Cyber Key Terrain:
A Conceptual Assessment

Wade L. Huntley
Senior Lecturer
U.S. Naval Postgraduate School

Paper prepared for
MARFORCYBER

The views expressed in this paper are the author's alone,
and do not represent policies or positions of the U.S. Navy or the U.S. government.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
06-2016	Final Report	04-2015 - 03-2016

4. TITLE AND SUBTITLE

Cyber Key Terrain: A Conceptual Assessment

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR

Wade L. Huntley

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School (NPS)

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Operations Analysis Directorate
3300 Russell Rd
Quantico, VA 22134

10. SPONSOR/MONITOR'S ACRONYM(S)
OAD

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES
None

14. ABSTRACT

This report presents an analysis of the concept of "cyber key terrain." The conceptual analysis reviews use of the term in recent governmental and non-governmental studies, and is accompanied by an extensive annotated bibliography. This report contributes to a larger U.S. Marine Corps Cyberspace Key Terrain study, whose purpose is to analyze current approaches to the cyberspace key terrain concept within the Department of Defense (DoD) in order to enhance methodologies for "identifying and analyzing the importance of cyberspace systems, services, and processes for Marine Air-Ground Task Force (MAGTF) mission areas."1 This report contributes to that broader purpose by assessing the conceptual clarity of existing uses of the cyber key terrain concept and considering the utility of the concept as a means to effective mission planning.

Two findings of this report bear reporting at the outset. The first of these findings is the limited scope of attention to the topic of cyber key terrain. The second concerns the general absence of awareness of the metaphorical quality of the concept of cyber key terrain in most applications.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					William Cox
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	SAR	18	**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFIED	Same as report (SAR)	SAR			7037846007

Executive Summary

Following are the major conclusions of this study:

- The concept of "key terrain" applied in cyberspace is necessarily metaphorical. This is not a deficiency, merely a fact to be kept in mind. The concept's metaphorical quality varies by application.
- There are a variety of definitions of "cyber key terrain" in governmental and nongovernmental studies. These definitions converge in certain features, most notably a focus on the physical attributes of cyberspace.
- Broader definitions of cyberspace or the cyber domain commonly view it as constituted by multiple elements or "layers," of which physical attributes form only one element or layer. These definitions often emphasize the importance of nonphysical (e.g. logical or persona) elements or layers as equivalent forums for conflict and force projection.
- Most definitions of cyber key terrain rarely address more virtual cyberspace elements (such as the "logical" or "persona" layers). Definitions of cyber key terrain that focus on physical cyberspace attributes thus fail to synchronize with common definitions of cyberspace more broadly.
- The utility of the concept of cyber key terrain also varies across tactical, operational and strategic levels of warfare doctrine and planning.
- A key unanswered question is whether a concept of key terrain can be developed that would be applicable to any element or layer of the cyber domain. Applying the concept of key terrain to virtual elements of cyberspace involves increasing degrees of abstraction and metaphor.
- The abstract nature of the concept of key terrain in virtual cyberspace begs a further question of whether the concept is best suited to generating doctrine and policy optimally effective for prevailing in conflict at those virtual layers. Non-spatial models, though less familiar in current military planning, may be more applicable to conflict in virtual environments.
- These questions raise a dilemma for military planning. A concept of cyber key terrain enables translating a wealth of historical knowledge and doctrine into cyber conflict. This approach risks over-emphasizing the conventional aspects of cyber conflict and overlooking more novel features. But the urgent need for doctrine and policy to guide action leaves little time for revisiting received wisdoms. Decisionmakers must find the appropriate balance between applying concepts like key terrain to cyberspace while vigilantly probing for the limitations of those applications.

Introduction

This report presents an analysis of the concept of "cyber key terrain." The conceptual analysis reviews use of the term in recent governmental and non-governmental studies, and is accompanied by an extensive annotated bibliography.

This report contributes to a larger U.S. Marine Corps Cyberspace Key Terrain study, whose purpose is to analyze current approaches to the cyberspace key terrain concept within the Department of Defense (DoD) in order to enhance methodologies for "identifying and analyzing the importance of cyberspace systems, services, and processes for Marine Air-Ground Task Force (MAGTF) mission areas."[1] This report contributes to that broader purpose by assessing the conceptual clarity of existing uses of the cyber key terrain concept and considering the utility of the concept as a means to effective mission planning.

Two findings of this report bear reporting at the outset. The first of these findings is the limited scope of attention to the topic of cyber key terrain. The second concerns the general absence of awareness of the metaphorical quality of the concept of cyber key terrain in most applications.

Work on the topic of cyber key terrain is in places deep but notably not broad. Within U.S. governmental study, considered attention is highest within entities focused on tactical concerns and proximate mission achievement. There is less attention at operational and especially strategical levels of thinking; for example, the 2015 *Department of Defense Cyber Strategy*, the 2011 *Department of Defense Strategy for*
Operating in Cyberspace, and the 2012 Department of Defense *Joint Operational Access Concept (JOAC)* all make no reference to the cyber key terrain concept.[2]

---

[1] Program, Cyberspace Key Terrain Workshop, Naval Postgraduate School, Monterey, CA, 7-8 July 2015, p.2.

[2] U.S. Department of Defense. *The Department of Defense Cyber Strategy*. Washington, DC: U.S. Department of Defense, 2015; U.S. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC: U.S. Department of Defense, July 2011; .S. Department of Defense. *Joint Operational Access Concept (JOAC)* (v 1.0). Washington, DC: U.S. Department of Defense, 2012. Other notable sources that make no reference to cyber key terrain include: U.S. Department of the Navy. *Next Generation Enterprise Network: Network Operations (NetOps) Concept of Operations (CONOPS)*.
Washington, DC: U.S. Department of the Navy, 2008; Commandant, U.S. Marine Corps. *Cyberspace Operations* (Marine Corps Order 3100.4). Washington, DC: Department of the Navy, 2013; National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*.
Version 1.0. Washington, DC: National Institute of Standards and Technology, 2014.

