NAVAL WAR COLLEGE
Newport, R.I.

Cyberspace for the Operational Artist:
Every Planner Has the Tools to Understand the Cyber Domain

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.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
17-14-2021	FINAL	

4. TITLE AND SUBTITLE

Cyberspace for the Operational Artist: Every Planner Has the Tools to Understand the Cyber Domain

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Major Joseph E. Bush, USMCR

Paper Advisor: Professor Michael R. Croskrey

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

Maritime Advanced Warfighting School
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

Distribution Statement A: Approved for public release; Distribution is unlimited.
Reference: DOD Directive 5230.24

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

Many joint planners ultimately responsible for integrating cyber capabilities into joint operations are not technical experts in the field and lack a trained "inner eye" to see cyber terrain. But the traditional conceptual frameworks of operational art, if applied to the cyber domain, yield illuminating results able to bridge the gap between a non-technical planner and the skillful employment of cyber capabilities. Examining cyberspace through the lens of operational art reveals striking similarities – and key differences – to familiar physical domains and traditional sources of combat power. By applying to cyberspace two traditional operational art frameworks – operational factors and operational functions – this paper demonstrates the cyber domain's accessibility to any joint planner. This paper focuses on analysis of factor space and the maneuver function.

15. SUBJECT TERMS

Cyberspace, Cyber Domain, Cyber Power, Operational Art, Operational Factors, Operational Functions, Planning, Maneuver

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Director, MAWS
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		29	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

INTRODUCTION

Operational art is a cognitive approach to planning. Planners do not rely simply on the joint planning process, but also on their intuition in applying elements of operational art underwritten by historical analysis.[1] Yet many joint planners ultimately responsible for integrating cyber capabilities into joint operations are not technical experts in the field and have little practical experience to build their intuition. They lack a trained "inner eye" able to see cyber terrain. The result is "bolt-on" plans for cyber forces that may meet expectations for briefing the commander but are not integral to the core operational idea.[2] But what if the best defeat mechanism for an enemy center of gravity is in the cyber domain? What if, for a particular operation, planners could best employ cyber power as the main effort, with actions in the physical domains designed to support delivery of an information payload in the cyber domain?[3] Sadly, many joint planners do not have the conceptual understanding of cyberspace necessary to make such a leap, and this shortfall hinders even the integration of cyber as a supporting effort.[4] What joint planners need most is a framework that makes cyberspace more accessible.

The answer to this experience gap is not to identify and task technical cyber experts to plan a campaign's cyber effects in isolation. Nor is it necessary to create entirely new conceptual

---

[1] U.S. Joint Chiefs of Staff, *Joint Operations* (Joint Publication 3-0, October 2018), xii. "Operational art is the cognitive approach by commanders and staffs–supported by their skill, knowledge, experience, creativity, and judgment– to develop strategies, campaigns, and operations to organize and employ military forces by integrating ends, ways, and means. The foundation of operational art encompasses broad vision; the ability to anticipate; and the skill to plan, prepare, execute, and assess. It helps commanders and their staffs organize their thoughts and envision the conditions necessary to accomplish the mission and reach the desired military end state in support of national objectives."

[2] Paul MacKenzie, "Cyberspace and Multi-Domain Operations" (Paper for the Joint Air & Space Power Conference, October 2019), 2.

[3] MacKenzie, "Cyberspace," 3.

[4] Sean Kern, "Expanding Combat Power Through Military Cyberpower Theory" (Master's thesis, Joint Advanced Warfighting School, Norfolk, VA, 2015), 2.

and planning frameworks specific to the cyber domain. Instead, the key to unlocking the potential of cyber power is to make it accessible to non-technical joint planners using concepts already well-understood and universally applied during the planning process. Operational art has just the tools needed. If applied to the cyber domain, the traditional conceptual frameworks of operational art yield illuminating results able to bridge the gap between a non-technical planner and the skillful employment of cyber capabilities. Examining cyberspace through the lens of operational art reveals striking similarities – and key differences – to familiar physical domains and traditional sources of combat power. Joint planners are operational artists who already possess the tools necessary to understand the cyber domain and fully leverage cyber power as an integral part of any operational idea. By applying to cyberspace two traditional operational art frameworks – operational factors and operational functions – this paper will demonstrate the cyber domain's similarities to the physical domains and accessibility to any operational artist.

This paper examines cyberspace operations using parts of two classic operational art frameworks: operational factors and operational functions. The operational factors are space, force, and time. Operational artists often begin a planning effort with a thorough analysis of the operating environment using these factors. This paper will focus on better understanding of the cyber domain through analysis of factor space. Although planners typically use operational factors to understand a *particular* battlespace, this paper will apply analysis of factor space more broadly to understand the *general nature* of cyberspace at the operational level. This analysis will reveal valuable concepts that help the cyber domain take shape in the planner's inner eye.

The operational functions, also called Warfighting or Joint Functions, are Command and Control, Intelligence, Movement and Maneuver, Fires, Sustainment, Protection, and Information. These functions are not in themselves types of combat power but rather conceptual lenses that a

planner uses to understand the capabilities of a particular type of combat power, the prerequisites for its use, and the various ways it can contribute to a joint operation. Throughout this paper's analysis, protection and maneuver will emerge as particularly helpful for a planner seeking to understand the employment of cyber power. Insights gained from analysis of factor space will reveal cyberspace as a domain with extraordinary opportunities for maneuver. This paper will thus devote a specific section to analysis of the operational maneuver function.

