REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 6 November 2007	**2. REPORT TYPE** FINAL	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE
The New Wizard War: Challenges and Opportunities for Electronic Warfare in the Information Age

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Anderson, Jon M., Lt Col, USAF

Paper Advisor (if Any): N/A

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

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
For Example: Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. 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

The emergence of distributed electronic warfare (EW) in Iraq as a response to the improvised explosive device threat has led to serious issues with electronic fratricide and frequency management. This paper assesses the roots of the information technology transformation that has benefited US adversaries in unexpected ways, and shows that the continued growth of information technology will result in spectrum management becoming necessary but insufficient for solving the electronic fratricide problem.. Finally, the paper concludes that operational commanders can alleviate the problems caused by distributed EW while effectively utilizing EW capabilities by aligning joint doctrine with new realities, ensuring planning staffs have sufficient expertise, establishing boundaries for decentralized execution, and implementing distributed EW in test, training, and exercises.

15. SUBJECT TERMS
Electronic Warfare, Network Centric Warfare, GPS, IED Jamming, Spectrum Management

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		**26**	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

THE NEW WIZARD WAR: CHALLENGES AND OPPORTUNITIES FOR ELECTRONIC WARFARE IN THE INFORMATION AGE

by

Jon M. Anderson

Lieutenant Colonel, US Air Force

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: ____________________

6 November 2007

Abstract

The New Wizard War: Challenges And Opportunities For Electronic Warfare In The Information Age

The emergence of distributed electronic warfare (EW) in Iraq as a response to the improvised explosive device threat has led to serious issues with electronic fratricide and frequency management. This paper assesses the roots of the information technology transformation that has benefited US adversaries in unexpected ways, and shows that the continued growth of information technology will result in spectrum management becoming necessary but insufficient for solving the electronic fratricide problem.. Finally, the paper concludes that operational commanders can alleviate the problems caused by distributed EW while effectively utilizing EW capabilities by aligning joint doctrine with new realities, ensuring planning staffs have sufficient expertise, establishing boundaries for decentralized execution, and implementing distributed EW in test, training, and exercises.

INTRODUCTION

> This was a secret war, whose battles were lost or won unknown to the public; and only with difficulty is it comprehended, even now, by those outside the small high scientific circles concerned. No such warfare had ever been waged by mortal men.
>
> Winston Churchill[1]

At its inception, during World War II, electronic warfare (EW) was something truly new and novel, earning inclusion in Winston Churchill's memoirs under a chapter titled "The Wizard War."[2] In many ways, the primary functions of EW in the 1940s changed little over the next 60 years; even diminishing somewhat as the information technology (IT) of the US quickly surpassed and then vastly exceeded that of its primary rival, the Soviet Union.[3] While IT transformed commerce, education, government, and even society itself, military theorists began to ponder the impacts of IT on the military, advocating and gaining support in the Department of Defense (DoD) for the transformational power of the network.

What was not expected, however, were the capabilities that IT would bring to US adversaries, even in an asymmetrical contest. Less than a year after the fall of Saddam Hussein, the improvised explosive device (IED), often triggered by radio, became the primary threat to US forces, leading to a massive deployment of EW equipment to ground forces. Although the primary strategy was to counter the IEDs, this marked a radical shift in the use of EW on the battlefield, leading to organizational changes in the Army and Marine Corps and a significant electronic fratricide problem that "polluted" the electromagnetic spectrum (EMS) in Iraq.

Although not yet fully recognized throughout DoD, EW has changed from primarily low-density, high demand capability against centralized command and control systems to high-density distributed electronic attack against radio devices that are now available worldwide. The US can no longer fully dominate the EMS. In order to deny portions of the EMS to the enemy, US forces must accept some degree of interference. Frequency managers have achieved a great deal of success in managing the spectrum, but the advent of wideband datalinks, fixed navigation signals, and overlapping frequency bands between friendly and enemy forces will result in some degree of conflict that cannot be resolved.

While technical solutions are in development that will make receivers smarter, this technology will also be available to adversaries, and may take a decade or more to reach the Warfighter. It also does not solve several underlying issues throughout DoD, such as diminishing EW expertise, lack of EW integration in joint planning, and vulnerabilities in US military IT capabilities. Ultimately, operational leadership is required to ensure objectives are met while minimizing electronic fratricide. Rather than planning using the abstract notions of cyberspace or information operations, balancing electronic warfare forces in space and time will provide the best solution to the new challenges in the electromagnetic environment.

WARFARE IN THE INFORMATION AGE

> Naval War is to Navies as Information War is to what?
>
> Martin Libicki[4]

At its core, the information age is the result of the microelectronics revolution that began with the invention of the transistor at Bell Labs in 1947.[5] Since then, the transistor has spawned new technologies every decade. In the last 50 years of the 20th Century, the United States led the world in high technology as it developed the mainframe computer, the integrated circuit, the microprocessor, the personal computer, the Internet, cellular telephony, and satellite communication.[6] Moore's Law has held up remarkably well,[7] leading to exponential growth in computing power available for cars, toasters, and cell phones. Technology, and specifically information IT, has been the primary source of economic growth in the United States, resulting in a reversal of what some analysts in the 1980s saw as the decline of American power.[8] In the first decade of the 21st Century, the world is wired, but going wireless, utilizing technology that *The Economist* called "the cross-breeding of Marconi's radio and the microprocessor."[9] The International Telecommunications Union (ITU) reported in September 2007 that there are 2.68 billion mobile phone subscribers worldwide, with 61% in developing countries.[10] The Information Age has arrived, not just in New York and Tokyo, but also in Islamabad, Bishkek , Kampala, and Managua.

