by John Knowles

WHY TWO DOMAINS ARE BETTER THAN ONE

In recent weeks, the long-running discussion regarding exactly how the electromagnetic (EM) and cyber environments relate to each other has come back to the forefront with several voices calling for what appears to be the establishment of a single Cyber-EM environment.

The most prominent of these was Chief of Naval Operations ADM Jonathan Greenert. Building on his earlier articles about the Cyber and EM environments published in Naval Institute's *Proceedings* magazine, Admiral Greenert contributed an op-ed piece for *AOL Defense* titled, "Wireless Cyberwar, the EM Spectrum, and the Changing Navy." He followed up what has been an exceptional effort to raise awareness of the EM environment by citing some excellent examples of the Navy's growing dependence on the EMS, the need to "improve our awareness of the EM and cyber environments," and the Navy's desire to "employ agility in the EM spectrum and cyberspace."

However, the concept at play seemed to be one of EM and cyber as a single environment. "With wireless routers or satellites part of almost every computer network, cyberspace and the EM spectrum now form one continuous environment," Greenert wrote.

As current events further push EM and cyber concerns forward, the number of voices calling for their consideration as one environment has grown. Though it appears to make sense on the surface, deeper consideration of the DOD's broad operational responsibilities in the electromagnetic spectrum (EMS) make a combined Cyber-EM domain something that should be reconsidered before the Navy or any Service goes too far down that path.

UNDERSTANDING THE EM-CYBER RELATIONSHIP

Recent discussion has focused on an important concept – the evolving relationship between the cyber environment and the EM environment. (If you want, you can substitute the word "domain" for "environment," as *JED* often does.) But what is frequently described as a single Cyber-EM environment is really two separate environments – the cyber environment and the EM environment. To understand why this is true, it is worth taking a closer look at the characteristics of the cyber and EM environments.

Cyberspace, according to the DOD's Joint Publication 3-12, is "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems and embedded processors and controllers." This means that cyberspace is not a natural physical environment. Cyberspace comprises man-made technologies and forms a portion of the information environment. This makes cyberspace very different from the EM environment.

The EM environment is a natural physical maneuver space that we visualize through the concept of the EM Spectrum (EMS). In this sense, the EM environment is like the Air, Land, Sea and Space domains. As a natural physical maneuver space, the EM environment (or operationally speaking, the EM Domain) cannot "merge" with another environment any more than the Air and Sea domains can converge to form a single Air-Sea environment or the Space and Cyber domains can converge to form a Space-Cyber environment. It just doesn't work that way.

CONVERGENCE – A POWERFUL BUT MISAPPLIED TERM

In technology-heavy disciplines like electronic warfare (EW) and cyber operations, it is tempting to cite technology-related examples as evidence of a continuous Cyber-EM environment. There are numerous EM systems (jammers, radars and communications systems) that are networked via cyberspace. Cyber systems are also increasingly using the EMS via wireless networks. This trend is a type of technological convergence. (Many argue that "technological convergence" isn't even the correct term for this trend and that "technology sharing" is a more accurate description.) The problem arises when we try to extend the significance of this trend beyond technology and argue that the cyber and EM environments are converging.

First of all, technology does not determine or define a natural physical maneuver space like the EM environment. The EM environment has existed from the moment of the Big Bang which is certainly long before humans began exploiting it for radio communications, radar, GPS, etc. Whatever tools the DOD uses to maneuver within the EM environment, those technologies do not define the environment. The same rule is true for the information environment, of which cyberspace forms a part. More importantly, there is no relationship between EM and cyber technological convergence and convergence between the EM and cyber *environments*. Just as technology cannot define a domain, technological convergence cannot drive domain convergence.

When technological convergence has occurred in the past, it has not

driven convergence between warfighting domains because physical environments cannot converge. Did the development of the aircraft carrier in the last century mean the naval and air environments were converging because we were flying planes from ships? Obviously not. Even though military aviation was a relatively new idea at the time, the Air and Sea domains were understood well enough for military leaders to know that the two could not form one continuous Air-Sea environment just because of technological innovation.