COUNTERARGUMENT: A NEW FRAMEWORK FOR A NEW DOMAIN

Some professionals argue that legacy conceptual frameworks and planning approaches are not helpful for cyberspace. The nature of the cyber domain differs vastly from that of the physical domains, and thus any attempt to apply legacy constructs, such as operational art, is misguided. The best planning approach for integrating cyber power into military operations is to leave the employment decisions in the hands of technical experts and (civilian) intelligence professionals. Martin C. Libicki, a leading theorist on the application of cyber power, writes:

> The establishment of the 24th Air Force and U.S. Cyber Command marks the ascent of cyberspace as a military domain. As such, it joins the historic domains of land, sea, air, and space. All this might lead to a belief that the historic constructs of war – force, offense, defense, deterrence – can be applied to cyberspace with little modification. Not so. Instead, cyberspace must be understood on its own terms, and policy decisions being made for these and other new commands must reflect such understanding. Attempts to transfer policy constructs from other forms of warfare will not only fail but also hinder policy and planning.[5]

Libicki justifies this reasoning at the operational level by noting that the effectiveness of a cyberattack directly correlates to the number of high-quality "exploits" – or weaknesses – that technical experts and intelligence professionals can identify before an operation.[6] His observation has two implications for planning. First, planning for cyber effects at the operational

[5] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, (Santa Monica, CA: RAND, 2009), xiii.
[6] Libicki, *Cyberdeterrence,* 154, 157.

level should err on the side of *preserving* vulnerabilities for intelligence purposes instead of exploiting them to degrade enemy capability; thus, intelligence professionals are best-suited.[7] Second, when used to degrade enemy capabilities, cyber effects work best as "bolt from the blue" surprise strikes or special operations, not when consistently integrated into every phase of a campaign like other forms of combat power.[8] The opportunities for successful cyberattack are rare. Cyber planners must not only reserve the exploitation for first-tier hackers ("too many second-tier hackers spoil the stew"), but they must also keep the *decision* to exploit "*within* the operational cyberwar outfit without bringing in higher-level decision-makers."[9]

In other words, the integration of cyber-power into joint operations is the proper responsibility of technical experts – with input from intelligence professionals – and is beyond the scope of joint planners or commanders. In this approach, cyber professionals do not need to make cyber power *more* accessible but *less* accessible. Considerations of cyber terrain should not be fully integrated into the overarching operational idea but should be stand-alone, even isolated from joint planning.[10]

Yet this paper's analysis will demonstrate the opposite: the joint planner is not only able to understand cyberspace but should also consider it alongside all other domains during planning. In practice, those who employ cyber power are non-technical commanders and planners; they rely on operational art to understand the battlespace. While too many cooks may spoil the

---

[7] Libicki, *Cyberdeterrence*, 155, 157
[8] Libicki, *Cyberdeterrence*, xv, 149
[9] Libicki, *Cyberdeterrence*, 157, emphasis added.
[10] Libicki, *Cyberdeterrence*, 156. Libicki acknowledges the importance of the military warfighter in aiding a cyber expert to understand the enemy system to be exploited through cyberattack, for example, an enemy air defense system. However, he does not fully integrate this idea into his conception of military planning for cyber operations, nor does he expand the idea to recognize that planning of joint military operations is itself an art with all the complexity of an air defense system.

technical stew, traditional paradigms do yield many valuable insights for the operational artists who are, in reality, often the decision-makers. This paper will begin to demonstrate the utility of the operational art approach by equipping the reader's inner eye to see cyber terrain through an analysis of factor space.

DISCUSSION OF FACTOR SPACE

Operational factors analysis traditionally begins with understanding the limits and contours of the definable physical space in a theater of operations.[11] Cyberspace presents an obvious curiosity in this regard since the "space" itself does not exist in the physical world. Although cyberspace has material components, its essence is more than the sum of its wires, routers, and hard drives. Joint Publication 3-12 *Cyberspace Operations* – the leading joint U.S. doctrinal publication on the topic – defines cyberspace as a "global domain *within the information environment* consisting of the interdependent network of information technology infrastructures and resident data, including internet, telecommunications networks, computer systems, and embedded processors and controllers." [12] Joint Doctrine, in turn, tautologically defines the information environment as the aggregation of the individuals and systems that store or use information.[13] The important conclusion here is that cyberspace as a domain is synthetic,

[11] Milan Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: U.S Naval War College, 2009),
III-4.
[12] U.S. Joint Chiefs of Staff, *Cyberspace Operations* (Joint Publication 3-12, June 2018), GL-4, emphasis added. Authors and theorists have spilled much ink on what cyberspace *is*, whether it is a domain at all. This line of inquiry is interesting but not germane to our discussion here. We will choose to accept the joint definition in order to more quickly move on to an analysis designed to make the domain accessible to the joint planner. For further discussion, see Peter Dombrowski and Chris Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *Naval War College Review* 67, no. 2 (2014): 75.
[13] U.S. Joint Chiefs of Staff, *Information Operations* (Joint Publication 3-13, November 2012), vii.

entirely human-made.[14] Even the idea of cyberspace *as space* is ultimately a construct, a useful metaphor invented to aid the imagination and facilitate structured thought.[15]

Much as oceans have distinct surface and subsurface layers, so the cyber domain has at least three (and as many as six) distinct layers.[16] The layered model of cyberspace is itself a construct intended to facilitate planning and one that nests well within factor space. The three layers of cyberspace identified in Joint Doctrine – physical network, logical network, and persona – are the most useful and will form the outline for this paper's analysis of factor space.[17] This paper will then examine the boundaries of cyberspace, its interaction with other domains, and the implications for the maneuver function.