For the US military, the potential of IT became apparent after the 1991 Desert Storm campaign. Although most of the technology used was cobbled together from Cold War systems, it was widely perceived as a new way of warfare by the American public, defeating third world nations with apparent ease from the air, and mopping up with a short ground war.[11] In the years that followed, in parallel with the massive shift in the business world caused by the emergence of the Internet, some military thinkers began to hail a revolution in military affairs (RMA), driven by IT. The names associated with this new way of war are familiar to any reader of military journals: "information warfare (IW)," "cyberwarfare," "netwar," "and "network-centric warfare (NCW)."[12,13,1415] Although varied in their specific focus, all of these terms are an outgrowth of IT and its fruit: rapid dissemination of information through a networked organization. A useful and broad definition for IW is "the use of information systems—computers, communications, networks, databases—for military advantage, either by the United States or by a variety of unfriendly parties."[16]

The visionaries for this information-driven RMA have predicted several implications of implementing IW concepts. Commanders will be able to utilize highly-connected dispersed forces to achieve "massed affects."[17] Information becomes a form of armor, as heavy tanks are replaced with lighter vehicles connected to the Net.[18] Hierarchical organizations can be flattened,[19] standard space and time considerations are "defied",[20] ground forces can be transformed from battalions and divisions into small "combat cells,"[21] and purely digital conflicts in cyberspace will precede, replace, or enhance physical combat operations.[22] The result of these intellectual efforts during the 1990s was a change in military thinking at the Pentagon. Secretary Donald Rumsfeld initiated an aggressive program of "transformation," largely driven by IT.[23] The Office of the Secretary of Defense developed a strategy for implementing NCW "enterprise-wide" throughout the DoD,[24] while joint Doctrine has incorporated some IW and NCW concepts in its Information Operations (IO) doctrine.[25] More recently, the US Air Force (USAF) established cyberspace as a new domain, proclaiming that the mission of the Air Force is "to fly and fight in Air, Space, and Cyberspace,"[26] while establishing Air Force Cyberspace Command to "integrate the Air Force's global kinetic and nonkinetic strike capability to support combatant commanders and to provide combat-ready forces for sustained offensive and defensive operations throughout the electromagnetic spectrum."[27]

By the time US military forces once again faced large-scale military operations in October 2001, the infant information capabilities of Desert Storm had matured into high-tech, computerized, networked forces. Fiber optic cables connected command centers at Central Command (CENTCOM) in Tampa, Florida and the Combined Air Operations Center (CAOC) in Saudi Arabia to the Pentagon and elsewhere.[28] The Global Positioning System

(GPS) had been fully operational since 1995,[29] enabling satellite-guided, all-weather munitions. In Afghanistan, Special Forces on horseback used GPS receivers to locate targets and call in airstrikes from B-52s at 20,000 ft.[30] Unmanned Predator drones allowed CENTCOM to watch the Battle of Takur Ghar in real time.[31] Operation Enduring Freedom (OEF) was widely proclaimed as the ultimate triumph of "netwar," leading one American general to proclaim that "We had accomplished in eight weeks what the Russians couldn't accomplish in ten years."[32] To the information warfare theorists, Afghanistan appeared to justify their incredible claims. As the United States prepared to invade Iraq, few foresaw that modern IT not only provided enormous capabilities for American forces, but would prove to be an equalizing force for insurgency.

THE NEW ELECTRONIC WARFARE ERA

> While making the most of advanced technology, you have to be careful that modern strategy is not influenced by what I call the Omdurman complex. You will remember that famous last cavalry charge across the desert by the soldiers of the Mahdi in 1898. The Omdurman complex consists of expecting that an army from the Third World will suddenly appear out of the desert in great numbers and charge at you in a mass in order to be mowed down by modern equipment.
>
> John Ralston Saul[33]

Eclipsed by the fantastic promises of netwar and cyberspace operations, EW was old hat by the start of Operation Iraqi Freedom (OIF), a type of warfare the US had been conducting since WWII. As a result, EW was absorbed into the grander vision of information warfare and information operations, alongside psychological operations (PSYOPS), military deception (MILDEC), operations security (OPSEC), and computer network operations (CNO).[34,35] The DoD's 2003 Information Roadmap pointed out several shortfalls in EW, noting that "DoD lacks a coherent EW vision," there exists a "disproportionate emphasis on the Suppression of Enemy Air Defense mission," and "there is no effective joint advocacy or planning for EW."[36]

While the Army had essentially abandoned EW in the 1970s,[37] the USAF also realized that its knowledge and capability had atrophied.[38] The Air Force and the Navy efforts over the past few decades have been focused on the Suppression of Enemy Air Defense (SEAD) mission, as both services worked to replace the aging EA-6B platform.[39] The EA-6B and its communications jamming counterpart, the EC-130 Compass Call, have held special status as low-density, high-demand assets,[40] establishing a long-term paradigm for EW of specialization and limited use. With the focus on the airborne SEAD mission, ground commanders had little experience with EW, and lacked doctrine, tactics, or equipment to employ it.[41] When the first radio-triggered IEDs appeared in Afghanistan in 2002, Army and Marine units had no means to counter the devices, other than a few low-power systems used by explosive ordnance disposal teams. Fortunately, the Navy had a warehouse full of obsolete jammers originally designed for ship defense. Known as Acorn, over 2000 were eventually deployed to Afghanistan, and were largely effective,[42] although 50% of all combat casualties in Afghanistan have been attributed to IEDs.[43]

In Iraq, however, the scale of the threat, as well as the ingenuity of the insurgents, proved to be far more problematic. Over 60% of casualties in Iraq have been caused by IEDs, including 1800 or more combat deaths.[44] The Iraqi insurgents used a variety of techniques to detonate the bombs, including trip wires, timers, radio, and infrared devices.[45] In some regions, 70% of IEDs were radio-triggered;[46] using car key fobs, radio-controlled toys, and other wireless technology.[47] Defeating IEDs became CENTCOM's top priority. In response to the CENTCOM Commander's call for a "Manhattan Project-like approach"[48] to counter IEDs, the Pentagon initiated an anti-IED task force in the fall of 2003, which by 2007 had become a DoD agency with a $4.4 billion budget – the Joint Improvised Explosive Device Defeat Organization (JIEDDO).[49] Technology efforts funded by JIEDDO include a stoichiometric diagnostic device (chemical analyzer), radio frequency (RF) neutralizers, IED detectors, and laser-based explosive detectors.[50] But the most ubiquitous countermeasure deployed to Iraq has been the RF jammer. To date, JIEDDO has funded over 30,000 jammers for Iraq and Afghanistan, each costing $60,000 to $80,000.[51]

