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

The Newest Warfighting Domain: Cyberspace

Sean Brandes [1]

1. LCDR, U.S. Navy, OPNAV (N2N6) Navy Pentagon Washington DC 20350-2000, US,
Email: sean.brandes@gmail.com.

Abstract

Cyberspace is a global commons not that unlike the oceans air or space. Debatably, these commons have seen the US military's superiority challenged over the last decade. Yet while the US arguably still maintains military advantage in land, air, sea, and space, it is the newly minted domain of cyberspace which potentially threatens to undermine these domains as they become increasingly interconnected and dependent on cyberspace technology. Thus, as the US military continues to work with international allies to leverage "Information as Warfare", the importance of this global common intensifies. A review of operational doctrine is warranted in order to ensure that cyberspace is treated on par with the traditional domains. This paper reviews current cyberspace operations strategy and policy, cyberspace environment characteristics, and current operational integration and intelligence support methodologies to determine if significant changes are required to further the effective utilization, integration and exploitation of cyberspace. Essentially, with minor modifications, current principles and doctrine that are applied to traditional intelligence efforts to support kinetic warfare may be employed for cyberspace operations to produce the desired battlespace effects. However, other significant challenges to cyberspace integration concerning cultural barriers, tactics and procedures, and personnel training and retention also need to be appreciated and considered.

Keywords: cyberspace, doctrine, warfighting, strategy, cybertechnology, intelligence

Cyberspace is a global commons not that unlike the oceans, air or space. Debatably, over the last decade all of these commons have seen the United States' superiority challenged. Yet, while the US arguably maintains military advantage in land, air, sea, and space, it is this newly recognized operational domain of cyberspace that potentially threatens to undermine this dominance. As cyberspace transcends traditional military warfare areas, boundaries between cyberspace and these other domains are evaporating. Cyberspace occurs in a realm located simultaneously at logical and physical layers that intersects activities in, through and concerning the electromagnetic spectrum, seamlessly crossing into other domains as well as geographic and recognized political boundaries. Consequently, this implies a union between the traditional warfare domains and cyberspace. Is the US military (and its international allies) ready for this union? Is this newest operational domain postured for success? Lastly, are there extra-military consequences of the US government posing cyberspace to be a viable battlespace? It is important to address potential unintended consequences of defining and declaring cyberspace an operational domain with respect to international collaboration and cooperation. While this paper will predominantly argue the merits of cyberspace as an operational domain, recognition of cyberspace as a global common requires acknowledgement

of potential problems that this might incur. However, due to the nascence of cyberspace as an operational domain, and its widespread growth and viability, it is prudent to examine how best to integrate, support and mature this domain.

Often, new technology is employed prior to the establishment of national policy, comprehensive governance and sound tactics, techniques and procedures which invariably limit operational impacts and complicates supporting efforts. Cyberspace is certainly not new, nor is it apt to call cyberspace a singular technological advancement, yet cyberspace is creating new challenges for the US, its military, Intelligence Community (IC) and its international allies as it permeates as it permeates unabated across all warfare areas. Information in cyberspace is discovered, processed, exploited and disseminated at unprecedented speed and volume, presenting unique challenges for military operations and the intelligence professional. This continuously evolving domain changes how conflicts are viewed and what intelligence support is required to enable operations. Cyberspace is already essential to today's military environment and is a critical component to any operational success. Estonia, Georgia, Stuxnet and Shamoon were highly publicized wake-up calls on how cyberspace can be exploited for political and military purposes.[i] As such, there is a rapidly developing awareness to fully leverage the IC's capabilities to address this growing and dynamic domain.