Physical Network Layer

The physical network layer of cyberspace comprises all the devices, infrastructure, connections, storage facilities, and transportation of equipment that stores or transfers data. [18] This layer includes the physics of data transfer via electrons (wires), photons (fiberoptics), the

[14] Cyber and Innovation Policy Institute (CIPI), "Cyber Primer for DoD: What You Must Know About Military Cyberspace" (Newport, RI: U.S. Naval War College, January 2021), 1.
[15] Vego, *Joint Operational Warfare,* III-14.
[16] Sean Heidgerken, "Concepts for Warfare in Cyberspace" (Master's thesis, Joint Advanced Warfighting School, Norfolk, VA, 2018), 9.
John Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly* 5, no. 2 (2011): 98. Sheldon identifies four layers: infrastructure, physical (think physics, electrons, photons, electromagnetic), syntactic (logical), and semantic (user interface).
Adrian Venables, Siraj Ahmed Shaikh, and James Shuttleworth. "The Projection and Measurement of Cyberpower." *Security Journal* 30, no. 3 (2017): 1002. To Sheldon's four layers Venables, et al. add a human layer that combines cyber personae and the real-world individuals who use cyberspace.
Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (New York: Penguin Press, 2017), 40. Klimburg views the data resident in cyberspace as another, separate layer.
[17] Joint Chiefs, *JP 3-12 Cyberspace Operations*, I-2.
[18] Joint Chiefs, *JP 3-12 Cyberspace Operations*, I-3.

electromagnetic spectrum (wireless connections), or other means. Thus, even certain components of the physical layer have an ethereal quality. Some have likened this layer to the bones in the human body, over which stretch the various other layers that make for a functioning whole.[19] All of the data or information that create the cyber domain must physically reside on or transfer through materials or processes in actual physical space.[20] Consequently, the cyber domain constantly interacts with the physical domains. Actions in those domains can alter cyberspace by creating or destroying its components or, more importantly, the data that resides on those components. Physical security is thus an integral part of the protection function within the cyber domain since it can prevent physical damage or physical access to systems by which an adversary can gain logical access to the network.[21]

A road network on the land domain is the most salient analogy to the physical network layer of cyberspace.[22] Although road networks have defined physical attributes, their most important attribute from a planning perspective is their *potential* to transfer force, information, or support. Network pathways, like roads, have little intrinsic value. However, their possession, loss, creation, or destruction can potentially affect operations because of the movement, sustainment, and control they enable. Just as planners would consider protection of key road infrastructure (bridges!) from air attack, so planners must consider operational protection of key cyber infrastructure from effects generated in different domains. Physical networks also present planners with opportunities to employ kinetic operational fires offensively.

---

[19] Heidgerken, "Concepts," 9; Klimburg, *Darkening Web,* 28.
[20] Heidgerken, "Concepts," 8.
[21] Joint Chiefs, *JP 3-12 Cyberspace Operations*, I-3.
[22] Lincoln Bonner, "Cyber Power: Attack and Defense Lessons from Land, Sea, and Air Power" (Master's thesis, School of Advanced Air and Space Studies, Maxwell, AL, 2011), 34.

Likewise, just as the advent of improved road networks (rail, high-speed interstates) has changed the speed of movement and quality of sustainment on the land domain, so too have new technologies, such as fiber optics and wireless routing, changed the type and quality of information movement in cyberspace.[23] This analogy should lead planners to seek new opportunities to exploit emerging infrastructure technology in cyberspace, just as armies of the 19th century sought to exploit railroads.

Logical Network Layer

The second layer, the logical network layer, gives shape to the abstraction that is cyberspace.[24] It consists of the logical rules of interaction, or protocols, that allow physical elements of the network to format data and communicate.[25] In this layer, programming code acts as both the laws of physics and the new "physical material" used to build within the synthetic space.[26] Also called the syntactic layer, it is the language of cyberspace; it consists both of the grammar that allows communication and the literary creations of that language – data – that store the narrative of the constructed landscape. Although some theorists break out separate data and semantic (human interface) layers, joint doctrine includes all three in the same logical network layer. [27] In the human body analogy, protocols are the central nervous system; data are the muscular system; semantics is the outer skin. Yet all three stretch over the physical bones of infrastructure to form the three-dimensional body.[28]

---

[23] Vego, *Joint Operational Warfare,* III-51.
[24] Joint Chiefs, *JP 3-12 Cyberspace Operations*, I-4.
[25] Venables et al., "Projection of Cyberpower." 1001.
[26] Heidgerken, "Concepts," 9.
[27] Venables et al., "Projection of Cyberpower." 1001; Joint Chiefs, *JP 3-12 Cyberspace Operations*, I-5.
[28] Klimburg, *Darkening Web,* 35, 40.

In the logical network layer, the structure of cyberspace veers sharply away from what one might expect given the structure of its underlying physical network. For instance, the code and data behind a single website may reside on multiple physically disparate servers. Nevertheless, within the logical network layer, a single URL (uniform resource locator) address represents the website, making it, in essence, a single entity.[29] The implication is that a planner must judiciously utilize the concept of distance in cyberspace. Distances apply straightforwardly to the physical infrastructure layer but not at all to the logical layer.[30] Logically, a machine located halfway around the world may be equidistant to a machine located in the same room. This concept is not new for the operational planner. In the past, the distance between bases of operation and operational employment areas directly affected the effort needed to project force and required much energy to cross.[31] But the advent of new technologies and associated domains, such as aircraft, drastically altered the relative operational impacts of distance, increasing the operational reach of the joint force. Nevertheless, airpower, based on the surface, was not entirely free from considerations of distance as measured by surface units. Likewise, planners must bear in mind the duality of a cyberspace domain that has qualities both measurable and immeasurable in terms of distance.

