SYNESIS
A JOURNAL OF SCIENCE, TECHNOLOGY, ETHICS, AND POLICY

The cyberspace paradox

Matthew Labert[1]
1. Federal Executive Fellow, Potomac Institute for Policy Studies, 901 N. Stuart Rd, Arlington, VA, 22203, USA.
Email: mlabert@potomacinstitute.org

Abstract

Cyberspace has recently found itself at the center of attention, but at what cost or to what benefit? In a time of fast-paced cyberspace development in doctrine and of commands, one must not lose focus of the holistic view of the existing information environment. This article uses Joint doctrine, to define cyberspace in the lexicon of Joint terminology, and suggests broadening the cyberspace strategy debate to incorporate the larger information environment. As a result, this article suggests that cyberspace be treated as part, albeit a large one, of the larger information environment. Furthermore, too much emphasis solely on cyberspace overshadows other information effects and areas of influence in the information environment.

The idea of the information environment is neither new nor limited to a certain strategy. In fact, there are examples of military strategies that successfully combine all aspects of the information environment, including cyberspace, into a coherent information warfare strategy. The United States currently has both the doctrine and the ability to engage in information warfare. However, because of its present fascination with cyberspace the United States is rewriting, or in some cases rejecting outright, its current information strategy. The cyberspace paradox thusly becomes how to develop a holistic strategy for the entire information environment that includes and incorporates the evolving and prominent domain of cyberspace.

Key words: cyberspace, information environment, information operations, information warfare, electronic warfare

"Cyberspace" is very much in vogue, but exactly what is cyberspace and how does it affect our military strategy? In spite of the current popularity of cyberspace, its definition and limits remain obscure and foreign. With its numerous complexities, how does one develop a cyberspace strategy?

Existing military doctrine grounds this discussion and establishes an authoritative source upon which to build. Joint Pub 1-02, the Department of Defense (DOD) dictionary of military terms, defines cyberspace as a "…global domain *within* [emphasis mine] the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."(1). Although some may take issue with this definition, it is nonetheless the fundamental source on which subsequent strategy is established.

If cyberspace is a global domain within the information environment, what then is the *information environment*? Joint Pub 1-02 defines the information environment as "…the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."(1). Clearly, from its definition one can imagine that the information environment is very broad and much larger than cyberspace alone. Subsequently, also by its definition, the scope of cyberspace is bounded and limited within the information environment and "information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." (1).

Convergence

To further understand cyberspace's current popularity, one must also briefly examine the phenomenon of convergence. As already suggested, the information environ-

ment is vast as it contains essentially everything that can collect, process, disseminate, or act on information. However, how does a user avail themselves to the enormity of all that is contained within the information environment? The answer is via technology. Thanks to the current and pervasive trend of technology, users are able to navigate the vast amounts of data through an "interdependent network of information technology infrastructures" (i.e., cyberspace) (1).

Cyberspace is popular because today's technology allows the user to access and operate within the information environment like never before. As more and more information is digitized, it becomes more readily available via technology. The more users utilize the technology to access information, the more users demand simpler technology. "Simpler" often refers to fewer technology systems/devices—yet more data from those systems—readily available. In this case, fewer distinct technologies imply that a user can now have access to many types of diverse sets of information via one authoritative system (i.e., the internet). Convergence, therefore, is the idea of creating data efficiencies by integrating technologies and data into something "easier" for the user to assimilate. Users continue to discover linkages and efficiencies the more they combine dissimilar information, which consequently increases their demand for additional convergences.

One can then further develop the idea of convergence via the cyberspace domain. Cyberspace, via ever-converging technologies, certainly enhances our ability for collecting, processing, and disseminating information, but now it also makes possible the acting-on of information. The establishment of common protocols (e.g., internet protocol (IP)), enables data sharing across disparate technologies, which consequentially also allows command and control of those same technologies. Thus, via the technology of cyberspace, a user truly has a single device that allows for the accessing, monitoring, and controlling of all aspects of information across an ever-growing environment.

A military strategy

How do cyberspace and the information environment affect military strategy? There is a current effort to adopt a strategy that capitalizes on the information environment known as "informationization." Informationization is an ongoing effort to develop a fully networked architecture capable of coordinating military operations throughout all warfare domains (typically land, air, sea, and space) as well as across the electromagnetic spectrum. To guide this new effort, a new doctrine called "Local War Under Informationized Conditions" advocates for the development of an advanced [Information Warfare] IW capability (2). The stated goal of this doctrine is to "establish control of an adversary's information flow and maintain dominance in the battle space."(2). This doctrinal focus is providing the impetus for Information Dominance as both a desired effect against an adversary and a means for achieving overall success.

To build upon this strategy even further, it is clear that cyberspace—or more correctly, the integration of cyberspace with other components of information warfare—is vital. For example, an offensive action using this strategy would seamlessly integrate the offensive capabilities of cyberspace (e.g., computer network attack) and the electromagnetic spectrum (e.g., jamming) into a coordinated action. Furthermore, this strategy known as "Integrated Network Electronic Warfare" (INEW) would be coordinated via a single governing authority at the highest levels of command, facilitating its complete integration into the overall operational plan (2).

This combination of information warfare capabilities allows for an offensive capability against an adversary's command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) networks and other essential information systems (i.e., across the information environment)(2). As such, the entire military spectrum of doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) are being realigned to support this revolutionary information warfare.