The operational objective for the widespread use of IED jammers was to "put them back on the wire," forcing insurgents to use mechanical triggers that would be simpler to detect.[52] This strategy appeared to be succeeding, reducing radio-controlled bombs to 10% of all IEDs in Iraq, although the overall number of attacks has not diminished.[53] Even so, JIEDDO claims that, with capabilities employed to the field, roughly half of all IEDs are detected and cleared by coalition forces.[54]

Although IT has profoundly enhanced American military power, it has also served as a "great equalizer."[55] Insurgents in Iraq often implemented NCW more effectively than coalition forces,[56] utilizing the Internet, pagers, cell phones, and other modern technology in very effective ways. With the loss of copper and fiber telephone lines during and after the 2003 invasion, 27 million Iraqis relied on wireless technology for communication,[57] enabling ad-hoc cell phone command and control networks, flat organization structures, and salvaged electronics from commercial devices to remotely control bombs. Like the insurgency itself, digital exploitation by a guerilla force was unexpected, just as the lessons learned from the past on the effectiveness of "low-tech avoidance"[58] had to be relearned.

Iraq's target-rich electronic environment raised the status of EW.[59] The success of IED jammers has not gone unnoticed by the Army, which reversed its 30 years of EW abandonment to stand up an EW doctrine center and create a cadre of EW operators.[60] Likewise the Marine Corps revisited its EW vision, transforming from platform-centric jamming to distributed capability.[61] US Strategic Command (USSTRATCOM) recently established the Joint Electronic Warfare Center as part of the Joint Information Operations Center (JIOC) to integrate and prioritize EW among the services. The JIOC commander stated that "I want to grow in EW."[62] But even as every soldier became an EW operator, the already crowded RF spectrum in Iraq, and especially in Baghdad, became "electronically polluted," creating a new host of problems for coalition forces.[63]

MILITARY SPECTRUM MANAGEMENT IN THE INFORMATION AGE

> One of the greatest challenges of the war has been managing the RF Spectrum.
>
> Gen (ret) John Abizaid[64]

The electromagnetic spectrum, normally depicted in charts such as Figure 1, leaves many with the impression that it is a physical space where signals interact.[65] In reality, the EMS is a conceptual tool used to avoid radio frequency interference between systems and users.[66] However, electromagnetic waves do not interact in space; rather, electronic warfare interference occurs inside radio receiver electronics.[67] In other words, jamming, whether intentional or unintentional, attacks receivers, not signals. Although information operations and cyberspace are useful constructs, another way to look at the type of tactical EW seen in Iraq is as a physical non-kinetic attack on the enemy's weapon system or command and control network.

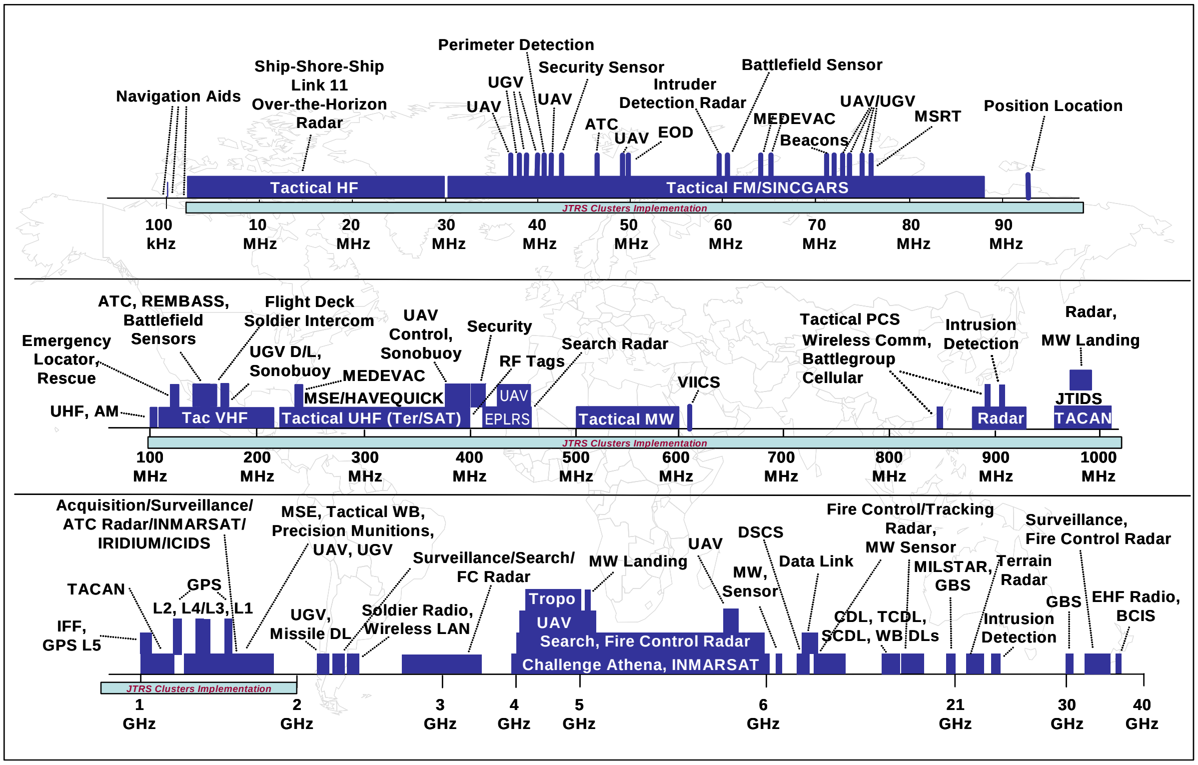

Figure 1. Warfighter Spectrum Use Below 40 GHz. (Badri Younes, "Spectrum Transformation: Acceleration," Presented to National Spectrum Managers Association 2006 Conference, May 17, 2006)