If road networks are an apt analogy for the physical network layer, then lines of communication (LOCs) are the appropriate analogy for the logical network layer.[32] Lines of

---

[29] Joint Chiefs, *JP 3-12 Cyberspace Operations*, I-4.
[30] CIPI, "Cyber Primer," 1.
[31] Vego, *Joint Operational Warfare,* III-11.
[32] Joint Chiefs, *JP 3-12 Cyberspace Operations*, II-12. Joint doctrine here relates securing wired or wireless bandwidth to maintaining LOCs. Yet this analogy is incomplete, because it incorrectly identifies LOCs as physical things instead of operational concepts that include movement, planning, intent, and the troops or materials transferred. LOCs are thus abstractions, and so the better analogy is to logical pathways.

communication are not the physical roads themselves but are abstractions that also include the troops and materiel they carry.[33] Planning and "rules of the road" transform road networks from inanimate features to LOCs, operational concepts that convey action and purposeful intent. These imaginary lines are an integral part of multiple operational functions, including sustainment, command and control, and maneuver. Likewise, logical network pathways ultimately rely on planning and "rules of the road" – as conveyed by code and protocol algorithms – to transform physical hardware into virtual pathways traveled by data, representing troops and materiel. However, unlike land lines of communication that utilize a road network, logical network pathways are not determinative in route but offer nearly unlimited possibilities for route selection. In this regard, they more closely resemble sea or air lines of communication; the nature of the domain allows the user to select from among potentially infinite routes for the LOC.

Thus, another critical – even central – characteristic of cyberspace is mutability. The synthetic nature of the space allows users to create or alter the logical rules, data, and virtual architecture in real-time.[34] Cyberspace is constantly changing in both "size" and "topography." As one experienced operational planner notes, "the essential nature of cyberspace is continuous change…Cyberspace is in a continuous process of construction and deconstruction, renewing itself in nearly infinite variety."[35] Although planners have long understood the highly dynamic nature of a traditional operational space resulting from interaction during combat, the expansion of cyberspace is new because it requires significantly less time and force to achieve.[36] Planners

[33] Vego, *Joint Operational Warfare*, IV-70.
[34] Timothy Williams, "Cyberwarfare and Operational Art" (Master's thesis, Advanced Operational Arts Studies Program, U.S. Army Command and General Staff College, Fort Leavenworth, KS, May 25, 2017), 12.
[35] Heidgerken, "Concepts," 8.
[36] Vego, *Joint Operational Warfare*, III-12.

can also view the constantly fluctuating data, rules, and pathways as changes in topography. One experienced cyberspace planner likens this complexity of change to broken or mountainous terrain.[37] The intricacy of software and constant changes in code create observation gaps that result in unguarded vulnerabilities for a defender, just as from within a stronghold in rugged terrain.[38] Yet even this analogy fails fully to capture the complexity of malleable cyberspace, where both attacker and defender can manipulate terrain before and during an operation.

Fortresses, trench systems, and human-made obstacles serve as helpful analogs for defensive measures in the logical network layer. All are synthetic features in land warfare that alter the terrain to enhance protection for the defender while slowing maneuver.[39] Fortresses cause the attacker to expend additional force and culminate the attack early.[40] Obstacles serve the dual purpose of slowing an attacker and causing him to deploy early and are thus most effective when covered by observation and fires.[41] Likewise, firewalls and (logical) port blocks are synthetic "terrain features" within cyberspace that enhance protection by slowing maneuver.[42] They serve the dual purpose of forcing an attacker to expend force – and thus to culminate – and to deploy attacking forces early, providing an opportunity for the defender to "see" the nature and strength of the attack. Thus, they are most effective when employed in-depth and tied to observation and fires. This analogy gives rise to the idea of cyber defense as a defense-in-

[37] Bonner, "Cyber Power," 34.
[38] Bonner, "Cyber Power," 59.
[39] Bonner, "Cyber Power," 66.
[40] Bonner, "Cyber Power," 18; Carl von Clausewitz, *On War* (Edited and Translated by Michael Eliot Howard and Peter Paret. New York, NY: Oxford University Press, 2006), 497.
[41] U.S. Joint Chiefs of Staff, *Barriers, Obstacles, and Mine Warfare for Joint Operations* (Joint Publication 3-15, March 2018), III-8. Although updated as late as 2018, *JP 3-12* discusses principles for employment of obstacles in physical space, yet never draws a connection to firewalls, port blocks, or any other cyberspace concept.
[42] Joint Chiefs, *JP 3-12 Cyberspace Operations*, I-7.

depth. The defender uses complex terrain, synthetic terrain features, and pre-planned responses to trade space for time while analyzing the attack for an opportunity to counter.[43] Countering an attack in fluid terrain requires not only the technical expertise of a tier-1 hacker but also the creativity of an artist, a maneuverist trained to seek and exploit advantage.

Persona Layer

The persona layer is the third and final layer in the three-layer model of cyberspace. It consists of digital representations of actors and their relationships to one another. These virtual entities, or cyber-personae, are simply user accounts that may be either associated with a real human individual or entirely automated. A real person may have numerous personae on various sites or networks that share common personal identifiers (such as name or email address) or may control numerous personae on a single site that share no identifiers. Multiple real-world actors or organizations may also use a single persona. [44]

Also called the social layer of cyberspace, discussions about the persona layer are difficult to distinguish from an analysis of factor force.[45] This is because cyber personae are essential to the conversion of cybered combat potential – represented by military cyber personnel, hardware, and systems – into cyber combat power. [46] Like aircraft, cyber personae are the vehicles that allow placement, access, and power projection into a domain otherwise

[43] Bonner, "Cyber Power," 25.
[44] Joint Chiefs, *JP 3-12 Cyberspace Operations*, I-4.
[45] Heidgerken, "Concepts," 10.
[46] Vego, *Joint Operational Warfare*, III-33. Here Vego discusses the difference between combat power and combat potential as well as factors influencing the conversion of potential to power. Although he does not explicitly discuss cyber power, his principles still apply.

inaccessible to humans. Thus, numbers and quality of personae are an essential consideration when evaluating the cyber combat potential of a force.[47]

Nevertheless, the synthetic nature of the persona layer also makes it integral to factor space in the cyber domain. The persona layer introduces several new forms of malleability: creation or deletion of new personae, movement of an individual from one persona to another, rapid manipulation of user account characteristics or information, or rapid change of the individual(s) controlling a particular persona.[48] This complexity builds upon the complexity of the physical and logical network layers, creating numerous new opportunities for maneuver.

