'wires and poles' composing the IE's physical dimension will be protected. Fidelity within the informational dimension will be established. Cyberspace exploitation and other intelligence preparation of the battlespace (IPB) (i.e., Electronic Orders of Battle (EOB)) will be accomplished. Furthermore, robust network attack capability packages will be developed with clearly established authorities to support the JFC achieve effects supporting time-sensitive strikes. Other required rules of engagement (ROE) will be addressed by the JFC. All services will be interoperable with EW capabilities within Cyberspace.

c. Risks

Significant risks are associated when operating EW in Cyberspace due to time horizons. The contested and congested domain, ubiquitous nature of advanced technologies, and hyper-capable individualization distributed globally achieving massed effects must all be considered by the JFC. Likewise, the evolution of cyber capabilities beyond 'wires and poles' to the 'wireless' domain of the 'cloud' expands the JOA in ways yet to be determined.

Successfully implementing this strategy will separate the adversary's decision maker from his forces and society. Militarily, it will be more difficult to determine victory. In what legal and ethical manner is the JFC's worldview to be imposed upon the adversary's society? For a JFC operating within a JOA, legal risks include crossing multiple COCOMs to achieve

effects within the JOA. Finally, the time/space compression nullifies many capabilities due to current coordination and execution approval processes.

4. Military Problem Description

a. More Effective EW Operations Within Cyberspace to Deny, Degrade, Disrupt, Influence and Usurp Target Information Systems and Decision Makers

The JFC must employ EW within Cyberspace by fully integrating all capabilities affecting information in near-real-time. Integrated capabilities within Cyberspace provide a "synthesized suite of effects to the JFC far exceeding the traditional simple menu of kinetic or non-kinetic delivered by air-breathing platforms,"[27] to include all EW elements.
Based on the nature of Cyberspace described above, it is essential that the JFC operates within command and control (C2) structures permitting rapid adaptability.

EW capabilities within Cyberspace must leverage a distributed cyber-sensor network.[28] The JFC must operate freely within the domain to effectively achieve effects through and within it. ES in Cyberspace identifies themes, refines messages and identifies targets. It also provides measures of effectiveness (MOE). EA will be a transmission path for JFC messages and suppression of the adversary's use of the EM spectrum. EP assists in maintaining JFC C2 integrity.[29]

EW attacks against an "adversary's C4ISR infrastructure to prevent or disrupt the acquisition, processing, or transmission of information in support of decision-making or combat operations"[30] will be integrated and synchronized with other non-kinetic and kinetic strikes. EW degrades C4ISR networks to prevent the adversary "from collecting, processing, and disseminating information or accessing information necessary to sustain combat operations"[31] enabling the JFC to achieve operational objectives. Integration of EW with other operations via

Cyberspace must be closely aligned throughout. Although it is difficult to precisely time effects, it is essential to determine accurate BDA for attacks against capabilities such as IADS.[32]

As all military operations depend upon availability of the EM spectrum,[33] access to Cyberspace is achieved through multiple means: RF spectrum proximity, IP-based networks, and physical connections. The JFC must be able to access the adversary's cyberspace domain, understand operational targets, and then align with precise, certified, weapons and operators to confidently achieve effects. Systems will be required to be cross-networked, networked-enabled, embedded within the widest range of forces and linked with US-based shore facilities.[34]

For the JFC, intelligence underlies all EW operations within Cyberspace. IPB is essential for understanding the underlying network architecture of the adversary's cyberspace capabilities and the relationships between his systems.[35] To achieve effects, the JFC must understand where and how the adversary's vulnerabilities. Equally vital is the intelligence requirement for accurate and timely EW MOE from national assets and CYBERCOM. Within the JFC's control, ES and CNE will determine the networks, communication links, etc, to develop attack plans and determine MOE. See Appendix D for detailed JFC application of EW through the 'phases' of war.

b. Adversary Use of Cyberspace

An adversary will initially focus initially on critical physical dimensions such as undersea fiber networks, [36] and wireless communications links. [37] Adversarial cyber attacks can impact the physical dimension. They can destroy electrical generators, disrupt commercial air and train traffic, destroy high-tension power-transmission lines, degrade weapons, delete financial databases and transactions, etc.[38] Most adversaries today can access Cyberspace and the resident knowledge within.[39] Thus, EW networks, including C2 of early warning radar networks, EW

threat library databases, etc, are all potentially subject to attack, denial, degradation or destruction.