To date, several different doctrinal, strategy and policy documents address the cyberspace environment, both in terms of national security and military priority.[ii] However, a 2013 Government Accountability Office report claimed "there is no single document that comprehensively defines the nation's cybersecurity strategy. Instead, various documents developed over the span of more than a decade have contributed to the national strategy, often revising priorities due to changing circumstances or assigning new responsibilities to various organizations."(2) Cyberspace strategies have been promulgated for years, yet the last three years have seen the most comprehensive efforts to date to quantify and leverage cyberspace. In 2011, the Department of Defense (DoD) released its strategy for operating in cyberspace. Comprised of five strategic initiatives, the long awaited "Department of Defense Strategy for Operating in Cyberspace" was high-level and primarily defensive in nature (3). The key tenets of this strategy are that: 1) cyberspace is an *operational* domain; 2) new defense operating concepts will be employed to protect DoD systems; 3) a "whole of government" cybersecurity strategy will be enabled; 4) efforts will be made to strengthen collective cybersecurity with international partners and allies; and 5) United States' ingenuity should be leveraged through training and innovation. Of significance, the first tenet was the first time cyberspace was noted as an operational domain. At the time, the Deputy Secretary of Defense William Lynn said that there are "concerns that cyberspace is at risk of being militarized... We have designed our DoD Cyber Strategy to address this concern."(4) He further stated this strategy involved an "emphasis on cyber defenses" – as opposed to offense or retaliation–that was meant to illustrate DoD's commitment "to protecting the peaceful use of cyberspace (4). Indeed, establishing robust cyber defenses no more militarizes cyberspace than having a navy militarizes the ocean."(4) However, this same strategy establishes that cyberspace will be treated as an operational domain on par with the operational domains of land, air, sea and space. Those traditional domains have long-established doctrine, strategy, and policy that guide operations. Such governance is still evolving for cyberspace.

Cyberspace is a ubiquitous yet often subjectively defined term that is used today to describe various aspects of the globally connected information technology infrastructure. Even a cursory search of the extant literature reveals volumes of work discussing the implications of cyberspace; and depending on the author's target audience, the variations of cyberspace characterizations are usually just as diverse. Military leadership generally views cyberspace differently than does other government organizations, private industry or academia. This difference is magnified as one considers these same institutions on an international scale. Even within the military, depending on whether the main focus is on protecting and providing network services, or exploiting internet vulnerabilities for intelligence purposes, finding a universally accepted definition of cyberspace is complicated. The Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms definition states that cyberspace is a "domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." (5) This definition makes no mention of operational domain or warfare and is suited primarily to the traditional world of those charged with operating and maintaining the networks. However, the Joint Staff recognized the need to standardize existing Joint termi-

nology to further the development of "cyberspace as a warfighting domain" and circulated a Joint cyber operations lexicon (6). This lexicon characterized cyberspace operations as "employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the DoDIN [DoD Networks]." (6, p. 8) This definition still centers on maintaining networks, however, it prompted additional amplification(s) in the operational domain. At present, cyberspace may be viewed in a greater context than simply providing access to data and information; cyberspace may now also be manipulated to *achieve objectives*. Joint Publication 3-13 elaborates on the "computer network operations" aspect by stating that cyberspace operations can be used to "deny or manipulate adversary or potential adversary decision making through targeting an information medium, the message itself, or a cyber-persona." (7) This shift from appreciating cyberspace as largely the information exchange networks which need to be maintained and protected (albeit still a critical component) to understanding that cyberspace is also an operational domain that requires planning consideration and coordination on par with the traditional domains is key. As Stuxnet and Shamoon demonstrated, the cyberspace domain is capable of producing direct physical/kinetic effects.