Boundaries of Cyberspace

Although the logical network and persona layers are potentially limitless, there are nevertheless boundaries in cyberspace. The first type of boundary arises from considering that there is not a single cyberspace, but multiple cyberspaces.[49] Each individual network is potentially a separate "space." Some of these networks are interconnected, while some are entirely independent, even insulated, from all others. An independent network may be physically separated or logically separated, unable to communicate due to different protocols or data formats.[50] Although some may conceive of the World Wide Web as the global cyber domain, the global cyber domain actually consists of all networks, public or private, connected or not. The land domain is a good analogy in this regard since it includes all global landmasses even though

[47] Vego, *Joint Operational Warfare*, III-35. Here Vego discusses the differences between tangible and intangible elements of factor force. Cyber personae likely fall somewhere between these categories. Although outside the scope of this paper, further exploration of the role of cyber personae in an analysis of factor force would likely yield insightful results.
[48] Joint Chiefs, *JP 3-12 Cyberspace Operations*, I-4.
[49] Kern, "Expanding Combat Power," 13.
[50] Albert-László Barabási, *Linked: The New Science of Networks* (Cambridge, MA: Perseus Pub., 2002), 167-69.

the maritime domain separates some. Thus, insulated networks are analogous to islands, while the World Wide Web is similar to the Eurasian landmass.[51] Connected or not, all networks, like all landmasses, share specific characteristics that define a single domain. In the physical domains, planners attempt to use capabilities in alternate domains to bridge gaps between landmasses, as with the use of naval power to conduct amphibious operations or airpower for airborne assault. Likewise, planners can consider bridging gaps between insulated networks by physically transporting and introducing code using a flash drive or similar device.[52]

The second type of boundary in cyberspace arises from its global reach and interaction with political boundaries present in other domains. Because actors, equipment, and intellectual property all reside within political boundaries – whether physically defined or conceptual – there is no such thing as stateless maneuver space in the cyber domain.[53] This principle stands in stark contrast to the vast global commons in the maritime and space domains. However, this is not a new concept for planners: political boundaries on land create corresponding boundaries in much of the air domain. Likewise, the physical location of network components and (real human) actors is the starting point for determining state boundaries within cyberspace.[54] However, this paper's previous analysis of the divergence between the physical network and logical network layers immediately reveals the difficulties with this approach. A single website, for example, may reside on multiple servers within different sovereign territories. The complexity increases when one considers that private corporations create and own the vast majority of cyberspace.

---

[51] Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge University Press, 2007), 33.
[52] Bonner, "Cyber Power," 34.
[53] Joint Chiefs, *JP 3-12 Cyberspace Operations*, ix.
[54] Joint Chiefs, *JP 3-12 Cyberspace Operations*, I-3.

These entities may have complex legal status within one or many sovereign states.[55] Cyberspace presents new opportunities and conceptual challenges for operations that cross national borders and the public-private divide.[56] Just as the advent of airpower introduced new possibilities to bypass military forces and strike civilian infrastructure, so too has the advent of cyber power raised questions about targeting civilian infrastructure, data, or cyber personae.[57]

Nevertheless, similar complexity in an operational area is not new to a joint planner. Operational areas in physical domains may include numerous sovereign territories, enemy units may straddle political boundaries, and engagements often occur on privately-owned land.[58] The same detailed analysis of factor space that has long aided planners to deconstruct the complex physical battlespace also produces results in cyberspace. Indeed, analysis of factor space reveals another source of complexity, the interaction between cyberspace and physical domains.

Interaction with Other Domains

The interaction of the physical domains within a theater of operations has long been a concern of operational factors analysis, for example, recognizing the opportunities presented by the confluence of air, land, and maritime domains within a littoral area.[59] Cyberspace is not an

[55] Libicki, *Cyberdeterrence,* xvii, 64.
[56] Heidgerken, "Concepts," 21.
[57] Craig Greathouse, "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?" *Cyberspace and International Relations*, pp. 21-40. Springer, Berlin, Heidelberg, (2014): 33-34.
[58] Joint Chiefs, *JP 3-12 Cyberspace Operations*, I-4. Joint doctrine attempts to impose some order on this complexity by applying the framework of blue, red, and gray cyberspace. These zones correspond, respectively, to cyberspace controlled by the U.S. and its mission partners, enemies or adversaries, and neutral actors. Areas of "control" do not always correspond to political or legal boundaries, just as traditional enemy forces may control territory in a neutral country.
[59] Vego, *Joint Operational Warfare*, IV-35.

independent domain but interacts with each of the others.[60] Indeed, the cyber domain cannot exist without the physical presence of its components in other domains. The ultimate goal of cyberspace operations is to create effects that alter human action in the physical domains.[61] Therefore, some mistakenly conclude that cyberspace is *unique* in that it exists only to create effects in the physical domains. In contrast, traditional sources of combat power exist to create effects within their domain.[62] Yet this is not accurate. The use of one domain as a means to create intended effects in another primary domain is as old as warfare itself. As Corbett points out, humans live on the land, and so the purposes of naval (maritime) power will always support political goals on land.[63] The primacy of the land domain – or should we say, the ordered importance of domains – only became more evident with the advent of air and space, in which it is even more difficult to imagine sustained human presence. Suddenly the relative impermanence of effects on the sea paled in comparison to the brief pulses of combat power from the air. The cyber domain is no exception. *Interactions* among domains have always been of great importance to the military planner. Cyberspace affords new opportunities but not a new paradigm, and operational art provides valuable tools to analyze the opportunities.