Like Electromagnetic Pulses (EMP), the adversary will not only seek cyber attacks to EW systems, but EW threats to cyber networks. The JFC can expect targeting against his navigation, air defense, communications, intelligence, etc, systems. [40]

Additional devastating possibilities arise with EMP threats within the JOA or at critical nodes affecting the JOA. Due to the interconnection of other warfighting domains to Cyberspace, an EMP would destroy all electronic equipment, shutting down regional computers, erasing databases, destroying communication nodes, radios, and cell-phones.[41] It would cripple Cyberspace within the JOA, destroying the JFC's ability to operate. Non-nuclear EMP weapons development is especially worrisome as the non-military cyber environment is essentially defenseless. Thus, it is critical for the JFC to focus upon EP in addition to CND and OPSEC.

5. Synopsis

a. EW Operations Sequenced/Integrated With Other IO Capabilities

IO is an integrating strategy. Therefore, EW will be utilized to influence an adversary's will and affect those capabilities enabling action. This can be to influence key decision makers or affect their technical capabilities to observe, orient, decide or act.[42] To do so, EW must integrate fully with all joint operations to achieve maximum potential towards JFC objectives.[43] Cyberspace necessitates EW planners not only coordinate with other aspects of JFC operations utilizing EM, but must also those conducting CNO.

The route to achieving JFC effects is grounded in the physical and informational dimensions, that is, machines and data. Through these paths, EW significant affects on adversarial will. Integrating influence objectives with OPSEC, CNO, and CND presents cognitive realities for the adversary. These realities align with PSYOP plans to influence the

adversary. Additionally, EW integration with media, PSYOP, CNO and OPSEC is integral to supporting MILDEC plans. Integrating these IO capabilities with all instruments of power will achieve JFC objectives. These integrated activities also must be specifically sequenced to rapidly support the JFC via other kinetic and non-kinetic activities.

EP will be closely sequenced with OPSEC and CND to protect the JFC's information environment. ES must be sequenced to support other kinetic/non-kinetic attacks and as MOE. Similarly, EA provides robust capabilities supporting kinetic operations when integrated within the JFC's fires plan. Achieving full potential of EW via Cyberspace will resemble the Chinese goal of "Integrated Network Electronic Warfare" which relies on "simultaneous application of electronic warfare and computer network operations against an adversary's [C4ISR] networks and other essential information systems."[44]

EW integrated operations in Cyberspace enables identification of processes, mechanisms and systems that the adversary's information is gathered and decisions made and disseminated, including critical nodes, redundancy and back-up systems.[45] EW identifies "key decision-making and communications nodes, linkages and their associated critical vulnerabilities are identified and attacked."[46] Also, along with CNE, ES provides network topology, software types, information paths, etc, for robust JFC IPB. It then provides MOE on kinetic and non-kinetic actions for follow-on JFC decisions. Appendix D details JFC integration of EW in the battle rhythm. Appendix F provides examples of integrated EW operations through Cyberspace.

b. Achieving JFC Objectives With EW-Enabling Effects Through Cyberspace

Clearly, then, JFC objectives can be achieved through EW in Cyberspace. EP supports CND and OPSEC defending the JFC's physical and informational dimensions to maintain

information and system integrity. It also enables execution of other kinetic and non-kinetic operations.

ES identifies adversarial network's physical nodes, for both intelligence and targeting. EA in Cyberspace targets adversarial "information warfare facilities, transmission means, reception platforms, and information-flow capabilities" to disrupt networks and achieve information superiority achieving battlefield maneuverability.[47] EA in Cyberspace will be synchronized with other capability operations. This enables operations ranging from SEAD to kinetic strike. IADS networks, given access obtained through CNE, may be susceptible to CNA. CNA will degrade, disrupt or disable effective IADS employment, enabling remote SEAD. If the networks are not accessible, then supporting networks, such as those maintaining electrical generators powering the IADS may be exploitable.