As Figure 1 illustrates, the EMS is heavily "occupied" by military systems in a Joint Operations Area (JOA). Each Geographic Combat Commander (GCC) is tasked by Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3320.01B to "establish a standing frequency management structure that includes a Joint Frequency Management Office (JFMO)."[68] At the Joint Task Force (JTF) level, spectrum may be managed by a JTF Spectrum Management Element (JSME).[69] Additionally, the JTF may establish an Electronic Warfare Coordination Cell (EWCC) to support EW planning and policies in the JOA.[70] The primary tool used to manage spectrum in the JOA is the Joint Restricted Frequency List (JFRL), which lists the networks and frequencies deemed critical to JTF objective.[71]

As IED jammers proliferated in Iraq, “electronic fratricide”[72] became a new issue for frequency managers to tackle. The jammers often prevented the soldiers operating them from using their tactical radios, and impacted other communications and surveillance systems as well.[73] Jamming degraded datalinks on Unmanned Aerial Vehicles (UAVs) such as the Predator.[74] In many cases, soldiers turned off the jammers to keep communication channels open.[75] The problem was made worse by the use of EC-130 and EA-6B aircraft to clear convoy routes, which increased the interference due to wider propagation of jamming signals.[76,77]

The Multinational Force – Iraq (MNF-I) was ill-equipped to handle the challenges of electronic fratricide. When the problems began, there was no EWCC,[78] and EW expertise was lacking at the headquarters.[79] EW was excluded from the joint planning process, a situation which was corrected with the establishment of an EWCC in Iraq in late 2005.[80] As CENTCOM and the MNF-I adjusted planning processes, some of the shortcomings of the available tools became apparent, leading the Office of the Secretary of Defense (OSD) to create a new organization to seek better technology solutions for spectrum management.

In the Spring of 2006, the DoD’s chief information officer combined the Defense Spectrum Office and the Joint Spectrum Center to form the Defense Spectrum Organization (DSO).[81] The long-term strategy for DSO is to develop a new spectrum management tool called the Global Electromagnetic Spectrum Information System (GEMSIS), while incrementally improving the current joint spectrum management tool, Spectrum XXI.[82] DSO is also looking toward “emerging technologies such as software-defined radio and cognitive radio” to enable dynamic spectrum access.[83]

ANALYSIS AND RECOMMENDATIONS

> "Safe to say, adversaries will figure out ways to blunt the U.S. informational advantage. From Operation Anaconda in Afghanistan to numerous misadventures in Iraq, they already have."
>
> Max Boot[84]

Prior to OIF, electronic fratricide caused by EW was largely manageable. With SEAD as the primary mission, a large percent of electronic attack occurred early in the campaign, often far away from the bulk of coalition forces, and at frequencies known from signals intelligence. The IED threat introduced a new problem: enemy use of *unknown* frequencies, sometimes overlapping frequencies used by coalition forces, and *geographically collocated or intermixed* with friendly units. As wireless technology continues to proliferate, other conditions are likely to emerge, including known, fixed frequencies used by both enemy and friendly forces (e.g. GPS), signals that require very large bandwidths (e.g. ultrawideband), deliberate enemy use of friendly frequency bands, and enemy use of civilian communication systems (e.g. cell phones and wireless data networks). Even though technologies such as software-defined radio may help with the problem, the troubles experienced by the Joint Tactical Radio System (JTRS) indicate that technical solutions will be costly and take years to deploy,[85] and similar technology may be available to adversaries as well.

Satellite navigation is a particularly interesting case, because it is a significant force enhancement capability globally, is a dual-use system, and uses wideband signals that are relatively easy to jam. In many ways, the history of GPS blue-force denial is the opposite of the IED story. The immediate need to counter IEDs due to significant casualty rates led to rapid development and employment of EW capability to defeat the threat: 30,000 jammers deployed in less than four years. With GPS, however, presidential and congressional direction to develop a capability to deny hostile use of GPS (beginning in 1996)[86,87] resulted in almost no operational planning or deployment of GPS denial capability. The primary reason for this is the overlap of GPS civil and military frequencies. An aggressive effort to modernize GPS is underway, which will provide frequency separation,[88] however such an effort will take decades, as modernized receivers replace legacy GPS equipment. Meanwhile, use of GPS by adversaries has not materialized as a real threat, and the DoD awaits the technical solution.

Frequency management is a necessary task. Even without EW, deconfliction is required to ensure avoidable interference is managed. However, the enemy does not partake of the deconfliction process. As demonstrated in Iraq, an underground insurgency can ingeniously exploit information technology. Even the great powers understand the implications of using the same frequencies as the US to avoid EW or gain some other strategic advantage. The European Union (EU) originally attempted to overlay a signal for their Galileo satellite navigation system directly on the new GPS military frequencies.[89] Although the US and the EU resolved the dispute, China has recently applied the same strategy against both the EU and the US.[90]

Regarding IEDs, Deputy Secretary of Defense Gordon England stated that “It’s a hard problem. There is no solution, just better ways of dealing with it. You keep mitigating as much as you can, but at the end of the day, it’s warfare.”[91] While not yet approaching the complexity of the IED threat, a similar sentiment applies to electronic fratricide caused by EW. Although one strategy is to merely avoid EW altogether, this assumes that EW does not provide an essential capability. Such was not the case with IEDs. Although jamming was employed tactically, the net effect was to achieve an operational objective: reduce casualties in the JOA caused by the primary insurgent weapon. The joint operational community can achieve balance between electronic fratricide and operational objectives by taking several key steps.