ANALYSIS: MANEUVER IN CYBERSPACE

[60] Joey Jansen van Vuuren and Louise Leenen. "A Model for Measuring Perceived Cyberpower" (Academic Conferences and Publishing International Ltd, 2018), 320.
[61] Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What To Do About It.* (New York: Harper Collins, 2010), 232.
[62] Heidgerken, "Concepts," 11.
[63] Julian Corbett, *Some Principles of Maritime Strategy* (Mineola, NY: Dover Publications, Inc., 2004), 14. "Since men live upon the land and not upon the sea, great issues between nations at war have always been decided – except in the rarest cases – either by what your army can do against your enemy's territory and national life, or else by the fear of what the fleet makes it possible for your army to do."

This paper's analysis of factor space in the cyber domain generates an even greater understanding when paired with further analysis using operational functions. For example, the layered model of cyberspace provides myriad new possibilities for maneuver. In physical domains, there are five degrees of freedom that allow us to describe the movement of forces or materiel: horizontal position, lateral position, vertical position, direction of travel, and speed.[64] The complexity of describing movement varies by domain and type of equipment, varying the difficulty in tracking and targeting. For example, a ship on the surface layer of the maritime domain cannot change its vertical position. But different equipment can open new possibilities, such as the submarine that transits on the surface and can also change its vertical position within the subsurface layer. Furthermore, the rapidity with which forces can change any of these five degrees becomes a quality in itself, such as the maneuverability of a fighter aircraft in the air domain. This agility further complicates tracking and targeting. Nevertheless, most joint planners intuitively understand physical maneuver despite its complexities. Physical maneuver provides a useful starting point for gaining a conceptual understanding of maneuver in cyberspace.

The traditional five degrees also apply to cyberspace because the physical network layer includes infrastructure components, human actors, and machines connected to the network. These components are not always stationary, such as a server, but can be highly mobile, such as the computer aboard an aircraft. But the unique nature of cyberspace introduces five *additional* degrees of freedom that describe cyber movement. The additional degrees of freedom are: "virtual location, customizable rules of action, customizable physical pathways, customizable

[64] Bonner, "Cyber Power," 28.

virtual pathways," and persona manipulation.[65] These additional degrees of freedom and near-instant speed of action produce agility of movement unmatched in the physical domains.[66]

Virtual location describes the artificial position as represented by an internet protocol (IP) address. Although this address is a single value, the malleable nature of cyberspace allows an actor to change quickly or constantly cycle through IP addresses. *Customizable rules of action* describe the changeable nature of cyberspace syntax. These rules include directions for how data is formatted, norms for how machines communicate, and the protocols governing changes to these. They include both the specific grammar rules for the language of cyberspace *and* the underlying principles of linguistics. Another analogy would be the ability not just to create and delete matter, but also to alter the laws of physics governing that matter.[67] *Customizable physical pathways* refer to a user's ability to choose or alter the physical path of information through the physical network architecture. An actor can easily choose the physical path of information when there are multiple, redundant pathways. Adding new physical pathways or transmission modes (for the electromagnetic spectrum) is likely a lengthier and more difficult process because it involves connecting new physical infrastructure. *Customizable virtual pathways* refer to virtual route selection, which is essentially limitless. Just as actors can select the physical route of information from node to node, so they can alter the logical path of information by altering the logical relationships among nodes within the logical network.[68] Like selection of the exact sea

---

[65] Bonner, "Cyber Power," 30.
[66] Bonner, "Cyber Power," 28-29; Lincoln Bonner, "Cyber Power in 21st Century Joint Warfare," *Joint Forces Quarterly,* no. 74 (3rd Quarter, 2014), 103. Bonner observes that in cyberspace speed of action *and* speed of observation approach the speed of light. Aside from mutability, speed may well be the defining characteristic of cyberspace. Although deeper analysis of the implications of cyber speed to joint operations are outside the scope of this paper, using factor time analysis as the framework for further inquiry would prove useful.
[67] Bonner, "Cyber Power," 29.
[68] Bonner, "Cyber Power," 30.

route between two ports, the possibilities are theoretically limitless. Finally, *persona manipulation* refers to potential "movement" within the persona layer. As discussed, this includes creation or deletion of new personae, movement of an individual from one persona to another, rapid manipulation of user account characteristics, or rapid change of the individual(s) controlling a particular persona.[69]

Thus, the unlimited, malleable nature of cyberspace allows for dizzying combinations of movement resulting in limitless opportunities for maneuver. Indeed, maneuver in cyberspace is as much about altering the terrain itself as about moving through it. The idea of logical maneuver is unique to cyberspace and, therefore, may seem the least intuitive to an operational planner. Yet a firm understanding of operational art prepares planners to grasp this critical opportunity. Operational art has always identified maneuver as something conceptually distinct from movement. Maneuver is "the movement of one's combat forces aimed at obtaining a positional *advantage* relative to the enemy."[70] Maneuver is not primarily spatial but is about gaining advantage. Movement is a type of action; maneuver is a way of thinking. Adding degrees of freedom does increase the complexity of cyberspace, just as the advent of new domains has done throughout history. Yet the idea of maneuver has remained constant, an abstraction not about new forms of movement but about finding new ways to exploit that movement. Maneuver in the cyber domain, just as in other domains, is about "taking action to generate and exploit some kind of advantage."[71] The five new degrees of freedom simply reveal new possibilities for