Published nongovernmental analyses of cyber key terrain are limited, and consist mainly of works by individuals or organizations linked in some manner to governmental attention (the most

seminal of these works are discussed in this report).[3] In some cases, the omission is conspicuous; for example, one recent extensive study of "cyber mission assurance" makes no mention of the concept of "key terrain."[4] This limited scope of attention to the topic of cyber key terrain could have several explanations.[5]

A second initial finding is the general lack of recognition of the metaphorical quality of the concept of cyber key terrain in most considerations of the topic. The metaphorical nature of the notion of "terrain" in a virtual environment is obvious, and yet rarely noted. One early study of "key defensive terrain in cyberspace" was premised on the relevance of "spatial metaphors" for computer network defense strategies.[6] Tellingly, later citations to this work overlook that core premise.[7]

Of course, recognizing that the idea of "key terrain" in cyberspace is more metaphorical than literal is not necessarily problematic. Most cyberspace terms began as metaphors, only gradually accumulating indigenous meaning. "Virus," "worm" and "bug" metaphorically associate cyberspace to biological systems. Terms like "hardware" and "firewall" are more structural metaphors. The recent metaphor of "the cloud" confers the qualities of intangibility and ubiquitous presence to off-site data and applications access. Since the emergence of cyber security as a policy concern, analysts have recognized the both the utilities and hazards of utilizing metaphorical associations to build understandings of the novel phenomena of the information age.[8]

The following conceptual analysis of "cyber key terrain" is informed by the linkage between these two initial findings. The report identifies how lack of recognition of the metaphorical nature of the concept of cyber key terrain has both misdirected and limited its application as a tool for building effective strategic, operational and tactical doctrine. Building a stronger foundation for the term will, in turn, open opportunities for broader study of its relevance and application for understanding cyber security challenges and forging effective policy solutions.

[3] This report's author, in a search of his personal collection of over 300 items related to the topic of cyber strategy and policy, found only a handful of mentions of "cyber key terrain."

[4] Jabbour, Kamal, and Sarah Muccio. "The Science of Mission Assurance." *Journal of Strategic Security* 4, no. 2 (2011): 61–74. Both authors are affiliated with the Air Force Research Laboratory, Rome, NY.

[5] Generation and evaluation of potential explanations would be tangential to the purposes of this report.

[6] Pingel, Thomas J. "Key Defensive Terrain in Cyberspace: A Geographic Perspective." In *Proceedings of the International Conference on Politics and Information Systems (PISTA)*. (159–163). Orlando, 2003.

[7] Cf. Dressler, Judson, William Moody, Calvert L. Bowen, III, and Jason Koepke. "Operational Data Classes for Establishing Situational Awareness in Cyberspace." In *2014 6th International Conference on Cyber Conflict*, edited by P. Brangetto, M. Maybaum, and J. Stinissen. Tallinn: NATO CCD COE Publications, 2014; Cloud, Jr., Donald W. "Integrated Cyber Defenses: Towards Cyber Defense Doctrine."

Master's thesis, Naval Postgraduate School, 2007. This latter work goes further, explicitly "throwing out" metaphor and embracing a narrow literal definition of cyberspace limited to networked uses of electronics and the electromagnetic spectrum for managing data. Cloud, p.11.

8 See, for example, Libicki, Martin C., *Defending Cyberspace and Other Metaphors*, Washington DC: National Defense University, 1997.

Conceptions of Cyberspace Key Terrain

There is no U.S. government doctrinal definition of "cyber key terrain," and the need for conceptual grounding is commonly noted.[9] The thus-far coarse condition of the concept of cyber key terrain may in part result from a dearth of strategic-level attention to it in U.S. Department of Defense strategic thinking (as noted above). There are, however, a variety of definitions and utilizations of "cyber key terrain" in other governmental and non-governmental studies. Most commonly, these definitions and uses focus mainly or exclusively on the technical and/or physical attributes of cyberspace. In many cases, these references are just in passing.[10] But in a number of notable instances, this tendency is more developed:

- Joint Publication 3-12, applying the established U.S. definition of key terrain as "any locality or area, the seizure or retention of which affords a marked advantage to either combatant," defines cyber key terrain as "network links and nodes that are essential to a particular friendly or adversary capability."[11] The document embeds this definition in a section on "movement and maneuver" but does not further develop the concept.
- The *U.S. Army LandCyber White Paper 2018-2030*, aiming to describe the broad future of Army cyberspace operations, draws on the same underlying definition of key terrain in asserting the need to "identify key terrain on Army networks where critical applications reside and critical information is required to support ongoing military operations."[12] The occasional uses of the concept elsewhere in the document do not further develop the concept or identify any significant distinctions in applying the concept of key terrain in land or cyber domains.
- In a study devoted fully to "mapping the cyber terrain," the authors utilize definitions of cyber key terrain "those physical and logical elements of the domain that enable mission essential warfighting functions," and "physical and logical infrastructure and

9 See, for example, U.S. Army War College. *U.S. Army War College Key Strategic Issues Lists 2013–2014*. Carlisle, PA: Army War College, 2013, Question #5, p.31. This observation is also informed by the author's participation in the Cyberspace Key Terrain Workshop, Naval Postgraduate School, July 7-8, 2015.