First, with the significant shift in EW capability and application, it is time to rethink joint EW doctrine. A new version of JP 3-13.1, published in January 2007, does not reflect the emergence of distributed EW. Although doctrinally considered part of IO, integrating EW with CNO, PSYOP, MILDEC, and OPSEC may only apply to certain operations. In IED suppression, EW has primarily been used for command and control warfare and force protection. As one analyst warned over ten years ago, "information is not likely to be an appropriate integrating principle, either strategically or organizationally… instead, 'information warfare' needs to be broken down into its various components, and those need to be integrated effectively into the full range of military operations."[92] Perhaps the neglect of EW during the 1990s can be attributed to its incorporation into IW and IO, while its resurgence has been driven by the tactical need to counter a physical command link between a bomber and his bomb. Likewise, including EW in a cyberspace construct may be meaningless to the soldier with a jammer mounted on his vehicle. Jamming is a five-dimensional physical phenomenon that can be controlled in frequency, space and time. The current emphasis on frequency management mirrors the civilian world of spectrum management, where interference cannot be tolerated. Rather than seeking to provide a high quality of service such as is expected from commercial service providers, the use of EW, and the negative impact on friendly forces, should be balanced against objectives.

Second, EW needs to be "demystified" at all levels of warfare, just as the Army endeavors to demystify it in their tactical training.[93] EW is widely perceived as a "black art," impenetrable to outsiders due to both security classification and its technical nature.[94] The complexity of the computer models used to determine EW effects and potential electronic fratricide also tend to put EW in the hands of specialists. Much of the technical expertise supporting the GCCs has resided in the Joint Spectrum Center (now part of DSO), disconnecting EW knowledge and operational planning. Each GCC should have an organic EW team who can advise the Combatant Commander (COCOM) on the capabilities and limitations of EW, with equivalent support provided to the JTF Commander, if required.

Third, although JP 3-13.1 states that EW is "centrally planned and directed and decentrally executed,"[95] the implications of widely distributed EW need to be carefully analyzed. NCW has tended to lead to "increased centralization on all levels."[96] A tactical commander well-trained in EW and operating under "task-oriented command and control" should be able to respond more quickly to a situation requiring jamming than waiting for permission from headquarters to jam, or eliminating the option due to higher headquarters direction.[97]

On the other hand, the operational commander must have sufficient control to balance political and strategic issues associated with spectrum, including impact on civilians, coalition partners, and safety-of-life services. Some have proposed implementing a "frequency tasking order (FTO)"[98] similar to the air tasking order (ATO), but this would result in even greater centralization then exists today. Although airborne EW often affects large areas, lower-power ground-based jammers have more limited range, due to both radiated power and terrain masking. Operational commanders may be able to establish rules of engagement (ROEs) for tactical commanders that define the acceptable operational envelope for EW. With sufficient EW knowledge at both the operational and tactical levels, the detrimental effects can be minimized in both space and time while giving tactical commanders the freedom to utilize EW capability.

Finally, EW needs to be incorporated into joint test, training, and exercises, preparing forces for operating under conditions where communication, navigation, or sensor equipment may be temporarily lost. A short-term loss of GPS could result in a UAV crash, or worse. Such vulnerability needs to be remedied, since an enemy jammer could create the same effect. The loss of tactical voice communications for 1 hour or longer should be planned for, with soldiers able to accomplish the mission when connectivity is lost. Joint exercises will also illuminate interoperability issues between the Services and among land, sea, and air components.

CONCLUSION

EW has changed, for better or worse. Although the superiority of American IT is unquestionable, the prophets of IW did not foresee the equalizing effect of commercial IT and the subsequent need for electronic countermeasures. The rapid push to deploy EW to Iraq complicated the precarious balance of spectrum use employed by frequency managers in the theater.

Enemy spectrum, is by definition, a jamming target, and should be off-limits for friendly forces, if possible. But increasingly, there is a lack of “clear” spectrum as wideband signals provide an increasingly larger number of digital bits per second. Clever adversaries may exploit US dependence on information networks by deliberately overlapping US spectrum use or utilizing civil spectrum deemed untouchable to US forces.

While some technologies may help in the long-term, the use of the EMS is an operational problem, with operational solutions. Effective planning, preparation, and leadership is the best approach to employing EW in the modern age.

NOTES

1. Reginald V. Jones, *The Wizard War* (New York: Coward, McCann & Geoghegan, 1978): xix.
2. Ibid.
3. Max Boot, *War Made New* (New York: Gotham Books, 2006): 430.
4. Martin C. Libicki, *What Is Information Warfare?* (Washington DC: National Defense University, Center for Advanced Concepts and Technology, 1995): 91.
5. Max Boot, *War Made New*, 309.
6. Ibid., 308-317.
7. Ibid., 313.
8. Ibid., 316.
9. "When everything connects; The coming wireless revolution," *The Economist* 383, No. 8526 (April 28, 2007): 12.
10. "Global Trends in Telecommunications," ITU News Magazine 07, No. 8, http://www.itu.int/itunews/manager/display.asp?lang=en&year=2007&issue=07&ipage=Telecom-trends&ext=html (accessed 4 Nov 07).
11. James Adams, *The Next World War* (New York: Simon & Schuster, 1998): 50-51.
12. Glenn Buchan, *Information War and the Air Force: Wave of the Future? Current Fad?* (Santa Monica, CA: RAND Corporation, 1996): 2.
13. John Arquilla and David Ronfeldt, "A New Epoch—And Spectrum—Of Conflict," Edited by John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND Corporation, 1997):4.
14. Ryan Henry and C. Edward Peartree, "Military Theory and Information Warfare," *Parameters* XXVIII, No. 3 (Autumn 1998): 129-130.
15. Chris Wu, "An Overview of Research and Development in China," *Cyberwar, Netwar, and the Revolution in Military Affairs*, Edited by Edward Halpin, et. al. (New York: Palgrave MacMillan, 2006): 176.
16. Bruce D. Berkowitz, "Warfare in the Information Age.," Edited by John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND Corporation, 1997):175.
17. Jeffrey R. Cares, "An Information Age Combat Model," http://www.alidade.net/recent_research/IACM.pdf (accessed 3 Oct 07): 1.
18. David Talbot, "How Technology Failed in Iraq," *Technology Review*, http://www.technologyreview.com/Infotech/13893/ (accessed 30 Oct 07).
19. John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica, CA: RAND Corporation, 1996): 9.
20. Ibid., 13.
21. Ryan Henry and C. Edward Peartree, "Military Theory and Information Warfare," 130.
22. Ibid., 130-131.