EA and CNA operations degrade adversarial C2 capabilities, reducing situational awareness, communication within the network, coordination actions or MOE. When integrated, EW in Cyberspace denies the adversary access to the information systems critical to conduct combat operations.[48]

"EW has massed capabilities to attack most, if not all, EM-susceptible adversary network apertures ('soft' and 'hard'), protecting friendly networks." Adversary's space, communications, wireless networks, IADS, ISR, etc, are all susceptible to EW.[49] Additionally, the JFC's use of airborne EA can deliver CNA taking down adversary capabilities for extensive periods without requiring daily target revisit sorties.[50]

EW provides capabilities to deny, degrade, usurp the very connective structural base of an adversary's strategic worldview. Basing collective world-views upon communications and network-layers, these physical dimensions are vulnerable to attack. Therefore, synchronized and

integrated EW operations in Cyberspace can destroy the enemy's observation, orientation and worldview, paralyzing decision making and actions. Alternately, disruption or usurpation of the adversary's informational dimension can influence him to take actions favorable to the JFC. Thus, EW enables mass and maneuver to the JFC throughout the ROMO.

6. Necessary Capabilities

a. Additional Authorities/Changes to Applicable Laws Required by the JFC to Effectively Operate Within Cyberspace

There are specific authorities and laws required to employ EW in Cyberspace. Based upon the domain's nature, EW capabilities must be planned and integrated at the conflict's onset. Pre-approval of EW capabilities within Cyberspace must be granted to the Regional COCOM responsible for effects within his AOR. Current authorization requirements and delegated authorities are too cumbersome in this stochastic environment.

Additionally, the compressed time, space and distance within Cyberspace necessitates that C2 be pushed to the lowest possible level.[51] Such changes enable flexibility and speed. The JFC will achieve EW fast-transient maneuver with such construct.

The JFC will not be able to dominate[52] both RF and Cyberspace. The JFC will operate in congested and contested operating environments in which the adversary operates as freely as non-combatants and friendly joint forces. Legal refinement is required to consider second and third-order effects.

Finally, legal frameworks need to redefine the JOA. As Cyberspace is ubiquitous, lacking geographic boundaries, the JFC's maneuverability is constrained by current Unified Command Plan models. Providing the JFC with authorities within a "logical" JOA defined by where effects occur will maximize effectiveness within Cyberspace.

b. Emerging Technologies Enabling EW Within Cyberspace

Along with additional authorities and legal concerns addressed above, there are also emerging technological requirements. For EW, technologies focused upon the physical and informational dimensions are critical. Through these emerging technologies, the JFC will more effectively affect cognitive dimensions.

Emerging technologies within the physical dimension must be incorporated to protect the JFC's information environment and exploit the adversary's. New critical infrastructure hardening and protection capabilities are required. This will enable JFC with fight-through capabilities from adversarial attacks on EW information systems and capabilities.

Within the EM spectrum, EW planners utilize the JRFL as a critical management tool.[53] In Cyberspace, similar technologies managing networks, databases, systems and information paths of the adversary's targeted networks must be employed. Like EW, Cyberspace "cease buzzer" procedures must be incorporated.[54] Technologies enabling "guarded," "protected," and "taboo" nodes, wires, topologies, and packets, must be developed.[55]

Physical domain technologies enabling ES of the adversary must be more robust. Such ES used to collect information within the EM spectrum "can be used to plan C2-attack operations and provide feedback"[56] Likewise, CNE utilized to collect EW-related network system information can enable more effective friendly EW operations.

Additionally, the ability to exploit the wires of Cyberspace[57] will become vital. The capabilities provided by highly directional, non-nuclear EMP for more precise effects against targeted cyberspace physical dimension nodes and wires must be available in certain situations.[58]

Within the physical dimension, technological advances must be incorporated. "Vast amounts of data can be assimilated, processed, and made available to military users, allowing precision weapons to be directed against long-range targets. Protecting the integrity of these data

is a major objective of current IW technology."[59] Specific capabilities required to secure the JFC's IE are detailed in Appendix E.