10 Examples include: Rogers, Michael S., Commander, United States Cyber Command, *Statement before the Senate Committee on Armed Services*. 114th Cong. (2015), p.6; Caton, Jeffrey L., "Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications," Carlisle Barracks, PA; Strategic Studies Institute, U.S. Army War College, 2015, p. 30; Hernandez, Rhett, Commanding General, U.S. Army Cyber Command/2nd Army, *Statement before the House Armed Services Committee on*

Emerging Threats and Capabilities Concerning Digital Warrior: Improving Military Capabilities in the Cyber Domain. 112th Cong. (2012), pp. 5, 8; Deptula, Kendra, "Automation of Cyber Penetration Testing Using the Detect, Identify, Predict, React Intelligence Automation Mode," Master's thesis, Naval Postgraduate School, 2013, pp. 21-23; Alanis, Oscar, "Operational Art in Cyber Defense," Master's thesis, USMC Command and Staff College, 2010, pp.12-13.

11 Joint Chiefs of Staff. *Cyber Operations* (Joint Publication 3-12). Washington, DC: Joint Chiefs of Staff, 2013, p.II-10. The following section returns in more detail to this publication.

12 U.S. Army. *The U.S Army Landcyber White Paper 2018–2030*. Fort Meade, MD: U.S. Army Cyber Command, 2013, pp. 7, 43.

mission data."[3] This definition fits the technical and operations-level mapping exercise that the study undertakes.

- In a study aimed at the somewhat broader goal to increase cyber decision-making effectiveness through improved utilization of existing situational awareness knowledge, the author identifies "cyber key terrain" as a primary means by which the DoD and DHS have sought to operationalize "knowledgebases." This work defines cyber terrain as minimally "the logical ***information***, and physical (or virtual) ***networks***, ***systems*** *(hardware and software)* and ***devices*** that make up an organization's IT infrastructure," and "key" as the "criticality" of "*one's* ***dependency*** *on an asset*" (rather than "*an attribute of the asset itself*").[4] This definition, while open-ended, emphasizes the physical and data attributes of cyberspace.

  Subsequently, the work presents a "methodology" for identifying cyber key terrain utilizing "the doctrinal concept of "***key terrain***" from the land domain."[5] The work does not engage the fit of the land domain doctrine to cyberspace circumstances, particularly to virtual cyberspace dimensions.

- A study proposing a framework to establish "operationally relevant situational awareness of the cyberspace warfighting domain" specifies one of six required "data classes" to be: "Prioritized cyber key terrain that allows understanding of operational and technical risks."[6] Also utilizing the criterion of "criticality," this work defines cyber key terrain roughly as "all critical information, systems, and infrastructure; whether owned by the organization or used in transit by its information."[7] This definition expresses a typical focus on hardware and data.

[3] Bodeau, Deborah, Richard Graubart, and William Heinbockel. *Mapping the Cyber Terrain*. Bedford, MA: MITRE, November 2013, pp.1,3

[4] Foote, Scott. "Mission-Cyber Dependency Modeling: A Methodology." Document no. WN140101. Draft, The MITRE Corporation, McLean, VA, 2014, p. A-4. Italics and bold original.

[5] Ibid, p.A-8. Italics and bold original.

[6] Dressler, Judson, William Moody, Calvert L. Bowen, III, and Jason Koepke. "Operational Data Classes for Establishing Situational Awareness in Cyberspace." In *2014 6th International Conference on Cyber Conflict*, edited by P. Brangetto, M. Maybaum, and J. Stinissen. Tallinn: NATO CCD COE Publications, 2014, p.178.

[7] Ibid, p.180.

18 Ibid. This work's " hypothetical operational case study" does not help this issue: it stipulates that "the commander" has already identified his cyber key terrain at the outset.

More importantly, it provides no metric of criticality; the study itself immediately allows that "even these systems must be prioritized and may be less vital than a specific network link supporting a real-time airborne mission."[18] Accordingly, the authors later conclude:

"An efficient method for determining cyber key terrain to assure mission accomplishment has yet to be found."[8]

- A U.S. military master's thesis seeking to establish the preconditions for warfareoriented cyberspace doctrine directly asserts, "A basic understanding of the terrain of cyberspace is necessary to any credible doctrinal discussion on this domain." Having defined cyberspace narrowly as data management via networked systems of electronics and the electromagnetic spectrum, the work renders cyber terrain in wholly technical terms, and computer network defense as akin to fortification.[9] Although this work does not address the concept of key terrain directly, it makes numerous direct associations to physical characteristics; stating, for example: "Mountains or hills do exist in cyberspace in the form of signal bandwidth and data throughput constraints which make traversing certain cyberspace paths more difficult (like climbing uphill)."[10]

Some other analyses invoke more considered and/or broader definitions of cyber key terrain. Many of these efforts, while contributing to development of a robust concept of cyber key terrain, remain tethered to techno-physical conceptions.

In an early study of "key defensive terrain in cyberspace," Thomas Pingel argues that a physical conception of cyberspace is in fact a prerequisite to meaningfully determining cyber key terrain. The analysis begins by asserting that only by establishing metaphorically "the similarities between real space and the space in which computer networks exist" is it "then possible to provide a reasonable definition of what key terrain in cyberspace might be." Articulating this premise, the analysis declares that "Computer networks are spatial simply because they exist in our physical world." These networks'

"physical lines and information switches and protocols" constitute the "topology" of cyberspace. [11]

[8] Ibid, p.184. The authors here also validate their claims on the basis of their own " intensive operational experience working at the highest levels of command in the area of cyber situational awareness for the U.S. Department of Defense." Ibid, p.184.

[9] Cloud, "Integrated Cyber Defenses: Towards Cyber Defense Doctrine," pp. 11, 14-16, 18. The focus on fortification draws on Pingel, "Key Defensive Terrain in Cyberspace: A Geographic Perspective," discussed in this section.

[10] Ibid, p.22.

[11] Pingel, "Key Defensive Terrain in Cyberspace: A Geographic Perspective," pp.1-2.