23. John Terino, “Information Technology Driving Transformation, DOD Official Says,” *Aerospace Daily* 201, no. 15 (Jan 23, 2002): 3.
24. Director, Force Transformation, Office of the Secretary of Defense, “Network-Centric Warfare: Creating a Decisive Warfighting Advantage,” http://www.oft.osd.mil/library/library_files/document_318_NCW_GateFold-Pages.pdf (accessed 30 Oct 07).
25. Joint Pub 3-13, *Information Operations*, 13 Feb 06, I-2.
26. Michael W. Wynne, “Flying and Fighting in Cyberspace,” XXI, no. 1 (Spring 2007):6.
27. Henry S. Kenyon, “Cyberspace Command Logs In,” *Signal* 61, no. 12 (Aug 2007): 35.
28. Max Boot, *War Made New*, 363.
29. “Global Positioning System Fully Operational,” http://www.navcen.uscg.gov/gps/geninfo/global.htm (accessed 5 Nov 07).
30. Max Boot, *War Made New*, 354-355.
31. Noah Schachtman, “Taking Aim at Military Technology,” http://www.wired.com/science/discoveries/news/2003/03/58107 (accessed 29 Oct 07).
32. Max Boot, *War Made New*, 382.
33. John Ralston Saul, “A New Era of Irregular Warfare?,” *Canadian Military Journal* 5, No 4 (Winter 2004-2005): 11.
34. Martin C. Libicki, *What Is Information Warfare?*, 27.
35. Joint Pub 3-13, *Information Operations*, ix.
36. Department of Defense Information Operations Roadmap, 30 October 2003: 59-60.
37. Stephen Trimble, “US Army Moves Back Into Electronic Attack Mission,” *Jane’s Defence Weekly* http://www8.janes.com/Search/documentView.do?docId=/content1/janesdata/mags/jdw/history/jdw2007/jdw32060.htm@current&pageSelected=allJanes&keyword=us%20army%20moves%20electronic%20attack&backPath=http://search.janes.com/Search&Prod_Name=JDW& (accessed 22 Oct 07).
38. David A. Fulghum and Robert Wall, “E-War Rediscovered,” *Aviation Week & Space Technology* 161, no. 10 (September 13, 2004): 29.
39. John A. Tirpak, “Where Next With Electronic Attack?,” *Air Force Magazine* 89, no. 10 (October 2006): 30-31.
40. Ibid., 33.
41. Brian Peña, “Under the Umbrella,” *Marine Corps Gazette* 91, no. 5 (May 2007): 22.
42. Rick Atkinson, “Left of Boom: The Struggle to Defeat Roadside Bombs (Part 1: The IED Appears),” *Washington Post*, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/29/AR2007092900751.html (accessed 23 Oct 07).
43. Clay Wilson, “Improvised Explosive Devices (IEDs) in Iraq and Afghanistan: Effects and Countermeasures,” *Congressional Research Service Report for Congress* (Washington DC: Library of Congress, August 28, 2007): CRS-1.
44. Ibid.
45. Stew Magnuson, “Adaptive Foe Thwarts Counter-IED Efforts,” *National Defense*, January 2006 http://www.nationaldefensemagazine.org/issues/2006/jan/adaptive_foe.htm (accessed 25 Oct 07).

46. Rick Atkinson, "Left of Boom: The Struggle to Defeat Roadside Bombs (Part 4: Moving Left of Boom)," *Washington Post*, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/29/AR2007092900751.html (accessed 23 Oct 07).
47. Rick Atkinson, "Left of Boom: The Struggle to Defeat Roadside Bombs (Part 1: The IED Appears)."
48. Ibid.
49. Noah Shachtman, "Pentagon Bomb Squad a Dud?," http://blog.wired.com/defense/2007/03/in_the_fall_of_.html (accessed 5 Nov 07).
50. 50 Clay Wilson, "Improvised Explosive Devices (IEDs) in Iraq and Afghanistan: Effects and Countermeasures," CRS-4.
51. Nathan Hodge, "US Military Looks to 'Offensive' Focus in Counter-IED Fight," http://www8.janes.com/Search/documentView.do?docId=/content1/janesdata/mags/jdw/history/jdw2007/jdw32885.htm@current&pageSelected=allJanes&keyword=hodge%20counter-IED&backPath=http://search.janes.com/Search&Prod_Name=JDW& (accessed 22 Oct 07).
52. Rick Atkinson, "Left of Boom: The Struggle to Defeat Roadside Bombs (Part 4: Moving Left of Boom)."
53. Ibid.
54. Nathan Hodge, "US Military Looks to 'Offensive' Focus in Counter-IED Fight."
55. Max Boot, "The Paradox of Military Technology," *The New Atlantis* 14 (Fall 2006): 14.
56. Dawn S. Onley, "Critics Take Shots at Net-Centric Warfare Planning," *Government Computer News* (February 2, 2005), http://www.gcn.com/online/vol1_no1/34963-1.html?topic=daily-updates (accessed 30 Oct 07).
57. Rick Atkinson, "Left of Boom: The Struggle to Defeat Roadside Bombs (Part 4: Moving Left of Boom)."
58. John Ralston Saul, "A New Era of Irregular Warfare?,": 11.
59. Martin C. Libicki, *What Is Information Warfare?*, 31.
60. Stephen Trimble, "US Army Moves Back Into Electronic Attack Mission."
61. Richard R. Burgess, "Jamming: The Marine Corps Refines Its Vision of Electronic Warfare," *Sea Power* 50, no. 12 (June 2007): 22.
62. "Infowarriors," C4ISR Journal (October 4, 2006), http://integrator.hanscom.af.mil/2006/October/10122006/10122006-18.htm (accessed 29 Oct 07).
63. David A. Fulghum, "Technology Will Be the Key to Iraq Buildup," *Aviation Week & Space Technology* 166, no. 3 (January 15, 2007): 412.
64. Joint Staff (J6), Spectrum Fact Sheet, http://www.jcs.mil/j6/c4campaignplan/spectrum_fact_sheet.pdf (accessed 4 Oct 07).
65. Kevin Werbach, "Open Spectrum: The New Wireless Paradigm," *Spectrum Series Working Paper #6* (October 2002), http://werbach.com/docs/new_wireless_paradigm.htm (accessed 29 Oct 07).
66. Michael W. Schneider, *Electromagnetic Spectrum Domination: 21st Century Center of Gravity or Achilles Heel?*(Fort Leavenworth, KS: US Army Command and General Staff College, 1994): 23-25.
67. Kevin Werbach, "Open Spectrum: The New Wireless Paradigm."
68. CJCSM 3320.01B, 25 March 2006, B-1.

