U.S. Air Force B-52 Stratofortress, B-1 Lancer, and B-2 Spirit launch from Andersen Air Force Base, Guam, for integrated bomber operation, August 2016 (U.S. Air Force/Richard P. Ebensberger)

Searching for Digital Hilltops

A Doctrinal Approach to Identifying Key Terrain in Cyberspace

By Scott Douglas Applegate, Christopher L. Carpenter, and David C. West

During the 1991 Gulf War, the U.S. military delivered a crushing defeat to the Iraqi army in one of the most one-sided battles in history.[1] A concept known as net-centric warfare was partially responsible for this victory and marked the first real integration of information technology (IT) into combat systems on a large-scale basis. Net-centric warfare is characterized by the integration of computer and networking technologies into every functional area of operations, which can increase performance, enhance intelligence, and improve efficiencies in order to greatly increase combat power.[2] While still in its infancy, net-centric warfare increased commanders' situational awareness and enhanced their ability to deliver overwhelming combat power to decisive points on the battlefield. However, the pervasive introduction of IT into combat systems has created both opportunities and vulnerabilities. The need to defend or exploit these systems eventually led the Department of Defense (DOD) to designate cyberspace as a new warfighting domain through which combatants are able to conduct a new breed of military operations.

Just as planners must characterize the operational environment in the physical domains, cyberspace operators and planners must do so in this new warfighting domain. Defining the operational environment includes identifying critical assets, centers of gravity, avenues of approach, decisive points, and key terrain. Particularly problematic issues such as the misidentification of key terrain

Lieutenant Colonel Scott Douglas Applegate, USA, is a Joint Action Officer and Strategic Planner for the Cyber Policy Division, Joint Staff J5. Major Christopher L. Carpenter, USA, is a Joint Staff Officer, J35, United States Forces, Korea. Lieutenant Commander David C. West, USN, is an Information Professional serving as the N6 to Naval Special Warfare Group One.

in cyberspace, the absence of effective cyberspace doctrine that defines concepts and terms in coordination with the other warfighting domains, and the lack of cyberspace knowledge by operational planners within the joint force have greatly stymied the ability of the U.S. military to operate effectively in this domain. To do so, the military must create a common lexicon and clarify the concepts and processes of identifying key terrain in cyberspace within joint doctrine.

Background

Cyberspace is different from the physical warfighting domains of land, sea, air, and space. It is a nonphysical realm consisting of the interdependent networks of IT infrastructures and resident data, including the Internet, telecommunications networks, computer systems and embedded processors, controllers, and even the individuals who interact with these systems.[3] It is home to a new kind of warfare that seeks to disrupt, deny, degrade, distort, or destroy the information and/or systems necessary to employ military power in the physical domains. As IT creates a more interconnected world, operations in cyberspace are shifting from a secondary defensive role to an alternate means of applying military power parallel to or in conjunction with the other warfighting domains. A new battlespace is emerging where attribution is difficult and the players range from nation-states and military commands to criminal organizations and lone operators. The relatively low cost of entry to this battlespace compared to the physical warfighting domains can allow small nation-states and even nonstate actors to compete. Additionally, cyberspace operations (CO) asymmetrically favor the attacker. Defenders must secure their entire infrastructure and every system, whereas an adversary need only find a single weakness in a target's defenses to employ cyberspace effects.

CO can deliver unique capabilities and combat power through cyberspace, but the U.S. military does not act in a unified manner when conducting these operations, especially when acting in concert with other warfighting functions.[4] The U.S. military concentrates offensive efforts under U.S. Cyber Command (USCYBERCOM), while Defensive Cyberspace Operations are spread at echelon between the Defense Information Systems Agency and the Services' chains of command.[5] This dispersed responsibility requires coordination in order to be successful, but the inability to identify key terrain in cyberspace and the lack of mature joint cyberspace doctrine create gaps, redundancies, and confusion between the Services and across the different echelons of command. Ultimately, the absence of a common CO lexicon and multiple interpretations of operational concepts lead to a waste of resources and an overall degraded operational posture in cyberspace. We now turn to an examination of overlooked and misunderstood aspects of cyberspace operations.

Previous Efforts to Identify Key Terrain in Cyberspace

Numerous researchers, planners, and practitioners have attempted to define cyber key terrain in cyberspace as the military has increasingly integrated cyberspace into its operations over the last three decades. These previous efforts suffered from three key flaws or omissions in their methodologies. First, in almost every case, the researchers focused on *what* items should be considered key terrain rather than on *how* to identify key terrain in a contextual manner. Second, previous efforts omitted the planning concepts of objective and mission, which are essential to identifying key terrain for a military operation. Finally, these efforts often confused or misidentified key terrain with critical assets. These flaws left planners struggling to grasp the concept of key terrain in cyberspace and, more importantly, grappling with how to implement this concept in an efficient and effective manner during planning and operations.