Establishing this metaphorical association enables the analysis to then directly apply the U.S. Army definition of *key terrain* as "any feature, locality, or area which affords a marked advantage to the combatant who controls it."[12] Emphasizing the role of *fortification* in control of physical terrain and asserting the "astounding similarities between the methods of securing computer networks and fortifying cities" leads the analysis naturally to emphasize the role of firewalls and other barrier functions in computer network defense.[13]

Pingel's brief and early account is provocative but limited. While recognizing the role of metaphor in generating understandings of cyberspace, the assessment projects a single metaphor that effectively flattens the definition of cyberspace and precludes alternative conceptions of the challenge of cyber security (such as biological contagion or complex system resilience). The approach also implicitly renders the concept of cyber key terrain meaningful only to spatial cyberspace contexts, ironically limiting potential application of the concept to more virtual environments. Finally, the argument acknowledges no limitations to the spatial metaphor, treating it more as a literal association: cities and networks both face "a similar problem to be overcome."[14] Tellingly, though the work sets up to provide a "reasonable definition of what key terrain in cyberspace might be," it never provides a definition beyond the implicit extension of the traditional definition of earthly key terrain it invokes.

A more recent and developed account in a similar vein is provided by John R. Mills (in 2012, Special Assistant for Cybersecurity in the Department of Defense and a colonel in the U.S. Army Reserve). At first glance, Mills seems also to follow a physical conception of cyber key terrain – indeed, like Pingel, the premise of this assessment is that "traditional Clausewitzean key terrain concepts" apply to cyberspace precisely "because Cyber does have physical manifestations."[26] While this approach projects an implicitly physical definition of cyber key terrain,[27] the eight "earthly manifestations" of applying "Clausewitzean principles" to cyberspace that form the substance of the analysis in fact stretch the boundaries somewhat. Five elements (data centers, internet service providers, undersea cables, computer BIOS, and supply chains) are principally physical; but three others are less tangible: international standards bodies, the cyber workforce and innovation also count as "key terrain" for U.S. cyber security. Mills himself allows that cyberspace entails some "contemporary key terrain elements that

[12] Ibid,. p.2, citing United States Dept. of the Army, *Operations*. Department of the Army field manual; FM 100-5. 1986, Washington DC: Headquarters Dept. of the Army.
[13] Pingel, "Key Defensive Terrain in Cyberspace: A Geographic Perspective," pp.3-4
[14] Ibid, p.4
[26] Mills, John R. "The Key Terrain of Cyber." *Georgetown Journal of International Affairs* [special issue] (2012) 99–107, at p.99.
[27] Mills does not offer a definition of cyber key terrain itself, but invokes Clausewitz's general conception: "Key terrain refers to vital ground that needs to be obtained via military or security strategies." Mills, "The Key Terrain of Cyber," p.99, n.4.

Clausewitz might not have foreseen but would possibly include in an updated version of his theory of key terrain."[15]

But these elements, if less tangible, are still aspects of the corporeal world, consistent with the general category of "physical manifestations" that, in Mills rendition, make Clausewitzean conceptions of key terrain applicable to cyber in the first place.[16] International standards bodies, cyber workforces and innovation are not physical, geographic elements of cyberspace, but neither are they virtual elements; nor are these elements, in their general nature, unique to the cyber domain. Skilled workforces and sustained innovation capacity are critical to U.S. military capacities in all other domains.[30] International standards bodies, such as the Internet Corporation for Assigned Names and Numbers (ICANN) or the International Telecommunications Union (ITU), may be no more "key" to the control of cyberspace than the World Trade Organization (WTO) or International Monetary Fund (IMF) are "key terrain" in controlling the course of the global economy.

One of the most expansive treatments of the topic of cyber key terrain is provided in a recent assessment by Raymond, et.al. (three of the four joint authors are affiliated with West Point's Army Cyber Center).[31] Starting (as does Pingel) with the U.S. Army definition of "key terrain" as "any locality or area, the seizure or retention of which affords a marked advantage to either combatant,"[32] the analysis premises that applying the concept to cyberspace, despite added complexities, is equivalently vital to conflict success: "Whether on the kinetic battlefield or in cyberspace, understanding key terrain in your situation gives you a distinct advantage over an adversary who doesn't conduct this analysis."[33]

Importantly, this analysis recognizes that the concept of key terrain is not necessarily always physical even in traditional domains, noting General David Petraeus' assertion that in the U.S. conflicts in both Afghanistan and Iraq, "the key terrain is the human terrain."[34] Applying this recognition to cyberspace, the authors construct a notably encompassing conception of cyber terrain:

> As with human terrain, cyber terrain will not always be directly tied to a physical location, and may include operating systems or application software, network

[15] Mills, "The Key Terrain of Cyber," p.100.

[16] A recent consideration of "principles of war for cyberspace" remarks that the human-controlled malleability of the "cyber terrain," distinguishing cyberspace from other domains of conflict, is better interpreted by Sun Tzu's notion of " five different kinds of terrain" necessitating differing strategies from commanders than by " Clausewitzian kinetic options." This observation supports the view that applying Clausewitzean ideas of "key terrain" beyond the physical aspects of cyberspace is at best problematic. But this work does not delve further into the application of the concept of "terrain" to cyberspace or address the topic of "key terrain" at all. Cahanin, Steve E. "Principles of War for Cyberspace." Air University, 2011, pp.10-11.

> protocols, computing devices, and even individuals or virtual personas. The DOD does not define cyber terrain, so we will define it as *the systems, devices, protocols, data, software, processes, cyber personas, and other networked entities that comprise, supervise, and control cyberspace*.[35]

[30] See, for example, Pembleton, Gary L,. "Assessing Technology Innovation in the PLA," Master's thesis, Naval Postgraduate School, Monterey, CA, March 2015.