69. Ibid., A-5.
70. Joint Pub 3-13.1, *Electronic Warfare*, 25 January 2007, II-4,5.
71. Ibid., III-1.
72. Ibid., IV-6.
73. David Fulghum, "Iraq's Electromagnetic Environment is Polluted," *Aviation Week & Space Technology* (November 7, 2005), http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=awst&id=news/11075p2.xml (accessed 29 Oct 07).
74. David A. Fulghum, "Technology Will Be the Key to Iraq Buildup," 167.
75. Rick Atkinson, "Left of Boom: The Struggle to Defeat Roadside Bombs (Part 4: Moving Left of Boom)."
76. David Fulghum, "Iraq's Electromagnetic Environment is Polluted."
77. Arthur F. Huber, Gary Carlberg, Prince Gilliard, and L. David Marquet, "Deconflicting Electronic Warfare in Joint Operations," *Joint Force Quarterly* 45 (2nd Quarter 2007): 90.
78. David Fulghum, "Iraq's Electromagnetic Environment is Polluted."
79. Arthur F. Huber, Gary Carlberg, Prince Gilliard, and L. David Marquet, "Deconflicting Electronic Warfare in Joint Operations," 93.
80. "US 'Needs to Do Better' with EW Assets," *Jane's Defence Weekly* (November 02, 2005), http://www8.janes.com/Search/documentView.do?docId=/content1/janesdata/mags/jdw/history/jdw2005/jdw12448.htm@current&pageSelected=allJanes&keyword=better%20ew%20assets&backPath=http://search.janes.com/Search&Prod_Name=JDW& (accessed 22 Oct 07).
81. Maryann Lawlor, "Organization Targets Bandwidth Battles," *Signal* 61, no. 8 (April 2007): 47.
82. Ibid., 48.
83. Paige Atkins, "Spectrum of Transformation," *Military Technology Online Edition* (May 1, 2007), http://www.military-information-technology.com/article.cfm?DocID=2022 (accessed 22 Oct 07).
84. Max Boot, *War Made New*, 429.
85. Greg Green, "JTRS: Impossible Dream, or Just an Expensive One?," http://www.defensenews.com/story.php?F=1193244&C=thisweek (accessed 6 Nov 07).
86. TITLE 10 U.S.C., Subtitle A, PART IV, CHAPTER 136, § 2281, http://www4.law.cornell.edu/uscode/html/uscode10/usc_sec_10_00002281----000-notes.html (accessed 6 Nov 07).
87. US SPACE-BASED POSITIONING, NAVIGATION, AND TIMING POLICY, December 15, 2004, http://pnt.gov/policy/ (accessed 6 Nov 07).
88. Brian Barker, et al, "Overview of the GPS M-Code Signal," http://www.mitre.org/work/tech_papers/tech_papers_00/betz_overview/betz_overview.pdf (accessed 6 Nov 07).
89. "EU, US Split over Galileo M-Code Overlay," *GPS World*, http://www.gpsworld.com/gpsworld/Business+News+&+Outlook/GPS-Inside---December-2002/ArticleStandard/Article/detail/42304 (accessed 6 Nov 07).
90. "Compass: And China's GNSS Makes Four," *Inside GNSS*, http://www.insidegnss.com/node/115 (accessed 6 Nov 07).

91. Rick Atkinson, “Left of Boom: The Struggle to Defeat Roadside Bombs (Part 4: Moving Left of Boom).”
92. Glenn Buchan, *Information War and the Air Force: Wave of the Future? Current Fad?*, 12.
93. Glenn Goodman, “Interview: Col Lauri Moe Buckhout,” *Journal of Electronic Defense* 30, no. 6 (Jun 2007): 46.
94. Ibid.
95. JP 3-13.1, III-1.
96. Milan N. Vego, “Command and Control in the Information Age,” *Joint Force Quarterly* 35 (Autumn 2004): 100.
97. Ibid., 105.
98. Arthur F. Huber, Gary Carlberg, Prince Gilliard, and L. David Marquet, “Deconflicting Electronic Warfare in Joint Operations,” 92.

BIBLIOGRAPHY

Anon. "Infowarriors," C4ISR Journal (October 4, 2006), http://integrator.hanscom.af.mil/2006/October/10122006/10122006-18.htm (accessed 29 Oct 07).

Anon. "US 'Needs to Do Better' with EW Assets," *Jane's Defence Weekly* (November 02, 2005), http://www8.janes.com/Search/documentView.do?docId=/content1/janesdata/mags/jdw/history/jdw2005/jdw12448.htm@current&pageSelected=allJanes&keyword=better%20ew%20assets&backPath=http://search.janes.com/Search&Prod_Name=JDW& (accessed 22 Oct 07).