The most consistent trend noted across the research efforts to identify key terrain in cyberspace was a desire to create lists of devices, logical constructs, personas, and processes that constitute *cyber key terrain*. In the article "The Key Terrain of Cyber," John Mills identifies eight areas of focus in his efforts to define the terrain of cyberspace: data centers, commercial Internet service providers, undersea cables, international standards bodies, basic input/output systems, supply chains, cyber workforce, and innovation. Mills identifies all of these focus areas as key terrain, which leaves the reader with the impression *all* terrain is key.[6] In the article "Key Terrain in Cyberspace: Seeking the High Ground," the authors argue that key terrain exists in the geographic, physical, logical, cyber-persona, and supervisory planes of cyberspace. Furthermore, the authors 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.[7] The problem with these laundry lists of items is that they lack context and leave the reader with the impression, again, that absolutely everything in cyberspace is key terrain. The lists tell a reader *what* to look *at* rather than teaching them *how* to look *for* key terrain. A planner cannot determine what constitutes key terrain in cyberspace outside the context of the mission and the objectives of that mission.

A critical omission in previous research efforts is the failure to tie key terrain to objectives or missions. Researchers consistently attempt to identify key terrain in a vacuum. Key terrain is only *key* because it gives an advantage to an attacker or defender in relation to the achievement of mission objectives. Deborah Bodeau, Richard Graubart, and William Heinbockel touch on the need to identify "key cyber terrain, critical assets, or crown jewels" and discuss the importance of context in their 2013 work on the subject. However, they never define that context in terms of specific military missions or mission objectives. Instead, they suggest a series of questions and potential sources for information that planners could use across a variety of topics to identify key terrain.[8]

Key Military Definitions

Mission: The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore.

Objective: The clearly defined, decisive, and attainable goal toward which every operation is directed; the specific target of the action taken that is essential to the commander's plan.

Key Terrain: Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant.

Critical Asset: A specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively.

Critical Asset List: A prioritized list of assets or areas, normally identified by phase of the operation and approved by the joint force commander, that should be defended against air and missile threats.

Defended Asset List: A listing of those assets from the critical asset list prioritized by the joint force commander to be defended with the resources available.

The third flaw noted is the lack of a common lexicon and the consistent misuse of doctrinal terms in relation to key terrain in cyberspace. A number of authors use the terms *critical assets* and *key terrain* synonymously, implying these terms are interchangeable when they are not. Bodeau, Graubart, and Heinbockel discuss the importance of identifying "key cyber terrain," yet when they describe their process, they substitute the term *critical assets* for key terrain and lump together "key terrain, critical assets or crown jewels" as though they have identical meanings.[9] IdeaScale, a commercial vendor training DOD Cyber Protection Teams to identify key terrain during their missions, also uses the terms *key terrain* and *crown jewels* interchangeably.[10] The imprecise use of these terms by academics and trainers implies a lack of understanding of the difference between critical assets and key terrain. DOD defines a critical asset as "a specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively."[11] There are almost certainly assets in the cyberspace domain that could be defined as critical, and their identification should be prioritized due to the potential impact on national security. However, defining and protecting critical assets should not be confused with identifying key terrain. Understanding how the identification of critical assets shapes the identification of key terrain during a mission is important to the success of our cyberspace planners. This process allows planners to prioritize critical assets, create a Critical Asset List, determine which assets should be defended, develop a Defended Asset List, and then identify key terrain in relation to these assets and mission objectives. Defining these terms and imparting a common understanding to practitioners and planners will better enable the identification of key terrain in the context of mission objectives. To that end, this article provides a list of key joint doctrinal definitions of the relevant terms to the reader (see sidebar).[12]

Flaws and omissions in previous research efforts imply that planners and practitioners working in cyberspace may lack understanding or knowledge of doctrinal planning processes used in the physical domain. Planners in these other domains, especially Army and Marine Corps planners, have efficient and effective processes for identifying key terrain that are integrated into both the Services' and the joint planning processes. It is thus important for planners working in cyberspace to understand how these processes are accomplished in the physical warfighting domains. Often, simply removing the *cyber* concept from complex problems in the cyberspace field leads to better understanding and better solutions to seemingly wicked problems.