[31] Raymond, David, Gregory Conti, Tom Cross, and Michael Nowatkowski. "Key Terrain in Cyberspace: Seeking the High Ground." In *6th International Conference on Cyber Conflict*, ed. P. Brangetto, M. Maybaum, and J. Stinissen (287–300). Tallinn: NATO CCD COE Publications, 2014. http://www.usma.edu/acc/siteassets/sitepages/publications/06916409.pdf

[32] Ibid, p.288, citing the Department of the Army Field Manual 3-90-1: Offense and Defense Volume 1, 2013 [np]. [33] Ibid, p.288.

[34] Ibid, pp.289-90.

[35] Ibid, p.290. Italics original.

These authors' definition of "cyber key terrain" follows directly from application of the traditional definition of "key terrain" to this encompassing conception of "cyber terrain": "[W]e define cyber *key terrain* as systems, devices, protocols, data, software, processes, cyber personas, or other network entities, the control of which offers a marked advantage to an attacker or defender."[17] Usefully, the analysis then develops examples of how this definition can be applied at multiple "layers" of cyberspace, though it does not articulate the concept itself at each layer (the following section engages in more detail this article's application of cyber key terrain to multiple cyberspace layers).[18]

Notably, Raymond et. al. also appreciate that the concept of key terrain, while "most commonly applied at the tactical level of warfare," is "relevant at the strategic and operational levels as well."[19] Accordingly, the assessment articulates the cyber key terrain concept at each level: tactical cyber key terrain involves advantage to attack or defense of a network; operational cyber key terrain offers "an advantage in a specific campaign or major operation;" strategic cyber key terrain, though not precisely defined, could involve things like network device supply chains, nuclear launch systems, or a presidential candidates email account. Crucially, however, the authors also acknowledge that "tactical actions could have operational or strategic consequences …

[17] Ibid, p.294. Italics original.

[18] Ibid, p.295.

[19] Ibid, p.289.

depending on the context."[20] This discussion, original for broaching the topic, is too brief to consider how such contexts can be assessed for planning and decision-making purposes in cyberspace contexts, in which highly tailored cyber operations could generate considerable strategic impact, particularly collaterally. The authors' abbreviated discussion of Stuxnet at the operational level exemplifies this challenge.[21]

The genesis of the concept of cyber key terrain in these works explains why most uses focus on the most physical attributes of cyberspace. First, several works explicitly apply the U.S. military definition of key terrain that emphasizes the tactical importance of possession of tangible spatial assets. Secondly, some works assert that the concept of key terrain is applicable to cyberspace *particularly because* cyberspace has physical attributes
(e.g. routers and electromagnetic signals), implicitly suggesting that applicability of the concept may be limited to these physical aspects. But none of the works reviewed in this section make that delimitation explicitly.

This genesis thus raises two related questions. First, can there be a concept of cyber key terrain relevant across all dimensions of cyberspace in which conflict may take place?
Second, if not, would the inapplicability of the concept in the virtual planes of the cyber domain qualify its application to operational and strategic doctrine that must grapple with cyber security challenges holistically? Answers to these questions depend on the relative importance of the virtual dimensions of cyberspace to cyber security fundamentally. The following section takes up these issues

Key Terrain and Cyberspace Layers

As discussed in the preceding section, definitions of cyber key terrain tend to focus on the physical aspects of cyberspace. However, broader discussions of the security challenges in cyberspace frequently envision the realm more expansively. In particular, a number of U.S. government and non-governmental assessments view cyberspace as constituted by multiple elements or "layers," of which physical attributes form only component. These definitions commonly emphasize the importance of non-physical (e.g. logical or persona) elements or layers as equivalent forums for conflict and force projection.

[20] Ibid, p.296.

[21] Ibid.

A good example is Joint Publication 3-12.[22] This document, intended to provide definitions and doctrine for all armed forces, depicts cyberspace in terms of "three layers: physical network, logical network, and cyberpersona."[42] (See Figure 1)

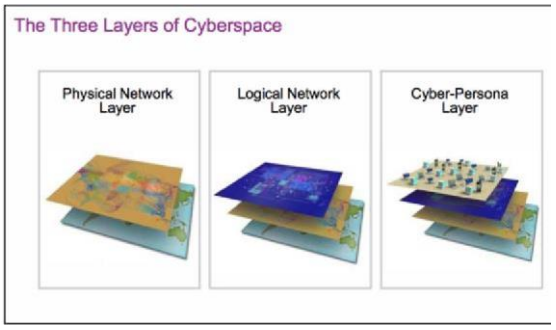

Figure 1: JP 3 -12 Depiction of Cyberspace

Notably, JP-3-12 offers definitions for, and assessments of the security requirements of, each layer: Layers

- "The physical network layer of cyberspace is comprised of the geographic component and the physical network components. It is the medium where the data travel. … The physical network component is comprised of the hardware, systems software, and infrastructure … [but] uses logical constructs as the primary method of security." [23]
- "The logical network layer consists of those elements of the network that are related to one another in a way that is abstracted from the physical network, i.e., the form or relationships are not tied to an individual, specific path, or node." [24]
- "The cyber-persona layer represents yet a higher level of abstraction of the logical network in cyberspace; it uses the rules that apply in the logical network layer to develop a digital representation of an individual or entity identity in cyberspace. … However, one individual may have multiple cyber-persona, … [and a] single cyberpersona can have multiple users." [45]