The cyberspace paradox

Many United States experts recognize the strategy, referenced in the section above, as a fundamental shift in warfare, however this is the crux of the cyberspace paradox. What is the problem? The Informationization strategy and its subsequent doctrine is not that of the United States, but actually that of the People's Republic of China. In contrast to China's holistic informationization-strategy, the United States has chosen to concentrate its strategy on the primacy of cyberspace. It is because of this motivation that cyberspace truly gains its current popularity. Cyberspace has recently been elevated to its own warfare domain, equal to that of land, sea, space, and air. Unlike its sister domains, cyberspace was deemed critical enough

to stand up a new 4-star level command to be responsible for all aspects of cyberspace operations (i.e., network attack, exploit, and defense). Moreover, changes to the entire DOTMLPF have been fast-tracked in support of this cyber-centric focus. Furthermore, the very foundation of doctrine, cyber-terminology, is being re-defined in an effort to keep up with these monumental changes.

This is not to suggest that the United States does not have other information warfare capabilities. Quite the contrary, the United States has numerous strategies and doctrines that pertain to information, such as Joint Pub 3-13 *Information Operations* and Joint Pub 3-13.1 *Electronic Warfare* and their respective DOTMLPF-support structures. However, with the current laser-like focus on cyberspace and development of new cyberspace doctrine, one more layer of bureaucracy has just been added to this already-complex information structure.

It is also not being suggesting that the United States must mirror the strategy of an opponent, as clearly, this is dangerous and undesirable. However, without understanding the holistic view of information warfare, such as our opponents, the U.S. faces being surprised and overwhelmed (e.g., U.S. network defense may prevent against a network attack, but would be of little value against an electronic attack under the People's Republic of China INEW strategy).

Not all is lost however, nor is it difficult to adjust to compensate. Cyberspace is certainly a large part of the information environment, so the current focus on cyberspace does have its benefits. The convergence of technologies and subsequent availability of data, via cyberspace, certainly makes the mastery of cyberspace a critical component when considering affecting the information environment. However, data and its usage do not exist exclusively in cyberspace. Therefore, the benefits gained from cyberspace cease being beneficial when the emphasis on cyberspace detracts from the larger analysis of the information environment.

Although information warfare is not defined in Joint Pub 1-02, information superiority (what one would strive to achieve in information warfare) is, in fact defined as "[t]he operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."(1). The definition then continues by referencing "information operations." Information operations is then defined as "[t]he integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own."(1). Clearly, these sounds very similar to the Chinese strategy described above, so instead of a *concentration* on cyberspace, why not broaden the attention to the *integration* of cyberspace?

Cyberspace and its associated terminology need not be re-defined, but certainly modernized to account for an increased understanding of the information environment. In fact, the Vice Chairman of the Joint Chiefs of Staff promulgated a memorandum with updated cyber-definitions. However, instead of integrating themselves into the larger information environment, the terminology does the opposite and tries to incorporate other information-ideas into cyberspace. Joint Pub 3-13 *Information Operations* states that its primary purpose is "…ensure all of the capabilities comprising IO [information operations] are effectively coordinated and integrated into our nation's warfighting capability against current and future threats."(3). One must define cyberspace terminology in its proper context within established doctrine.

Joint Pub 3-13 also states that United States Strategic Command (USSTRATCOM) is the 4-star level command with specific authority and responsibility to coordinate information operations, including cyberspace (3). There is little doubt that cyberspace is critical, as a 4-star level command, United States Cyber Command (USCYBERCOM), was recently created to manage it. The establishment of CYBERCOM, even as a subordinate to STRATCOM, created a new layer of bureaucracy between cyberspace and the other facets of the information environment. The creation of CYBERCOM is not bad in and of itself, however, both senior and subordinate staffs must make a concentrated effort to make sure their efforts are coordinated across the information spectrum.

Likewise, the Military Services already have specialty organizations in different aspects of information operations (e.g., Army–PSYOP/CA, Navy-EW, etc.) as delineated by their service-specific missions. Furthermore, these organizations are already designated as functional commands in support of USSTRATCOM. However, with the emphasis on cyberspace and the subsequent stand-up of USCYBERCOM, the Services are quickly creating/realigning

cyber organizations. Again, cyber organizations are not undesirable in and of themselves, but those organizations should strengthen the existing information organizational structure vice creating new ones. In fact, if the existing information-DOTMLPF structure and Service mission areas currently support this organization, why make radical changes simply to accommodate a modified cyberspace?

The intent of this article is not to suggest that cyberspace is not important, nor that the emphasis of cyberspace is not worthwhile. The goal is to advocate that it is even more significant to focus on cyberspaces within the larger context of the information environment. If cyberspace is as critical as current emphasis suggests, yet cannot remain integrated into the existing information environment, then perhaps the entire information-DOTMLPF is flawed. However, by simply viewing cyberspace within its proper place—within the information environment—attention will necessarily shift to a much broader view of cyberspace integration. Instead of creating new seams and gaps with new layers of bureaucracy and support structure, efforts should be concentrated on creating efficiencies in the existing structures and doctrine. Are we ready to place all of our information warfare eggs into the cyber basket? Does the old adage "as cyberspace goes, so goes the information war" still hold true?

Disclosures

The views expressed in this article are those of the author and do not necessarily represent the official policy or position of the Department of the Navy, Department of Defense, or the U.S. Government.

Competing interest

The author declares that he has no competing interests.

References

1. Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms. (2001(As Amended Through April 2010))
2. Krekel, B. (October 9, 2009). Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation. McLean, VA: Northrop Grumman Corporation Information Systems Sector.
3. Joint Pub 3-13: Information Operations. (13 February 2006). xvi