Or try looking at the putative Cyber-EM convergence theory in another way. If we take the cyber and EM technologies out of the equation, is the term "convergence" a good description of the Cyber-EM relationship? It is worth noting that no one in the DOD was arguing that the cyber and EM environments formed one continuous environment until after wireless data communications and software-defined radars and radios started to appear in the battlespace.

CYBER SYSTEMS ARE BECOMING MORE DEPENDENT ON THE EMS

If cyber and EM convergence isn't really what is happening, then what *is* happening between cyberspace and the EM environment? To answer that question, let's look at some historical examples in naval warfare.

During the early part of the last century, we began developing technologies that enabled our weapons systems to exploit the EM environment. In naval warfare, for example, ships began using radios before World War II. Then radars came into use. In the 1950's, we developed RF- and IR-guided missiles. Soon afterward, we developed electronic warfare systems to detect and defeat RF- and IR-guided anti-ship missiles. Ships then began to use satellites for navigation, weapons targeting and data communications. IFF systems evolved, too. What was happening was simple: ships – and by extension, naval warfare – was becoming more dependent on the EM environment. Yet no one was arguing that the naval environment was "converging" with the EM environment.

For the past 100 years, the same trends have been emerging in other warfighting environments. Air warfare has become dependent on the EM environment. Land warfare has become dependent on the EM environment. Space operations are extremely dependent on the EM environment. Throughout this period of growing EM dependence, no DOD leader has characterized this trend as "convergence" or called for a single Air-EM environment or Space-EM domain.

Now, let's look at cyber warfare. Over the past decade, cyber networks have become increasingly dependent on access to the EM environment, as they evolved from "wired" to "wireless" architectures. Like the other warfighting environments, this EM dependence is the true essence of the Cyber-EM relationship. It is worth noting here that while cyber operations are becoming more dependent on access to the EM environment, the opposite is not true. Most of the systems and devices that use the EM environment, as well as the EW systems that provide EM control,

are not inherently dependent on cyberspace. Whether or not an EM system has access to cyberspace, that access does not enable their ability to maneuver in the EM environment.

From an EM environment perspective, cyber systems reside strictly in the "data transport" layer. Even potential or prospective cyber attacks delivered by RF jammers are essentially performing a communications function – delivering software code into a victim system – as opposed to a jamming function. For the most part, cyber systems are simply EMS "users" (just like radars, radios and GPS receivers), because data networks need access to the EM environment to move information around the battlespace. Their increasing use of the EM environment does not constitute convergence. Rather it demonstrates EM dependence, which is the true nature of the Cyber-EMS relationship.

The reason many in the DOD do not understand this relationship is because the DOD has spent the past 20 years building a network-centric fighting force. This focus on net-centricity has skewed much of the DOD's thinking around computers and networks to the point that cyber technologies have been endowed with significance well beyond their true importance. It is time to return to a more rational understanding of maneuver space, operational responsibilities, mission and technology with regard to the EM environment and the cyber environment.

THE NEED FOR AN EM STRATEGY

Over the years, *JED* authors, such as John Clifford, Jesse "Judge" Bourque, Col Jeff Fischer and others, have explained why the DOD needs to understand that the EM environment is a unique maneuver space upon which all of the other warfighting domains – Air, Land, Sea, Space and Cyberspace – depend.

The EM environment is vast, and the DOD must maintain operational responsibility for all of the parts it needs to use, manage and control. The DOD cannot afford to build most of its EM strategy around those small portions of the EM environment that support cyber-centric or network-centric operations while pushing the vast majority of its EM responsibilities to the outer edges of this strategy. Instead the DOD needs a strategic focus that covers the whole EM environment all of the time because it is using ever larger portions of this EM maneuver space. As the US Army discovered when Iraqi insurgents began using radio-controlled improvised explosive devices (RCIEDs), an adversary will always seek to exploit areas of the EM environment where the DOD yields operational control.

The best way to prevent this from happening again and again in the future is for the DOD to recognize that it needs a comprehensive strategy for the EM environment – one that integrates EM use, EM management and EM control. Many of the "piece-parts" needed for this strategy already exist. Some areas, such as EM management and electronic warfare, are even beginning to coordinate more effectively. This is a step in the right direction. But the DOD needs to do a lot more, and the first step is to recognize that it needs a better strategy for the EM environment.