Within this construct, the attention JP 3-12 pays to the concept of cyber key terrain is decidedly limited. As noted above, JP 3-12 defines cyber key terrain only in terms of "network links and nodes that are essential to a particular friendly or adversary capability."[46] This limited application contradicts the doctrine's broader depiction of cyberspace, and in particular the extensive treatment it offers to security challenges at the persona layer. The contradiction is starkest in the context of the doctrine's definition, which is offered in a section on "movement and maneuver" that goes on to conclude, "Movement and maneuver in cyberspace can occur in all three layers: the physical network, logical network, and the cyber-persona layer."[47] A concept of cyber key terrain defined in terms of the physical layer cannot be applied to challenges of

[22] Joint Chiefs of Staff. *Cyber Operations* (Joint Publication 3-12). Washington, DC: Joint Chiefs of Staff, 2013.
[42] Ibid, p. I-2.
[23] Ibid, p. I-3.
[24] Ibid, p. I-3. [45] Ibid, pp. I-3-4. JP 3-12 notes the particular challenges that the cyber-persona layer presents for gaining "situational awareness" sufficient to " enable effective targeting and creation of the JFC's desired effect." Fanelli and Conti also previously observed: " Physical personas and cyber personas often exist in one-to-

movement and maneuver in non-physical layers of cyberspace. If in principle "movement and maneuver" are relevant at all layers, and "key terrain" is a vital concept for "movement and maneuver," then a concept of cyber key terrain applicable to virtual as well as physical layers of cyberspace is required.

A similar disjunction emerges from the *U.S Army Landcyber White Paper*. Recognition of the multi-layered nature of cyberspace is less developed but still explicit. The initial discussion depicts cyberspace as "terrain that sustains collective activity and shapes the security related behavior of humans and their machines," and the glossary defines
"cyberspace terrain" as the "Physical and non-physical terrain created by and/or composed of the human layer, logical layer, and physical layer."[48] Yet discussion of the role of terrain and key terrain in cyberspace throughout the rest of the document consistently omits specific attention to the human, cognitive and virtual dimensions of the cyberspace environment, instead applying the concept generically or focusing on critical information, network sensors, signals integrity and infrastructure.[49]

Tellingly, the *Landcyber White Paper*'s one mention of "cyberspace personas" is to assert the "rising premium on conventional and special operations forces' ability to consider the human aspects of conflict and cyberspace operations."[50] This brief discussion overlooks recognition elsewhere (e.g. JP 3-12) that cyber personas are often independent of single individuals, and can live on without them. Indeed, the suggestion that special operations forces are the first answer to persona threats ignores how cyber personas sometimes can be combatted only within cyberspace itself.

many or many-to-many relationships. A person may have multiple cyber personas while a single cyber persona may in fact represent multiple, loosely related persons." Fanelli, Robert, and Gregory Conti. "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict." In *2012 4th International Conference on Cyber Conflict*, edited by C. Czosseck, R. Ottis, and K. Ziolowski 319–331). Tallinn: NATO CCD COE Publications, 2012, p.326

46 Joint Chiefs of Staff. *Cyber Operations* (Joint Publication 3-12), p.II-10.

47 Ibid, pp. II-10-11.

48 U.S. Army. *The U.S Army Landcyber White Paper 2018–2030*, pp. 6, 46.

49 Ibid, pp. 7, 8, 11, & 17.

50 Ibid, p.22.

Many definitions and assessments of cyber key terrain do not address virtual cyberspace elements or layers. Some works, having defined cyber key terrain in wholly physical

and technical terms, simply do not engage a broader conception of cyberspace.[25] In other cases, definitions with greater potential scope are truncated by absence of full consideration of their application to logical and especially persona cyberspace layers:

- The full study devoted to "mapping the cyber terrain," noted above, adopts of definition of cyber key terrain that nominally includes physical and logical attributes. But the study focuses on technical and operational elements of cyberspace security, developing a mapping methodology for networks and systems. The study does not project a multi-layered conception of cyberspace (e.g. including a "persona" dimension) or address cognitive-level cybersecurity threats.[26]

- The Foote study aiming to improve utilization of existing situational awareness knowledge provides a definition of cyber key terrain that is in principle open-ended by focuses on the physical and data attributes of cyberspace.[27] In subsequently offering a methodology for identifying cyber key terrain, the work identifies one step entailing identification and prioritization of "critical assets" within the "Physical, Logical, and Cyber-Persona layers of cyberspace."[28] The work does not elaborate implementation of this step or consider the unique challenges posed by identifying "critical assets" in virtual (logical or persona) environments.

- John R. Mills application of Clausewitz's concept of key terrain to identify eight key cyber elements does stretch the boundary of the purely physical (as discussed in the previous section). But this study offers no explicit definition of either cyber key terrain or cyberspace generally, and the less tangible key cyber elements it identifies (international standards bodies, the workforce and innovation) are organizational and

"home front" qualities relevant to any domain. The study does not project a multilayered conception of cyberspace and, accordingly, does not seek to identify cyber key terrain at any non-physical or virtual level.[55] Indeed, because this assessment argues that Clausewitz's concept of key terrain is applicable to cyber precisely because cyber *has* physical manifestations, it implicitly ratifies the

[25] For examples, see Dressler, et.al., "Operational Data Classes for Establishing Situational Awareness in Cyberspace;" Pingel, "Key Defensive Terrain in Cyberspace: A Geographic Perspective;"
[26] Bodeau, Deborah, Richard Graubart, and William Heinbockel. *Mapping the Cyber Terrain*. Bedford, MA: MITRE, November 2013.
[27] Foote, Scott. "Mission-Cyber Dependency Modeling: A Methodology," p. A-4.
[28] Ibid, p.A-10.
[55] Mills association of the cyber workforce with key "human terrain" (Mills, "The Key Terrain of Cyber," p.104; cf. pp.99-100) offers an intriguing opportunity for broadening the concept of cyber key terrain into the persona layer of cyberspace. Mills does not develop this association.

critique that the concept of key terrain is meaningless at the virtual layers of cyberspace.[29]