[69] Joint Chiefs, *JP 3-12 Cyberspace Operations*, I-4.
[70] Vego, *Joint Operational Warfare,* VII-53.
[71] U.S. Marine Corps, *Warfighting* (Marine Corps Doctrinal Publication 1, 2018) , 4-4. "The traditional understanding of maneuver is a spatial one; that is, we maneuver in space to gain a positional advantage. However, in order to maximize the usefulness of maneuver, we must consider maneuver in other dimensions as well. The essence of maneuver is taking action to

generating advantage. Just as a counterattack in fluid cyber terrain requires the creativity of an operational artist, so the complexity of movement in cyberspace requires the intuition of a maneuverist with a trained eye for cyber terrain.[72]

CONCLUSION

Viewing cyberspace through the traditional lens of operational art demonstrates not only that joint planners *can* understand cyberspace, but also that they *should* fully integrate it into the central operational idea during the entire planning process. Joint planners ultimately responsible for the employment of cyber power use operational art to understand the physical domains, and so traditional frameworks are a natural choice to improve their understanding of cyberspace. Planning for cyber effects conducted by technical experts isolated from joint planners is not optimal, nor does the nature of cyberspace make this necessary. The very idea of cyberspace *as space* is a construct, and so we should not hesitate to apply constructs to this synthetic environment to enhance comprehension. The relevant metric is not technical precision but utility. This paper has demonstrated the utility of this approach by applying operational factors analysis – specifically, factor space – and using several of the operational functions, especially protection and maneuver. The application of factor space analysis has given shape to the synthetic cyber domain, making the terrain visible to the inner eye of the non-technical planner. It has revealed a space with many conceptual similarities to the physical domains and produced numerous insights to build the intuition of any planner.

---

generate and exploit some kind of advantage over the enemy as a means of accomplishing our objectives as effectively as possible."

[72] For further detailed discussion of maneuver in cyberspace, see: Gregory Conti and David Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict* (Kopidion Press, 2017), 88-120. Conti and Raymond believe that the concept of maneuver is about exploiting flanks. The many layers of cyberspace offer numerous, constantly-fleeting opportunities to find and exploit an adversary's flanks.

The physical network layer of cyberspace is conceptually similar to a network of roads in the physical domain: the roads themselves do not define the domain, and yet they enable the activity that makes the domain relevant. Thus, physical protection is critical. It is the logical network layer that gives shape to the cyber "space," just as planning, movement, and potential transform roads into lines of communication. In the ever-changing landscape of cyberspace, distance does not always apply, and complexity is like rugged, broken terrain. The complexity favors attackers, and thus defense in cyberspace is defense-in-depth, designed to trade space for time. Cyberspace, like the air domain, can erase natural boundaries, and yet political boundaries on the land domain are still relevant. So too are the physical and logical separation of disparate "landmasses" – or networks – within the global cyber domain. Planners already possess the cognitive framework of operational art to understand the interaction of cyberspace with other domains. The added complexity of cyberspace presents numerous opportunities to generate advantage through maneuver.

Ultimately, this paper's analysis shows that the use of operational art uniquely equips joint planners to understand the cyberspace domain as it relates to warfighting. However, the limited scope of this paper allowed only a narrow glimpse of the possibilities for non-technical planners to improve their understanding of warfighting in cyberspace. Further analysis is needed.

RECOMMENDATIONS

The insights about the cyber domain gained from an initial application of only two operational art frameworks justify further analysis using this method. Specifically, this paper recommends further analysis using the other operational factors – time and force – as well as factor relationships and objectives in cyberspace. Analysis using factor time would present numerous insights about cyberspace, a domain where speed of action creates time compression,

malicious code can have the persistence of naval mines, and the lack of warning time increases the value of the intelligence function.[73] Factor force analysis would reveal the primarily disruptive, not destructive, nature of cyber power. In addition to the traditional elements of force – troops, equipment, and doctrine – cyber personae contribute to the force's combat potential.[74]

A more thorough analysis of cyberspace using each of the seven operational functions would also further build intuition. These functions both apply to cyberspace itself *and* describe how cyber power enables the joint force. For example, we can better understand many offensive cyber effects by describing them in terms of operational fires; but cyber power also greatly enables kinetic operational fires by enabling scouting, control, and targeting systems.[75]

Finally, this paper's analysis of factor space has revealed a particularly complex, "messy" battlefield. If the ancient battlefield was a traditional chessboard and the modern battlefield is a game of three-dimensional chess, then cyber-enabled conflict is chess played on the faces of a Rubik's cube being manipulated by multiple players during play. Traditional models for organizing an operational area, including the conception of close, deep, and rear areas, are still useful, yet they become significantly strained by forces with instant cyber connections to the far side of the globe.[76] This paper, therefore, recommends further research on the implications of operational factors analysis of cyberspace to theater geometry.

---

[73] Bonner, "Cyber Power," 27, 46, 89.
[74] Greathouse, "Cyber War," 23; Bonner, "Cyber Power," 44; Kern, "Expanding Combat Power," 4.
[75] Joint Chiefs, *JP 3-12 Cyberspace Operations*, II-7.
[76] Venables et al., "Projection of Cyberpower," 1002.

BIBLIOGRAPHY

Allied Joint Publication-3.20: Allied Joint Doctrine for Cyberspace Operations. NATO Standardization Office, January 2020.

Arwood, Sam, Robert Mills, and Richard Raines. "Operational art and Strategy in Cyberspace." In *International Conference on Cyber Warfare and Security*, p. 16. Academic Conferences International Limited, 2010.