Key Terrain in the Physical Domains

It is important to define key terrain and the process for identifying it in the physical domain. One of the best tactical explanations for identifying key terrain can be found in Army Field Manual 3-21, *The Infantry Rifle Company*. The manual first discusses key terrain in the third step of the company commander's Troop Leading Procedures (TLP), which is the planning process conducted by tactical-level commanders. The TLP process runs parallel to the higher echelon's military decisionmaking process. Because company commanders lack a planning staff, the TLP process is tailored to simplify the planning process without missing the necessary steps for mission accomplishment.[13]

One of the most important aspects for any commander is to understand their operational environment. Army commanders have historically used the acronym *OAKOC*, which stands for Observation and Fields of Fire, Avenues of Approach, Key Terrain, Observation, and Cover and Concealment, to help in identifying the categories needed to analyze terrain.[14] Commanders must understand what terrain is important to their mission accomplishment. Properly identifying key terrain can mean the success or failure of missions at all levels of war. Focusing on the tactical-level doctrine best explains the process of identifying key terrain, as strategic-level doctrine tends to tackle this process too abstractly and assumes a level of understanding that is often absent.

Once commanders are given their mission and begin their analysis to understand the operational environment in which their element will fight, they will naturally focus on certain areas of terrain. A continued analysis will lead the commanders to determining whether there is key terrain to their mission success. The other factors of OAKOC will help commanders gain a better understanding of their environment and will ultimately aid

Cyber Flag 14-1 participants analyze exercise scenario in red flag building at Nellis Air Force Base, Nevada, November 2013 (U.S. Air Force/Christopher Tam)

them in their ability to define what terrain is worth fighting to control. The commanders will continue planning but at all times will ensure that they are protecting or dominating the areas that they defined as key. They will tie these pieces of terrain to objectives and task their subordinate elements to ensure that their force owns these areas or a combination of these areas throughout the operation.

Context Matters

When defining key terrain, planners must understand that context matters. Key terrain is situation- and context-dependent, or relative to specific objectives of a given mission. Understanding this point will aid in joint planners' ability to remain involved throughout the entire Joint Operations Planning Process (JOPP). It is important for planners, regardless of function or expertise, to understand where they fit into the planning process. It is equally, if not more, important for planners to be able to transition from strategic and operational to tactical objectives and vice versa.

When planners receive a mission, the planning process begins with gaining an understanding of the operational environment. This step is critical throughout all levels of war, but one can argue that depending on the level at which the operation occurs, the key terrain will be different. The major difference originates in the narrowing scope, span of control, and objectives resident at each level of war: strategic, operational, or tactical.[15] Tactical-level operations will identify specific requirements and capabilities needed to achieve their objectives, which are nested under the achievement of the operational and strategic objectives. Although the desired endstates may be similar, if not the same, the objectives will be substantially different as commanders at each level of war focus on objectives within their scope and areas of responsibility and influence. The difference in the objectives at each level of war will result in the identification of different critical assets and key terrain at each level. In many instances, the key terrain identified at the tactical level may be some of the same features identified at the operational level, but tactical-level commanders will always focus on terrain within their areas of operation specifically identified to increase their advantages for mission accomplishment.

Key Terrain Is Key Terrain

The importance of context highlights two key problems in the cyberspace domain. First, there is significant confusion in terminology within the CO community. The definition for key terrain is specifically defined in joint doctrine, but the CO community as a whole has spent a substantial amount of time and effort trying to create a separate definition just for cyberspace. Additionally, there is a tendency to use terms such as critical assets and

Two U.S. Marine Corps MV-22B Osprey tiltrotor aircraft participate in Valiant Shield 2014 in Tinian, Northern Mariana Islands, September 2014 (DOD/Alex Walters)

key terrain interchangeably. Second, there is a tendency to focus on tactical terrain at all levels within the CO community. USCYBERCOM, a sub-unified command that should arguably be operating at the operational and strategic levels of war, is often focused at the tactical level. The technical complexity and vast size of cyberspace push one to think that key terrain must be more complicated. This leads to a single organization trying to define key terrain across an entire warfighting domain. That belief is flawed and could be simplified if the community focused on specific, mission-related objectives within its span of control. These efforts must be decentralized and pushed down to the appropriate headquarters at each level of war.

Defining key terrain in cyberspace should follow the same doctrinal processes as the identification of key terrain in any of the other warfighting domains. There is no need to create a separate definition for *cyber key terrain*, as the joint definition for key terrain is adequate and applicable across all domains. Planners at the appropriate levels should seek to identify key terrain in relation to the specific objectives of their missions. This involves developing an understanding of the operational environment, to include the cyberspace aspects of that environment, evaluating terrain from an OAKOC perspective, determining critical assets, and identifying terrain that gives the attackers or defenders a marked advantage in relation to achieving their mission objectives. What makes key terrain key terrain is the context of the feature in relation to mission and objectives. The terrain may be any of the features listed earlier, but it is the context that really matters. Approaching the problem of identifying key terrain in cyberspace from this perspective should help planners at all levels to better understand and frame the problem.