7. Summary

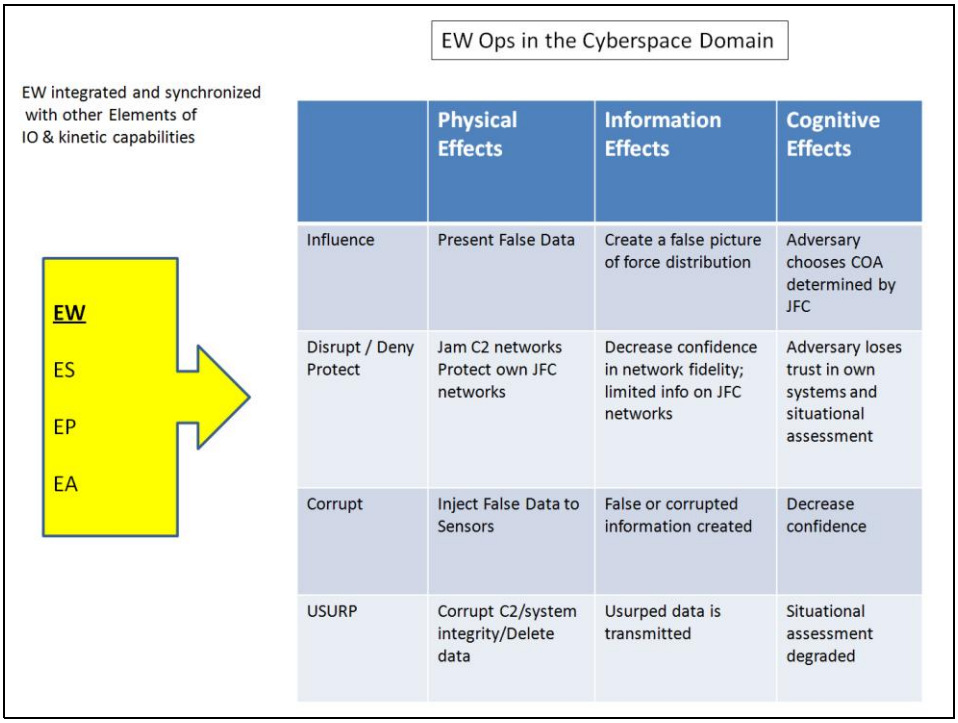
a. JFC Operational Advantages of EW in Cyberspace

As Cyberspace is fundamentally an interconnected network of electronics, computers, routers, utilizing the EM spectrum, EW's ability to affect the physical and information domains enables the JFC to influence the adversary's cognitive dimension. Due to the domain's occupied nature, JFC presence provides leveraging opportunities as identified and creation of operational advantages when able. This creates flexibility and maneuverability for the JFC. Integrating and synchronizing EW capabilities supports JFC kinetic, influence and MILDEC.

Through unity of effort, EW/Cyberspace capability authorities delegated to lowest available levels, the JFC can effectively exploit opportunities on the domain. Enabling local commanders to recognize and exploit vulnerabilities when recognized, they can proactively meet JFC objectives.[60] In this way, the JFC gains significant operational advantage by executing authorized capabilities against ubiquitous and instantaneous threats within a stochastic environment.

Meeting specified capability requirements identified in 6.a and 6.b, the JFC will operate in a flexible, creative, and adaptive system. Subordinate commanders, enabled via systems processes, are able to take required actions as needed. The associated risk of this system is mitigated through trust in the system, the information and the commanders. Trust is achieved within the system through data fidelity (attribution) and proper authentication measures. Trust of C3I information is also maintained through network security and data integrity.

Through the ROMO, the JFC integrates and synchronizes EW operations to maximize effects. The adversary's cognitive dimension is affected through data and information denial, disruption, degradation and disruption via EW. As described in 4a, integrated EW operations in Cyberspace achieves JFC effects by protecting the physical and informational dimensions of the IE.



	Physical Effects	Information Effects	Cognitive Effects
Influence	Present False Data	Create a false picture of force distribution	Adversary chooses COA determined by JFC
Disrupt / Deny Protect	Jam C2 networks Protect own JFC networks	Decrease confidence in network fidelity; limited info on JFC networks	Adversary loses trust in own systems and situational assessment
Corrupt	Inject False Data to Sensors	False or corrupted information created	Decrease confidence
USURP	Corrupt C2/system integrity/Delete data	Usurped data is transmitted	Situational assessment degraded

Figure 2: EW Effects via Cyberspace

For example, denying, degrading, corrupting or usurping adversary communication systems restricts his ability to transmit "battlefield information to all echelons, allowing timely and effective decisions relative to force deployment and movement."[61] Thus, the JFC affects the adversary's situational awareness. Denying, degrading or corrupting this information via EW through Cyberspace provides advantageous effects for the JFC against the adversary's ability to orient. Defensively, the JFC's ability to "detect and thwart attempts to tamper with one's own sources of information… (assures) the integrity of command and control, communications, and intelligence systems."[62]