Barabási, Albert-László. *Linked: The New Science of Networks.* Cambridge, MA: Perseus, 2002.

Bonner, E. Lincoln. "Cyber Power: Attack and Defense Lessons from Land, Sea, and Air Power." Master's thesis, School of Advanced Air and Space Studies, Maxwell, AL, 2011.

Bonner, E. Lincoln. "Cyber Power in 21st Century Joint Warfare." *Joint Forces Quarterly,* no. 74 (3rd Quarter, 2014): 102-109.

Center for Strategic Leadership. *Strategic Cyberspace Operations Guide*. Carlisle, PA: U.S. Army War College, 2016.

Clarke, Richard A. and Knake, Robert K. *Cyber War: The Next Threat to National Security and What To Do About It.* New York: Harper Collins, 2010.

Clausewitz, Carl von. *On War*. Edited and Translated by Michael Eliot Howard and Peter Paret. New York, NY: Oxford University Press, 2006.

Corbett, Julian S. *Some Principles of Maritime Strategy*. Mineola, NY: Dover Publications, Inc, 2004.

Conti, Gregory and David Raymond. *On Cyber: Towards an Operational Art for Cyber Conflict*. Kopidion Press, 2017.

Cyber and Innovation Policy Institute (CIPI). "Cyber Primer for DoD: What You Must Know About Military Cyberspace." Newport, RI: U.S. Naval War College, January 2021.

Dombrowski, Peter, and Chris C. Demchak. "Cyber War, Cybered Conflict, and the Maritime Domain." *Naval War College Review* 67, no. 2 (2014): 70-96.

Gady, Franz-Stefan, and Alexander Stronell. "Cyber Capabilities and Multi- Domain Operations in Future High-Intensity Warfare in 2030," *Cyber Threats and NATO 2030: Horizon Scanning and Analysis,* 2020.

Greathouse, Craig B. "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?" In *Cyberspace and International Relations*, pp. 21-40. Springer, Berlin, Heidelberg, 2014.

Hall, Charles. “Operational Art in the Fifth Domain.” Master’s thesis for the U.S. Naval War College, Newport, RI, 2011.

Hareide, Odd Sveinung, Øyvind Jøsok, Mass Soldal Lund, Runar Ostnes, and Kirsi Helkala. “Enhancing Navigator Competence by Demonstrating Maritime Cyber Security,” Journal of navigation 71, 71, no. 5 (September 2018): 1025–39.

Heidgerken, Sean. “Concepts for Warfare in Cyberspace.” Master’s thesis for the Joint Advanced Warfighting School, Norfolk, VA, 2018.

Hossier, Mary. “The Joint Officer in the Next War Better Know His Cyber… and Good: Methods to Integrating Cyberspace Operations Into Joint Planning.” Master’s thesis for the U.S. Naval War College, Newport, RI 2020.

U.S. Joint Chiefs of Staff. *Joint Operations*. Joint Publication (JP) 3-0, October 2018.

U.S. Joint Chiefs of Staff. *Cyberspace Operations*. Joint Publication (JP) 3-12, June 2018.

U.S. Joint Chiefs of Staff. *Information Operations*. Joint Publication (JP) 3-13. November 2012.

U.S. Joint Chiefs of Staff. *Barriers, Obstacles, and Mine Warfare for Joint Operations*. Joint Publication (JP) 3-15. March 2018.

Keisler, Joshua. “The Cyber Domain: Defining it and Norming Users’ Behavior.” Master’s thesis for the U.S. Army War College, Carlisle, PA, 2016.

Kern, Sean. “Expanding Combat Power Through Military Cyberpower Theory.” Masters thesis for the Joint Advanced Warfighting School, Norfolk, VA, 2015.

Klimburg, Alexander. *The Darkening Web: The War for Cyberspace.* New York: Penguin Press, 2017.

Libicki, Martin C. Cyberdeterrence and Cyberwar, Project Air Force. Santa Monica, CA: RAND, 2009.

Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press, 2007.

MacKenzie, Paul. “Cyberspace and Multi-Domain Operations.” Paper for the Joint Air & Space Power Conference, October 2019. https://www.japcc.org/cyberspace-and-multi-domain-operations/

Sheldon, John B. "Deciphering Cyberpower: Strategic Purpose in Peace and War." *Strategic Studies Quarterly* 5, no. 2 (2011): 95-112.

Turunen, Maija. "The Possibilities of Cyber Methods as Part of Maritime Warfare: Baltic Sea." In *European Conference on Cyber Warfare and Security*, pp. 527-XIX. Academic Conferences International Limited, 2019.

U.S. Marine Corps. *Warfighting*. Marine Corps Doctrinal Publication 1, 2018.

Vego, Milan N. *Joint Operational Warfare: Theory and Practice*. Newport, RI: U.S Naval War College, 2009.

Venables, Adrian, Siraj Ahmed Shaikh, and James Shuttleworth. "The Projection and Measurement of Cyberpower." *Security Journal* 30, no. 3 (2017): 1000-1011.

Vuuren, Joey Jansen van, and Louise Leenen. "A Model for Measuring Perceived Cyberpower." Academic Conferences and Publishing International Ltd, 2018.

Williams, Timothy. "Cyberwarfare and Operational Art," Master's thesis for the Advanced Operational Arts Studies Program, U.S. Army Command and General Staff College, Fort Leavenworth, KS, May 25, 2017.

Witte, John, "The Panacea and the Square Peg: Strategic Fallacies of the Air, Undersea, and Cyber Domains." Master's thesis for the Joint Advanced Warfighting School, Norfolk, VA, 2015.