Current DoD strategy makes no mention of cyberspace as an operational *warfare* domain. Yet, in an October 2012 speech, Secretary of Defense (SECDEF) Leon Panetta essentially declared that the US would take pre-emptive action against would-be cyber attackers (8). He also called the internet a new terrain for warfare (8). These comments may mean that the US now views cyberspace operational warfare as fair game, provided the identity of the attacker is known. In 2012, Congress approved a law which allows the DoD to conduct offensive cyber operations in response to cyber attacks on the US provided that the cyberspace operations are aligned with the rules of conventional warfare.[iii] This provision means that the rules of the international Law of Armed Conflict and the US War Powers Resolution (which requires the President to gain Congressional approval within 90 days of entering into a war) must be followed. In September 2012, the State Department elaborated on the US position, explaining that some cyberspace attacks could constitute a prohibited use of force and therefore require a military response, stating "The United States government believes that cyber attacks can amount to armed attacks, and are subject to international humanitarian law and rules of war."(10) United States' doctrine, policy and rules of engagement (ROE) offer distinctions between cyberspace exploitation and attacks; however the owners of the networks upon which such transgressions are occurring may have a very different view. Even with SECDEF Panetta's assertion that attribution techniques have recently and significantly improved, attribution with confidence has long been the Achilles heel of responding to cyberspace attacks (8). As true in traditional warfare domains, ROE dictate that a valid and lawful military target requires a degree of distinctive identification and characterization be conducted during a targeting cycle. Given the technological complexities inherent to cyberspace, intelligence professionals are challenged to provide the necessary target fidelity. Attacking the wrong target in cyberspace may result in significant negative second- and third-order consequences far outside the intended target battlespace. Due to the interconnected nature of cyberspace, an attack on an improperly identified target could result in an unexpected and unmerited counterattack or may run unbridled into other networks and wreck havoc in the civilian sector. This is a major concern and inevitable point of contention as the US government advances their potential militarization of space in the eyes of domestic and foreign cyber actors.

Whether or not an overarching, encompassing national strategy is required, or is even in the best interest of the nation, remains subject to debate. Although doctrine exists, much of it predates the current cyberspace environment complexities (1). At one time, there were 13 different documents across DOD, Agency, Service and COCOM levels outlining cyberspace operations (1). The gaps in doctrine and strategy indicate that the development and employment of cyberspace and cyberwarfare has outpaced current thinking about cyberspace. Current DoD cyberspace definitions can be programmatic (which make them limiting) and difficult to comprehend. For example, "cyberspace" is defined, while other domains such as land and sea are not (5). There is no definition of "land operations" or "maritime operations," since these are generally assumed to be military operations occurring within these respective domains (5). However, recent organizational changes have allowed government and military organizations to better govern, protect and exploit cyberspace. The most obvious illustration of this progress is US Cyber Command (CYBERCOM). The physical manifestation of recent DoD strategy and policy maturation commenced with the establishment of CYBERCOM in 2009. CYBERCOM is synchronizing and facilitating cyberspace operations among the Services and Combat-

ant Commands (COCOM). Prior to the development of CYBERCOM, approaches to cyberspace operations were scattered throughout the different services and government agencies. Currently, while CYBERCOM is a sub-unified command subordinate to US Strategic Command, conventional wisdom suggests it is only a matter of time before it will be elevated to a fully functioning COCOM (1). The last two SECDEFs considered removing CYBERCOM from US Strategic Command and making it a unified COCOM, putting CYBERCOM on equal footing with the six regional COCOMs and the functional unified commands in charge of special operations, nuclear deterrence operations and global transportation. Many military leaders believe the move would make sense, cementing cyber warfare as a focal point of the DoD's national security responsibilities (1). Today, CYBERCOM is charged with ensuring clear operational lanes are maintained in and through cyberspace. This command is responsible for establishing command and control doctrine for operating in cyberspace, developing situational awareness in cyberspace, and authoring the required policies and standing ROE. CYBERCOM is also establishing a Cyber Mission Force consisting of a Cyber National Mission Force (CNMF), Cyber Combat Mission Force (CCMF) and Cyber Protection Platoons (CPP). The CNMF is primarily concerned with US defense and will deny and/or stop adversaries from attacking the nation's critical infrastructure. CCMF will provide support to the COCOMs, to include target development in support of operations and war plans. Lastly, the CPP will be entrusted to harden the DoD networks. These forces began operations in September 2013 and expect to be fully operational by September 2015. In line with CYBERCOMs assessments that cyberspace is a contested domain and its networks are a warfighting area, General Keith Alexander, US Army, commander of CYBERCOM and Director of the National Security Agency, said the role of the national mission force is not solely a defensive team, but would have offensive capabilities that would be deployed if the nation was attacked in cyberspace.[iv]