Fundamentally, the JFC's ability to affect the adversary's cognitive dimension is the goal of combat operations. Therefore, the JFC must know all dimensions within the IE. "Although understanding the technical aspects of an adversary's networks and their capabilities are two primary objectives, understanding the human, cultural, and procedural factors that govern the adversary's command and control are equally important."[63] Thus, targeting the adversary's cognitive orientation by degrading adversary's GCI radar, which "functions to speed the transfer of data, filter the extraneous target reports, calculate the threat, and advise the operating personnel on the best defensive measures," the data links coordinating data from acquisition radar to weapon control radars, and the command guidance systems which the computer tracks "the target and another to track and send guidance commands to the missile."[64]

b. Essential Functions and Capabilities That EW Executes Within Cyberspace Enabling the JFC to Execute Outside Time/Distance Constraints

EW executed within Cyberspace requires several mission essential functions and capabilities enabling the JFC to operate beyond time/distance constraints. In addition to traditional EW functions identified in section 2a, Appendix E lists additional functions required to execute EW within Cyberspace.

8. Command relationships & architecture

a. Required Command Relationships

The JFC has authority and OPCON over forces assigned within the JOA. Many of the EW and Cyberspace-enabling capabilities will be required from the regional COCOM or from CYBERCOM. The stochastic nature of Cyberspace requires EW capabilities available to the JFC immediately upon orders receipt.

The JFC will require many CYBERCOM-controlled capabilities and execution authorities. The assignment of assets and capabilities outside of JFC control needs to occur

immediately. This requires extensive interaction between regional COCOM and CYBERCOM. Under current Cyberspace force distributions and authorization requirements it's unlikely that these processes will occur rapidly enough to meet immediate JFC needs to synchronize and integrate within planning and response efforts.

Cyberspace EW capabilities must be assigned full-time within each regional COCOM, with only limited global special capabilities held within CYBERCOM's OPCON. These specific capabilities will be employed through higher-echelon coordination. The JFC's ability to achieve effects within the JOA is unachievable in Cyberspace without these full-time capabilities. Full-time capabilities OPCON to the regional COCOM enables long-term, comprehensive EOB and network vulnerability analyses, closely aligned to daily operational requirements. Through this integrated relationship, the JFC will be on the domain before crises occur, with access and sensors monitoring the domain, and with tailored, specific effects developed to meet JFC's requirements within the JOA. In this way, the JFC's ability to achieve effects within the JOA, although the electronic bits may cross multiple geographic boundaries, will be most effectively integrated and synchronized to achieve maximum results. Additionally, the future operating environment will require rapid approvals (pre-approvals) of EW Cyberspace capabilities to meet timely requirements within the JOA. Approval authorities must be delegated immediately to the lowest possible command levels as the distributed problem-solving style, backed by global surveillance and communications support, is the most effective command style to handle data overload and response time problems.[65]

b. Approval Process for EW Operations Within Cyberspace

As mentioned in 6a, Cyberspace's nature transcends traditional EW. As EW in Cyberspace has compressed the time/space dimensions, it's more likely that cyber warfare will

occur. The ease, affordability and relative anonymity of the domain will tempt many state and non-state actor to engage the JFC. If the JFC does not act rapidly, this IE may be destroyed first.[66] Clearly, then, it will be critical to have specific EW operations within Cyberspace pre-approved.

For all EW operations within Cyberspace, the Laws of War apply (discrimination, necessity, proportionality, and chivalry/humanity). Discrimination in Cyberspace "assumes that you know who attacked you [attribution problem]…they may be able to mislead, placing the blame on others by spoofing the source."[67] Assailants may hide their attacks by routing through nodes and devices through innocent intermediary systems, routed through multiple nations. As almost all JFC, government and commercial capabilities are inextricably linked to Cyberspace with certain national infrastructures so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.[68] However, applying proportionality is complicated as the attacker may not be easily identified.[69] Military planners must weigh the humanity of their actions, avoiding unnecessary suffering and destruction.[70] In some instances, EW in Cyberspace allows actions that kinetic options would disallow under concepts of humanity. For instance, temporarily disabling a dam's electronic control system would not be illegitimate if doing so did not let loose a flood or deprive civilians of water for the purpose of denying them sustenance.[71] The same concepts are applicable to affecting electrical grids through Cyberspace, vice kinetic options.[72] Finally, for CND-Reactive Attack capabilities automated against specific threats, US Code Title 10 authorities may need to be broadened to enable automated decision-making systems to meet the challenges of time/distance presented by EW in Cyberspace.

