Maneuvering Room - Electromagnetic Spectrum Dominance and National Security

The most important resource in U.S. national security may also be its most vulnerable – and taken for granted. "Want to fly a drone? Get directions from the Global Positioning System? Drop a smart bomb? Use radar to land your plane, communicate with a forward operating base on a mountaintop in Afghanistan, find an improvised explosive device or, better yet, detonate one? Then you'll need access to the electromagnetic spectrum."[1]

The electromagnetic spectrum (EMS) is the range of all possible frequencies of electromagnetic radiation. It's a quantitatively continuous spectrum of frequencies and wavelengths, including radio waves, microwaves, gamma, xray, and infrared. Virtually every technology used today needs to access and exploit the EMS, from cellular to WiFi to advanced military weaponry. Likewise, the electromagnetic spectrum is a maneuver space that transcends all operational domains - air, space, land, sea and cyber.

The EMS is a tricky resource. The exponential growth of modern conveniences, communications, and technologies has crowded the spectrum, making access the biggest challenge. The greatest competition for spectrum access today comes from the global wireless broadband industry as it tries to meet the growing consumer demand for mobility and data. The Department of Defense's (DoD) *2013 Electromagnetic Spectrum Strategy: A Call to Action* aims to balance access management and the development of capabilities in a shared access environment. Implementation will require new regulatory and policy initiatives. Existing technologies will have to be adapted to new spectrum requirements, while advanced electromagnetic spectrum systems still need a unifying architecture.

Meanwhile, American security strategic paradigms, like cross domain dominance and air sea battle, or capabilities, such as drones and cyber attacks, are at the mercy of the EMS. "[EMS] access is a prerequisite for modern military operations. DoD's growing requirements to gather, analyze, and share information rapidly; to control an increasing number of automated Intelligence, Surveillance, and Reconnaissance (ISR) assets; to command geographically dispersed and mobile forces to gain access into denied areas; and to "train as we fight" requires that DoD maintain sufficient spectrum access. Additionally, adversaries are aggressively developing and fielding electronic attack (EA) and cyberspace technologies that significantly reduce the ability of DoD to access the spectrum and conduct military operations."[2]

The complex technological requirements and bureaucratic demands created by spectrum management are a considerable challenge that others are already meeting head on. Russia's recent ability to disconnect Ukrainian forces in Crimea from their command and control confirmed two disconcerting facts: the dexterity of Russia's cyber warfare capabilities and that the U.S. was no longer the only country capable of doing this non-kinetically. Russia has been making progress in this area for some time. Their cyber attack on Estonia in 2007 paralyzed the country's entire Internet infrastructure, affecting the websites of Estonian banks, ministries, newspapers, broadcasters, and Parliament. At its worst, bank cards and mobile-phone networks were temporarily frozen. In July 2008, Georgian

[1] Patrick Tucker, "How the Army Plans to Fight a War Across the Electromagnetic Spectrum," *DefenseOne*, February 26, 2014, http://www.defenseone.com/technology/2014/02/inside-armys-first-field-manual-cyber-electromagnetic-war/79498/.
[2] "Electromagnetic Spectrum Strategy 2013; A Call to Action," *Department of Defense,* February 20, 2014, http://www.defense.gov/news/dodspectrumstrategy.pdf.

websites, including the pages of the president, the parliament, the foreign ministry, news agencies and banks, were attacked by Russian viruses weeks before Russia's military operations in South Ossetia.

The most active player in the EMS, however, is China. "It is China's capabilities for non-kinetic combat, its potential to 'develop capabilities to dominate in the electromagnetic spectrum,' which …could be 'game-changing,'" warned the former Deputy Chief of Naval Operations for Information Dominance in 2011.[3] The driving force in Chinese military strategy is about gaining leverage and the EMS is no exception. "China is aggressively pursuing a strategy focused on attacking and denying an adversary's use of networks, electronics, and information systems while protecting their own systems."[4] On the anti-access/area denial side, geo-positioning systems (GPS) are a prime example. The Air Force is training pilots how to fly without GPS, radar and radio communications, while the Navy is testing an antenna to reconnect drones with GPS satellites after being jammed. Meanwhile, China is taking preventative action by completing work on its own 35-satellite navigation system called Compass by 2020.[5]

Recognizing China's growing ambitions, the U.S. has been planning an Asia pivot for some time. The operational challenges have been well-documented, from the region's sheer size (mostly ocean) to the dependence on regional allies for a physical presence. Such challenges are magnified by the importance of spectrum access. "China is well aware that the Pacific Pivot will strain the US military's ability to protect its networks against electromagnetic sabotage. The People's Liberation Army is thus pumping tremendous resources into beefing up its spectrum-warfare operations, much as it has funded the formation of an elite hacker corps to wage cyberwar against its rivals."[6] China's commercialization of its spectrum technologies will also allow potential adversaries around the world greater leverage against the U.S. "If and when the U.S. military is pulled into future missions in the steppes of East Africa or the forests of Central America, it may run into opponents armed with jammers that were manufactured in greater Shanghai. And if our military gets bogged down in those conflicts because it can't dominate the spectrum to its liking, the Pacific Pivot will become significantly harder to pull off – much to China's joy."[7]

China may be the U.S.' greatest competitor in the electromagnetic spectrum, but other countries and actors are just as willing to compete. "The reality today is that the spectrum is a very busy place in wartime, and an adversary will migrate to whichever segment the U.S. is not controlling and exploit that vulnerability to their advantage."[8] It has become clear that control of their operating space –the electromagnetic spectrum – is fundamental to any national security planning. "Command of the electromagnetic spectrum has come to be regarded as a crucial advantage in modern combat, in much the same way that command of the sea and command of the air are."[9] In today's asymmetric threat environment, maneuvering room across the electromagnetic spectrum can't be taken for granted. Dominating in the spectrum must be a national priority.

---

[3] Robert Haddick, "Forget about China's missiles and stealth fighter; worry instead about 'non-kinetic' combat," *Small Wars Journal*, January 19, 2011, http://smallwarsjournal.com/blog/forget-about-chinas-missiles-and-stealth-fighter-worry-instead-about-non-kinetic-combat.

[4] "Electronic Warfare, The Changing Face of Combat," Association of Old Crows, May 24, 2011, http://www.myaoc.org/EWEB/images/aoc_library/Government_Affairs/AOC%20report.pdf.

[5] Brenden Koerner, "Inside the New Arms Race to Control Bandwidth on the Battlefield," *Wired*, February 18, 2014, http://www.wired.com/threatlevel/2014/02/spectrum-warfare/.

[6] Koerner, op.cit.

[7] Ibid.

[8] "Electronic Warfare, The Changing Face of Combat," op.cit.

[9] Loren Thompson, "Raytheon Prevails Again in Jammer Contest," *Forbes*, January 24, 2014, http://www.forbes.com/sites/lorenthompson/2014/01/24/raytheon-prevails-again-in-jammer-contest/.