Recommendations

The Joint Chiefs of Staff should add guidance to Joint Publication 3-12, *Cyberspace Operations*, to assist planners in the identification of key terrain within the context of missions and objectives. This will prevent cyberspace planners from operating in a vacuum and failing to align their operations to the overall mission. Additionally, the Joint Chiefs should consider updating doctrine to emphasize the use of the joint functions to evaluate operations in cyberspace at all levels of planning, just as they do in the physical domains.

A joint lexicon should be immediately established to enable the synchronization of CO across the joint force. This would include updating the definition of the

Critical Asset List to include cyberspace threats. A suggested definition is: a prioritized list of assets or areas, normally identified by phase of the operation and approved by the joint force commander, that should be defended against air, missile, and cyberspace threats.

A final recommendation is that CO should be integrated into both the joint education process and JOPP as a standard part of an operations planning team. Cyberspace operations affect all the physical domains and every joint function. Planners must be familiar with the effect that cyberspace consequences can have on their domain and with how the operations in their domain can affect CO. While CO may be a highly technical field, a joint planner only needs to understand the *what* to look for of CO and not the *how* to look. When CO is properly represented in the joint planning process, the planning group will rely on its cyberspace planner to determine the *how*. Only when planners firmly understand the role and potential impact of cyberspace in the planning process can the true value of CO be leveraged.

Conclusion

Although the technology and environment of cyberspace are vastly different from those of the physical domains, the process of identifying key terrain in cyberspace is the same as the process used in the other domains. Cyberspace planners mistakenly try to create a process isolated from the other domains and ignore key integrated planning concepts. Instead, the foundations of JOPP must be used during cyberspace planning and the identification of key terrain to ensure that cyberspace operations are aligned with the objectives throughout the levels of war. While the first inclination of cyberspace operators is to defend everything, the context of the mission should be the driving factor that determines the allocation of efforts and resources.

In addition to adhering to the principles of the planning process, cyberspace operators must have a common lexicon across the joint force. Planners must understand the difference between key terrain and critical assets in order to synchronize efforts between the strategic, operational, and tactical levels of planning. They must also realize that key terrain at one level of war may be different from that of another.

The lack of a common CO lexicon and the misidentification of key terrain in cyberspace indicate that the real problem is that the planning process lacks unification and the inclusion of CO representation. The JOPP forces planners to consider the joint functions during plan development but does not go beyond command and control when considering cyberspace. Since cyberspace touches all the joint functions, serious consideration must be given to cyberspace operations to create a truly comprehensive plan. This can only be done if cyberspace operators have a seat at the planning table from beginning to end of the joint planning process. **JFQ**

Notes

[1] Frederick W. Kagan, *Finding the Target: The Transformation of American Military Policy* (New York: Encounter Books, 2006).

[2] Jeffrey R. Witsken, "Network-Centric Warfare: Implications for Operational Design," U.S. Army Command and General Staff College, 2002.

[3] Joint Publication (JP) 3-12 (R), *Cyberspace Operations* (Washington, DC: The Joint Staff, 2010).

[4] Ben FitzGerald and Parker Wright, "Decentralizing Cyber Command and Control," Disruptive Defense Papers, April 2014.

[5] Jared Serbu, "U.S. Cyber Command Wants DISA to Take Greater Role in DOD Cyber Defense," Federal News Radio, May 29, 2014.

[6] John R. Mills, "The Key Terrain of Cyber," *Georgetown Journal of International Affairs*, March 23, 2013, 99–107.

[7] David Raymond et al., "Key Terrain in Cyberspace: Seeking the High Ground," 6th International Conference on Cyber Conflict, 2014, Tallinn, Estonia, 287–300, available at <www.westpoint.edu/acc/SiteAssets/SitePages/Publications/06916409.pdf>.

[8] Deborah Bodeau, Richard Graubart, and William Heinbockel, "Mapping the Cyber Terrain: Enabling Cyber Defensibility Claims and Hypotheses to Be Stated and Evaluated with Greater Rigor and Utility," MITRE, February 2014, available at <www.mitre.org/publications/technical-papers/mapping-the-cyber-terrain-enabling-cyber-defensibility-claims-and>.

[9] Ibid.

[10] IdeaScale, "Design Defense Around Your Mission or Business Cyber Key Terrain," ACT-IAC Cybersecurity Innovation Initiative, September 2015.

[11] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, November 2010, as amended through February 15, 2016).

[12] Ibid.

[13] Field Manual 3-21.10 (7-10), *The Infantry Rifle Company* (Washington, DC: Headquarters Department of the Army, 2006).

[14] Ibid.

[15] George J. Franz, "Effective Synchronization and Integration of Effects Through Cyberspace for the Joint Warfighter," U.S. Cyber Command, 2012.