9. Conclusion

The Joint Force Commander is presented with extraordinary vulnerabilities and capabilities through the Cyberspace domain. Conducting Electronic Warfare within Cyberspace is crucial to protecting the JFC's information environment, exploiting the adversary's IE, and gaining operational maneuverability. As demonstrated in this future operating concept, to most effectively operate within this domain, the JFC requires specific capabilities, restructured command and control constructs, and additional execution authorities. Only by implementing these changes will the JFC be able to successfully achieve national mission objects.

Bibliography

Adams, James, The Next World War. Simon & Schuster, 1998.

Air Force Doctrine Document 2-5 (draft), 11 Jan 2005.

Alberts, Gorstka, Stein, Network Centric Warfare: Developing and Leveraging Information Superiority. CCRP, 2000.

Arquilla, John and Ronfeldt, David, The Advent of Netwar. Rand, 1996.

Arquilla, John, "The Great Cyberwar," Wired, February 1998.

Armistead, Leigh, Information Operations: Warfare and the Hard Reality of Soft Power, Brassey's Inc., 2004.

Bourque, Jesse, "Why EW is Not Part of Cyberspace," Journal of Electronic Defense. Gainesville: September 2008. Vol. 31, Iss. 9; pp 38-40.

Bourque, Jesse, "Does EW + CNO = Cyber?" Journal of Electronic Defense. Gainesville: September 2008. Vol. 31, Iss. 9; pp 30-35.

Chief of Naval Operations, Strategic Studies Group XXVII, Collaborate & Compel – Maritime Force Operations in the Interconnected Age, December 2008.

Chrichlow, Robert, "Whom Gods Would Destroy," Naval War College Review, Summer 2000.

Clarke, Richard, "War From Cyberspace," The National Interest, November/December 2009.

Clausewitz, Carl von, On War, Princeton University Press, Princeton, NJ, 1989.

Denning, Dorothy E. Information Warfare and Security. ACM Press, 1999.

Emery, Norman LCol, "Irregular Warfare Information Operations: Understanding the Role of People, Capabilities, and Effects," Military Review, November-December 2008, pp 27-38.

Fabey, Michael, "EW: It's Not Just for Jamming Anymore," Defense News, Gannett Co, November 7, 2005, p. 14.

Fahrenkrug, LtCol David, "Cyberspace Defined."

Fulghum, David, "Cyberwar Plans Trigger Intelligence Controversy; U.S. national intelligence agencies, military at odds over what can be attacked in computer war," Aviation Week & Space Technology. New York: January 19, 1998. Vol. 148, Iss. 3; p. 52.

Goodman, Glenn, "Neglecting Electronic Protection," Journal of Electronic Defense. Gainesville: June 2009. Vol. 32, Iss. 6; p. 18.

Goodman, Glenn, "Lethal SEAD," Journal of Electronic Defense. Gainesville: April 2009. Vol. 32, Iss. 4; pp 26-30.

Harlow, John, "Army Looks to Thwart Building Cyber Threats," ARNEWS, February 26, 2009.

Houchin, Mitch, "Commercial Broadband Wireless and EW", Journal of Electronic Defense. Gainesville: April 2006. Vol. 29, Iss. 4.

Jaboor, Kamal, "The Science and Technology of Cyber Operations," High Frontier, Vol. 5, Number 3, Air Force Space Command.

Kampmark, Binoy, "Cyber Warfare Between Estonia and Russia", Contemporary Review 289.1686, Autumn 2007.