- The U.S. Army's *Cyber Electromagnetic Activities* Field Manual identifies three "physical," "logical" and "cyber persona" cyberspace layers, the latter of which is a "digital representation of an individual or entity identity in cyberspace," as in JP 3-12. The discussion recognizes that cyber persona identities are complex, can include social media projections, and are "normally not linked to a single physical location or form." The virtual layers, however, have few roles in the rest of the framework, and the concept of terrain in relation to cyberspace is barely mentioned.[57]

- Similarly, the U.S. Army's *Cyberspace Operations Concept Capability Plan 2016-*

2028 identifies three somewhat less similar cyberspace layers: "physical," "logical" and "social." The social layer includes the *cyber personas* distinct from individuals (often in many-to-one relationships). But this document sees personas only as catalogs of email addresses, cell phone numbers, and other online points of access, rather than as identity projections. Perhaps related to this truncated conception, the document references the role of "terrain" only minimally in non-cyber contexts.[58] Raymond et.al. provide a notable exception to the general tendency of discussions of cyber key terrain to collapse its application to a physical layer of cyberspace defined by routers and cables. This analysis posits five cyberspace levels:[59]

- Supervisory plane (involving command and control of cyber operations)
- Cyber persona plane (involving "identities" such as user accounts and credentials)
- Logical plane (involving operating systems, applications settings, and logical links between networked devices)
- Physical plane (involving computers and associated hardware)[60]
- Geographic plane (involving the actual location of information systems)

This analysis is one of the few to recognize that if cyberspace is constituted by multiple planes, and meaningful conflict can occur at any of these planes, then a robust cyber key terrain concept needs to be applicable at any plane, at least in principle. However, this

Greg Rattray, Chris Evans, and Jason Healey, "American Security in the Cyber Commons," *Contested Commons: The Future of American Power in a Multipolar World*: 140. (See Mills, p. 99, n.3). Rattray et.al. in that chapter support Mills' view that " cyberspace is fundamentally a physical environment," as against the view that

[29] Mills, "The Key Terrain of Cyber." In critiquing the view that " we were released from the earthly bondage of brick and mortar infrastructure into cyber's non-existent land of ones and zeros," Mills cites

"cyberspace transcends geographic and national boundaries, and therefore strains traditional notions of sovereignty and security." But this latter work still depicts cyberspace as comprised of both "physical and logical systems," comparable to " complex self-organizing systems, called scale-free networks." That latter work does not address the topic of cyber key terrain.

57 Headquarters, Department of the Army, *Cyber Electromagnetic Activities* (FM 3-38). Washington, DC: Headquarters, Department of the Army, 2014, pp. 3/8-9, 6/12-13.

58 Headquarters, Department of the Army. *Cyberspace Operations Concept Capability Plan 2016–2028*.

TRADOC PAM 525-7-8. Washington, DC: Headquarters, Department of the Army, 2010, pp. 8-9, 40, 70.

59 Raymond, et. al., "Key Terrain in Cyberspace: Seeking the High Ground," p.291-2, 295. This depiction draws on an earlier depiction by the lead offer. In practical terms, these five layers effectively incorporate the three presented by JP 3-12 and add two others, one each "above" and "below."

60 The authors note that this is the plane, which includes routers and networking equipment, that "people often interpret as being cyber terrain" in its entirety. Ibid, p.291-2.

article's application of cyber key terrain to these cyberspace layers is brief and consists mainly of offering examples rather than articulating categories. Moreover, those examples suggest a still-limited appreciation of the scope of some conceived layers.

Examples of the supervisory plane – botnets, wireless command and control channels, nuclear launch systems – are not in their nature distinct from the logical or physical layers: the importance of the "supervisory" nature of these cyberspace elements seems almost synonymous with identifying "key terrain" in these other layers.[30]

Examples at the cyber persona layer convey a particularly flat conception. The analysis importantly appreciates at the outset that cyber persona identities "might have a many-toone or one-to-many relationship with physical individuals."[31] But the examples offered focus on access to the accounts of specific people: system administrators, military commanders or political leaders.[32] These examples hardly reflect the essence of the persona layer idea, which is conflict involving vying projections of identities in cyberspace, not access to the accounts of specific individuals.[64]

In its most meaningful sense, the persona layer identifies the importance of using networked communications to conduct contests of ideology and allegiance over populations of any scale in very short time frames. A prominent current example is the use of social media for ISIS recruitment. Hacking an ISIS system administrator hardly joins that battle over "hearts and minds." In a sense, the persona layer is the most "human" of the cyberspace layers. Insofar as Raymond et.al. recognize the

[30] Ibid, pp.295-6.
[31] Ibid, p.291.
[32] Ibid, pp. 295-6. 64 An earlier work upon which Raymond et.al. draw offers a depiction of the persona layer recognizing this identity projection role, citing the international cyber hacking group "Anonymous" as an example. See Fanelli and Conti, "A Methodology for Cyber Operations," p.326

importance of "human terrain" outside cyberspace,[33] the underappreciation in this analysis of the real "terrain" at the persona layer is a conspicuous void.