The emergence of cyberspace operations is evident by these actions, yet specific challenges, issues, and solutions to fighting in cyberspace while synchronizing land, sea, air, and space operations remain embryonic. Cyberspace nuances, such as attribution, distinguishing between a cyber attack and cyber exploitation, ROE ambiguities, and the nature of cyberspace targets and targeting add complexity to operational integration. Table 1 presents some other differences and similarities between the cyber domain, and those of land, air, sea and space. In these traditional domains, I posit relatively few adversaries are competent enough to effectively threaten or challenge the US military. In contrast, the cyberspace domain is crowded with actors (such as China and Iran) capable of pressuring, confronting, or intimidating the US, its allies, and each other. The evolving cyberspace domain has changed the way conflict is viewed, and the nature of operational integration, and the intensity of the intelligence support needed. Thus, a clearer definition and understanding of cyberspace operational capabilities and strategies should assist the leadership to better understand the type of intelligence support which is required and drive collection strategies and priorities. The extent to which the cyberspace domain differs from the traditional kinetic domains represents a paradigm shift in modern military (and political) affairs and highlights challenges for commanders' to apply current rules of engagement, policy, and military doctrine. Characteristics such as a distributed and dynamic construct, inherent ambiguity, a compressed "speed of net" timeline, and the potentially global effects of cyberspace activity need to be considered in the context of intelligence support to cyberspace operations.

Conclusion

The comprehensiveness and effectiveness of recent cyber-operational efforts may be disputed, yet what is clear is that cyberspace is now recognized as a vital component of the military and national security environment and agenda (11). There is the need to transform military culture, away from predominately kinetic operations, and reluctance to engage cyberspace operations, to one that understands cyberspace's criticality and embraces opportunities for cyberspace integration. There is a growing recognition among senior military leadership that the cyberspace domain should not be dealt with in isolation; rather, cyberspace needs to be viewed on par with kinetic operations. This indoctrination has already begun at the service academy and service college levels and should be instituted across all milestone/command training endeavors. Within the DoD, leadership should be more willing to trade kinetic weapons in order to more actively plan

Table 1. List of Characteristics Comparing Cyber Domain vs. Traditional Warfare Domains.

Characteristic	Cyberspace Domain	Traditional Domains
Resources	• Inexpensive relative US air, land and sea • Human capital-driven	• Limited to nations with significant financial resources • Industrial-based assets
Physical	• Artificial construct, permeable virtual boundaries • Multi-use environment (government, military, commercial) • Distributed, dynamic and non-linear	• Exists naturally, discrete physical boundaries • Multi-use environment (government, military, commercial)
Actors	• Ambiguous • From nation-states to individuals to criminal organizations to commercial entities	• Identity of adversary usually known
Effects	• Global in nature • Non-Kinetic or Kinetic • Collateral damage on 2nd/3rd order effects potentially global	• Usually regionally focused (Space is exception) • Usually Kinetic (EW exception) • Collateral damage limited to active battlespace
Authorities for Offensive Action	• Elevated • Evolving ROE	• Local • Establish ROE
Intelligence Support	• Requires knowledge of adversary capabilities and intent • Compressed timeline (“net” speed) • Attribution is challenging	• Requires knowledge of adversary capabilities and intent

and conduct operations in cyberspace. One need only consider today’s austere budget climate and observe that the cyberspace mission continues to see its coffers increase as evidence of cyberspace’s growing importance and staying power.