Khalilzad, White, Strategic Appraisal: The Changing Role of Information Warfare, RAND, 1999.
Knowles, John, "Building the EW-Cyber Relationship," Journal of Electronic Defense. Gainesville: August 2009. Vol. 32, Iss. 8; p. 6.
Krekel, Bryan, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation." Northrop Grumman, October 9, 2009.
Libicki, Martin C., Cyberdeterrence and Cyberwar, RAND, 2009.
Love, Robert W., History of the U.S. Navy Vol. Two: 1942-1991, Stackpole Books, 1992.
Molander, Riddile, Wilson, Strategic Information Warfare: A New Face of War. National Defense Research Institute, 1996.
Neilson, Robert (editor), Sun Tzu and Information Warfare, National Defense University Press, Washington, D.C., 1997, p. 158.
Orr, George E., Combat Operations C3I Fundamentals and Interactions. AU Press, 1983.
Overy, Richard, Why the Allies Won, W.W. Norton & Co., 1995.
Potter, E.B., Sea Power: A Naval History, US Naval Institute, Annapolis, MD, 1981.
Ranstorp, Magnus, "The Virtual Sanctuary of Al-Qaeda and Terrorism in an Age of Globalization," Routledge, 2007.
Schleher, D. Curtis, Electronic Warfare in the Information Age. Artech House, 1999.
Shulman, Mark R., Legal Constraints on Information Warfare, Air University, March 1999.
Stallings, William, Computer Networking with Internet Protocols and Technology, Prentice Hall, 2004.
Stein, George, "Information War – Cyberwar – Netwar", September 1995.
Stein, George, "The 21st Century Air Force: An Integrating Imperative."
Thomas, Timothy, "China's Electronic Long-Range Reconnaissance," Military Review, November-December 2008.
Thomas, Timothy L. "Russian Views on Information-Based Warfare", Airpower Journal, Special Edition 1996.
Thomas, Timothy L., Cyber Silhouettes, Foreign Military Studies Office, Ft Leavenworth, KS, 2005.
Tsygichko, Vitaliy, "The Information Revolution and Information Security Problems in Russia," IO Sphere, JIOWC, San Antonio, Texas, 2008.
United Kingdom. Ministry of Defence. Joint Warfare Publication 3-80 Information Operations. June 2002.
United States. Department of the Air Force. Air Force Doctrine 2-5 Information Operations.
United States. Department of the Defense. Department of Defense Directive 3600.1 Information Operations.
United States. Department of the Defense. Department of Defense Directive 3222.4 Electronic Warfare and Command and Control Warfare Countermeasures.
United States. Joint Chiefs of Staff. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms.
United States. Joint Chiefs of Staff. Joint Publication 3-13 Information Operations [Washington, DC: Joint Chiefs of Staff: For sale by the U.S. G.P.O., Supt. of Docs.], 2006.
United States. Joint Chiefs of Staff. Joint Publication 3-51 Electronic Warfare [Washington, DC: Joint Chiefs of Staff: For sale by the U.S. G.P.O., Supt. of Docs.]
United States. Joint Chiefs of Staff. CJCSI 3210.03 Joint Electronic Warfare Policy [Washington, DC: Joint Chiefs of Staff: For sale by the U.S. G.P.O., Supt. of Docs.]

United States. Joint Chiefs of Staff. Unified Joint Task List Approved Tasks, 25 January 2009.
Wang Xuaming, 36 Strategems, Asiapac Publication, Singapore, 1992, p. 126.
Wass de Czege, Huba BGen, "Rethinking IO: Complex Operations in the Information Age," Military Review, November-December 2008, pp. 14-26.

End Notes

[1] Emery, Norman E., "Irregular Warfare Information Operations: Understanding the Role of People, Capabilities, and Effects," Military Review, November-December 2008, p. 33.
[2] Joint Publication 3-51, Joint Doctrine for Electronic Warfare, 7 April 2000, p. I-1-I-2.
[3] Joint Publication 3-13, February 13, 2006.
[4] Emery, p. 30.
[5] Neilson, Robert (editor), Sun Tzu and Information Warfare, National Defense University Press, Washington, D.C., 1997, p. 158.
[6] Fahrenkrug, David, "Cyberspace Defined," p. 1.
[7] Fahrenkrug, p. 2.
[8] Bourque, Jesse. "Why EW is not part of Cyberspace," Journal of Electronic Defense. Gainesville: September 2008. Vol. 31, Iss. 9; p. 38.
[9] Fabey, Michael, "EW: It's Not Just for Jamming Anymore," Defense News, Gannett Co, November 7, 2005, p. 14.