A straightforward conclusion arises from the material reviewed in this section: Definitions of cyber key terrain that focus on physical cyberspace attributes fail to synchronize with depictions of the security challenges of cyberspace as also spanning multiple virtual layers. Yet these broader depictions of cyber security challenges uphold the relevance of strategic, operational and tactical thinking in meeting those challenges.[34]

Applicability of the Key Terrain Concept

The disjuncture between physical-layer definitions of cyber key terrain and broader multi-layered conceptions of cyberspace raises directly the question of whether the concept of cyber key terrain has meaning for facing security challenges at non-physical (virtual) cyberspace layers. For example, one analysis of cyber defense, building on the physical-layer-only DoD definition of cyberspace as "a global domain … consisting of the interdependent network of information technology infrastructures," nevertheless emphasizes the importance of distinguishing "the place—cyberspace—from the activities that occur within that place." Accordingly, the cyber domain is unique in "the flexibility of the terrain in cyberspace and the lack of requirement to defend *specific* terrain."[35]

> Rather than defending a piece of territory or area of airspace, cyber defenses are concerned with protecting content and function. If organized, planned, and exercised properly, any compromised component of a network could be isolated and even discarded while the functions and data continue to exist in the remaining elements or are rerouted to new infrastructures. … This unique characteristic of cyberspace should figure prominently in any integrated defensive strategy.[68]

While this particular analysis does not investigate the topic of "key terrain," the implication is clear: in cyber security doctrine and practice properly attending to "function" rather than "place," the idea that defense is achieved by seizing or holding "terrain" may be misguided.

Thus, the necessarily more abstract and metaphorical nature of the concept of key terrain in more virtual layers of cyberspace begs a deeper question: does the underlying premise of the concept of key terrain hold at these layers? That is, are the requirements

---

[33] Raymond et. al., "Key Terrain in Cyberspace: Seeking the High Ground," p.290

[34] For a good discussion of this point more generally, see Gray, Colin S., "Making Strategic Sense Of Cyber Power: Why The Sky Is Not Falling," Strategic Studies Institute and U.S. Army War College Press, April 2013.

[35] Fahrenkrug, David T. "Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy." In *2012 4th International Conference on Cyber Conflict*, edited by C. Czosseck, R. Ottis, and K. Ziolowski (197–207). Tallinn: NATO CCD COE Publications, 2012, pp.198-99. [68] Ibid, p.199.

for prevailing in conflict at virtual layers of cyberspace best thought of in spatial terms distinguished by "ours," "theirs" and the contested spaces in between? What if the nature of virtual cyber conflict is better captured by alternative frames of thinking (such as a biological conception emphasizing diagnosis and recovery, or a complex systems conception emphasizing resilience and recovery)? If conceiving virtual cyber conflict in terms of seizing and holding some portion of that virtual environment fundamentally misrepresents the nature of virtual cyber conflict, then policies and doctrines built on that frame of reference will have poor chances of consistent success.

At best, making the concept of key terrain relevant to the fullest conceptions of cyberspace security challenges would require development of a more generic and abstracted understanding of the concept that would be meaningful in the dynamic, virtual and social environments of the cyber domain. However, because applying the concept of key terrain to non-physical cyberspace is necessarily more metaphorical and abstracted, its utility may also be more limited. Efforts to develop that application should be attuned to the potential limitations as much as inquisitive of the possibilities.

These observations have implications for utilizing the concept of cyber key terrain at operational and especially strategic levels of doctrine and planning. Strategy in any domain requires the fullest possible understanding of conflict integration and implication; that is, how any action may generate ancillary effects influencing ultimate outcomes. In cyberspace, a tactical question might deal exclusively with physical or tangible assets, but cyber strategy must take into account the potentially ubiquitous interplay of actions and effects across all layers.[36] Thus, a strictly physical conception of "key terrain" in cyberspace may be useful in certain specified tactical contexts, but will be decreasingly relevant at increasingly integrated and holistic levels of war-planning concern. Strategy, which must grapple with cyber security challenges integratively, minimally requires an articulation of the concept of "cyber key terrain" seminal enough to encompass both more literal and more abstracted applications.

Combining these points suggests that utilization of the concept of key terrain is more challenging as its application moves from the physical to the logical and persona layers of cyberspace, and as its application moves from tactical to operational and strategic planning challenges. If today's colloquial conceptions of key terrain are readily meaningful to interpret a physical tactical challenge (such as insuring the networking integrity of a naval battle group), those conceptions are equally insufficient for developing a strategy of victory at the persona layer (such as defeating ISIS use of social media to generate global allegiance and radicalization).

[36] In one view, cybered conflict not only enters into tactics, operations, and strategy, but blurs the boundaries between these levels. See Dombrowski, Peter, and Chris C. Demchak. "Cyber War, Cybered Conflict, and the Maritime Domain." *Naval War College Review* 67, no. 2 (2014): 71–97, at p. 74.

Conclusion

These questions raise a dilemma for military planning. The United States, and the world historically, have generated a wealth of knowledge and doctrine for succeeding in conflict. Technological and social evolution requires attentive updating of doctrine and policy to best achieve the ultimate objective: prevailing in conflict. The demands of the information age do not alter this basic historical dynamic. As cyberspace has emerged as a distinct domain of conflict with its own unique environmental properties, organizational efficiency naturally suggests the search for translation and application of prior knowledge as far as is possible. Mapping the concept of key terrain into the techno-physical aspects of cyber conflict is an example.

Unfortunately, this natural organizational dynamic risks over-emphasizing the conventional aspects of cyber conflict and overlooking its most novel features. Prevailing in conflict at more virtual layers of cyberspace, and in particular the persona layer characterized by contests of identities in social spheres, may require more original frames of reference. Organizational military processes work against such original thinking. But failing to engage cyber strategy at this level, and instead building military doctrine and operational practice on prepared and familiar understandings of conflict, risks planning to fight the last war rather than the next one.

At the same time, embracing a belief that a "cyber revolution" has dismissed the relevance of known strategy and doctrine is also a recipe for failure. Even if prevailing in conflict in the cyber domain requires original conceptions of strategy, the urgency of the security threats the U.S. military currently faces do not allow the luxury of wholesale reconstruction of doctrine and practice.

Thus, decision-makers face a genuine dilemma. There is no easy reconciliation. Policymakers and commanders equally must find the appropriate balances between applying existing knowledge and doctrine to cyberspace while vigilantly probing for the limitations of those applications.