Military leaders should also appreciate that cyberspace operations may require cooperative relationships with members of other government organizations and private industry, especially as future military operations will most likely occur in environments that involve more than US participants and military entities. This is a key fact because just as the US military declares cyberspace an operational domain does not mean others will follow suit, nor should they. This declaration should be limited in scope to mitigate unintended consequences (unnecessarily escalating the overall militarization of cyberspace) and inadvertently sever the very relationships upon which the United States may become increasingly reliant.

Disclaimer

The views presented here are those of the author and do not represent the views of the Department of Defense, the Department of the Navy, or the Potomac Institute for Policy Studies.

Table 2: Abbreviations and Acronyms.

BA	Battlespace Awareness
CNO	Chief of Naval Operations
CO	Cyberspace Operations
CCMF	Cyber Combat Force
CNMF	Cyber National Mission Force
CYBERCOM	United States Cyber Command
DoD	Department of Defense
DODIN	Department of Defense Information Networks
IC	Intelligence Community
NSA	National Security Agency
OCO	Offensive Cyber Operations
ROE	Rules of Engagement

Acknowledgements

This manuscript is an adaptation of a report that was written to satisfy thesis report requirements associated with the Cyber Federal Executive Fellowship program, per OPNAVINST 1500.79A, at the Potomac Institute for Policy Studies, May 2013.

Notes

i. There have been several other cyberspace "wake up" calls before (Eligible Receiver, Moonlight Maze, etc), yet lessons learned from those events were often forgotten or ignored.
ii. At one time, there were 13 different documents across DOD, Agency, Service and COCOM levels outlining cyberspace operations (1).
iii. The National Defense Authorization Act for Fiscal Year 2012 (9) was signed by President Obama on December 31, 2011.
iv. Gen KB Alexander testimony at Senate Armed Forces Hearing. 18 March 2013. House Armed Services Committee.

References

1. Hollis DM. USCYBERCOM: the need for a combatant command versus a subunified command. Jt Forces Q [Internet]. 2010 March 1 [cited 2013 Feb 14];58. Available from: http://www.ndu.edu/press/lib/images/jfq-58/JFQ58_48-53_Hollis.pdf.
2. US Government Accountability Office. Cybersecurity: national strategy, roles, and responsibilities need to be better defined and more effectively implemented (Publication No. GAO-13-187). Washington, DC: US Government Accountability Office; 2013, February. Available from: http://www.gao.gov/assets/660/652170.pdf.
3. Department of Defense strategy for operating in cyberspace. Washington, DC: Office of the Secretary of Defense. 2011 July. Available from: http://www.defense.gov/news/d20110714cyber.pdf.
3. Gjelten T. First strike: US cyber warriors seize the offensive. World Aff J. 2013; Jan/Feb 13. Available from: http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive.
4. Department of Defense Dictionary of Military and Associated Terms (Joint Publication 1-02). (8 Nov 2010 as amended through 15 Dec 2013). Available from: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
5. Cartwright J (2010, July 23). Joint Terminology for Cyberspace Operations. Memorandum for the Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates. Washington, DC: The Vice Chairman of the Joint Chiefs of Staff. Available from: http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf.
6. Information Operations (Joint Publication 3-13). (2012, November 27). Available from: http://www.fas.org/irp/doddir/dod/jp3_13.pdf.
7. Department of Defense Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York, NY. Presenter: Secretary of Defense Leon E. Panetta October 11, 2012. Available from: http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.
8. The National Defense Authorization Act for Fiscal Year 2012, H.R. 1540, 112th Cong, (2011). Available from: http://armedservices.house.gov/index.cfm/ndaa-home.
9. Koh HH. Remarks at the US Cyber Command Inter-Agency Legal Conference: International Law in Cyberspace, Sept. 18, 2012, Ft. Meade, MD. [cited 2013 Feb 14]. Available from http://www.state.gov /s/l/releases/remarks/197924.htm.
10. Department of Defense. Cyberspace Operations Joint Publication 3-12. 5 Feb 2013.