Anon. "When everything connects; The coming wireless revolution," *The Economist* 383, No. 8526 (April 28, 2007): 12.

Adams, James. *The Next World War.* New York: Simon & Schuster, 1998.

Arquilla, John and Ronfeldt, David., editors. *In Athena's Camp: Preparing for Conflict in the Information Age.* Santa Monica, CA: RAND Corporation, 1997.
Goodman, Glenn. "Interview: Col Lauri Moe Buckhout," *Journal of Electronic Defense* 30, no. 6 (Jun 2007): 46.

Arquilla, John and Ronfeldt, David. *The Advent of Netwar.* Santa Monica, CA: RAND Corporation, 1996.

Atkins, Paige. "Spectrum of Transformation," *Military Technology Online Edition* (May 1, 2007), http://www.military-information-technology.com/article.cfm?DocID=2022 (accessed 22 Oct 07).

Atkinson, Rick. "Left of Boom: The Struggle to Defeat Roadside Bombs (Part 1: The IED Appears)," *Washington Post*, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/29/AR2007092900751.html (accessed 23 Oct 07).

Atkinson, Rick. "Left of Boom: The Struggle to Defeat Roadside Bombs (Part 4: Moving Left of Boom)," *Washington Post*, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/29/AR2007092900751.html (accessed 23 Oct 07).
(accessed 30 Oct 07).

Boot, Max. *War Made New*. New York: Gotham Books, 2006.

Buchan, Glenn. *Information War and the Air Force: Wave of the Future? Current Fad?* Santa Monica, CA: RAND Corporation, 1996.

Department of Defense Information Operations Roadmap, 30 October 2003: 59-60.

Fulghum, David A. and Wall, Robert. "E-War Rediscovered," *Aviation Week & Space Technology* 161, no. 10 (September 13, 2004): 29.

Fulghum, David. "Iraq's Electromagnetic Environment is Polluted," *Aviation Week & Space Technology* (November 7, 2005), http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=awst&id=news/11075p2.xml (accessed 29 Oct 07).

Fulghum, David A. "Technology Will Be the Key to Iraq Buildup," *Aviation Week & Space Technology* 166, no. 3 (January 15, 2007): 412.

Henry, Ryan and Peartree, C. Edward. "Military Theory and Information Warfare," *Parameters* XXVIII, No. 3 (Autumn 1998): 121-135.

Huber, Arthur F. et al. "Deconflicting Electronic Warfare in Joint Operations," *Joint Force Quarterly* 45 (2nd Quarter 2007): 90-95..

Joint Pub 3-13, *Information Operations*, 13 Feb 06, I-2.

Jones, Reginald V. *The Wizard War*. New York: Coward, McCann & Geoghegan, 1978.

Lawlor, Maryann. "Organization Targets Bandwidth Battles," *Signal* 61, no. 8 (April 2007): 47-51.

Libicki, Martin C. *What Is Information Warfare?* Washington DC: National Defense University, Center for Advanced Concepts and Technology, 1995..

Magnuson, Stew. "Adaptive Foe Thwarts Counter-IED Efforts," *National Defense*, January 2006 http://www.nationaldefensemagazine.org/issues/2006/jan/adaptive_foe.htm (accessed 25 Oct 07).

Peña, Brian. "Under the Umbrella," *Marine Corps Gazette* 91, no. 5 (May 2007): 22.

Schachtman, Noah. "Taking Aim at Military Technology," http://www.wired.com/science/discoveries/news/2003/03/58107 (accessed 29 Oct 07).

Saul, John Ralston. "A New Era of Irregular Warfare?," *Canadian Military Journal* 5, No 4 (Winter 2004-2005): 7-20.
Schneider, Michael W. *Electromagnetic Spectrum Domination: 21st Century Center of Gravity or Achilles Heel?* Fort Leavenworth, KS: US Army Command and General Staff College, 1994.

Talbot, David. "How Technology Failed in Iraq," *Technology Review*, http://www.technologyreview.com/Infotech/13893/ (accessed 30 Oct 07).

Terino, John. "Information Technology Driving Transformation, DOD Official Says," *Aerospace Daily* 201, no. 15 (Jan 23, 2002): 3.

Tirpak, John A. "Where Next With Electronic Attack?," *Air Force Magazine* 89, no. 10 (October 2006): 30-31.

Trimble, Stephen. "US Army Moves Back Into Electronic Attack Mission," *Jane's Defence Weekly*
http://www8.janes.com/Search/documentView.do?docId=/content1/janesdata/mags/jdw/history/jdw2007/jdw32060.htm@current&pageSelected=allJanes&keyword=us%20army%20moves%20electronic%20attack&backPath=http://search.janes.com/Search&Prod_Name=JDW&
(accessed 22 Oct 07).

US SPACE-BASED POSITIONING, NAVIGATION, AND TIMING POLICY, December 15, 2004, http://pnt.gov/policy/ (accessed 6 Nov 07).
http://www.mitre.org/work/tech_papers/tech_papers_00/betz_overview/betz_overview.pdf
(accessed 6 Nov 07).

Vego, Milan N. "Command and Control in the Information Age," *Joint Force Quarterly* 35 (Autumn 2004): 100-107.

Werbach, Kevin. "Open Spectrum: The New Wireless Paradigm," *Spectrum Series Working Paper #6* (October 2002), http://werbach.com/docs/new_wireless_paradigm.htm (accessed 29 Oct 07).

Wilson, Clay. "Improvised Explosive Devices (IEDs) in Iraq and Afghanistan: Effects and Countermeasures," *Congressional Research Service Report for Congress* (Washington DC: Library of Congress, August 28, 2007): CRS-1.

Wu, Chris. "An Overview of Research and Development in China," *Cyberwar, Netwar, and the Revolution in Military Affairs*, Edited by Edward Halpin, et. al. New York: Palgrave MacMillan, 2006.

Wynne, Michael W. "Flying and Fighting in Cyberspace," *Air and Space Power Journal* XXI, no. 1 (Spring 2007):6.