[10] Knowles, John. "Building the EW-Cyber Relationship," Journal of Electronic Defense. Gainesville: August 2009. Vol. 32, Iss. 8; p. 6.
[11] Stein, p. 5.
[12] JWP 3-80, p. 2-4.
[13] Orr, p. 96.
[14] Khalilzad, White, *Strategic Appraisal: The Changing Role of Information Warfare*, RAND, 1999, p. 204.
[15] Orr, p. 91.
[16] Orr, pp. 96-97.
[17] Thomas, Timothy L., *Cyber Silhouettes*, Foreign Military Studies Office, Ft Leavenworth, KS, 2005, p. 83.
[18] Libicki, p. 12.
[19] Khalilizad, White, p. 162.
[20] Stein, George, "The Twenty-first Century Air Force: an Integrating Imperative", p. 2.
[21] Ibid, p. 4.
[22] Ibid, p. 4.
[23] Chief of Naval Operations, Strategic Studies Group XXVII, *Collaborate & Compel – Maritime Force Operations in the Interconnected Age*, December 2008, p. 115.
[24] Wilson, Clay, p. 15.
[25] Wilson, Clay, pp. 7-9.
[26] Chief of Naval Operations, Strategic Studies Group XXVII, *Collaborate & Compel – Maritime Force Operations in the Interconnected Age*, December 2008, p. 115.
[27] Stein, p. 4.
[28] Jaboor, p. 14.
[29] JWP 3-80, p. 2A-2.
[30] Krekel, Bryan, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," Northrup Grumman, October 9, 2009, p. 12.
[31] Krekel, p. 12.
[32] Khalilizad, White, p. 201.
[33] Bourque, p. 38.
[34] Wentz, Barry, Starr, "Military Perspectives on Cyberpower," National Defense University, July 2009, pp. 75-76.
[35] Libicki, Martin C., *Cyberdeterrence and Cyberwar*, RAND, 2009, p. 155.
[36] Chief of Naval Operations, Strategic Studies Group XXVII, *Collaborate & Compel – Maritime Force Operations in the Interconnected Age*, December 2008, p. 69.
[37] Bourque, Jesse, "Does EW + CNO = Cyber?", Journal of Electronic Defense. Gainesville: September 2008. Vol. 31, Iss. 9; p. 32.
[38] Clarke, Richard, "War From Cyberspace," The National Interest, November/December 2009, p. 1.

[39] Stein, p. 8.
[40] Bourque, Jess. "Does EW + CNO = Cyber," Journal of Electronic Defense. Gainesville: September 2008. Vol. 31, Iss. 9, p. 30.
[41] Adams, p. 149.
[42] JWP 3-80, p. 2-6.
[43] JP 3-51, p. III-1.
[44] Krekel, Bryan, p. 7.
[45] JWP 3-80, pp. 3B-4 – 3B-5.
[46] JWP 3-80, p. 2-4.
[47] Thomas, Timothy, "China's Electronic Long-Range Reconnaissance," Military Review, November-December 2008, p. 49.
[48] Krekel, p. 23.
[49] Bourque, Jesse, p. 33.
[50] Bourque, Jesse, p. 34.
[51] Clausewitz, Carl von, p. 111.
[52] Bourque, Jesse, "Does EW + CNO = Cyber?", p. 32.
[53] JP 3-51, p. III-2.
[54] JP 3-51, p. IV-9.
[55] JP 3-51, p. B-3.
[56] Schleher, p. 4.
[57] Chief of Naval Operations, Strategic Studies Group XXVII, *Collaborate & Compel – Maritime Force Operations in the Interconnected Age*, December 2008, p. 69.
[58] Adams, James, *The Next World War*, Simon & Schuster, New York, NY, 1998, p. 150.
[59] Schleher, D. Curtis, "Electronic Warfare in the Information Age", Artech House, 1999, p. 3.
[60] Orr, p. 73.
[61] Schleher, p. 31.
[62] Nielson, Robert E. (editor), p. 158.
[63] Wentz, p. 79.
[64] Schleher, p. 28.
[65] Orr, pp. 110-111.
[66] Clarke, p. 2.
[67] Clarke, p. 2.
[68] Shulman, p. 8.
[69] Shulman, p. 6.
[70] Shulman, p. 13.
[71] Shulman, p. 16.
[72] Shulman, pp. 16-17.