OACOK, OKOCA, or OCOKA?

Reframing Terrain Analysis for Cyberspace

By Maj. JC Fernandes and Maj. Alexander Master

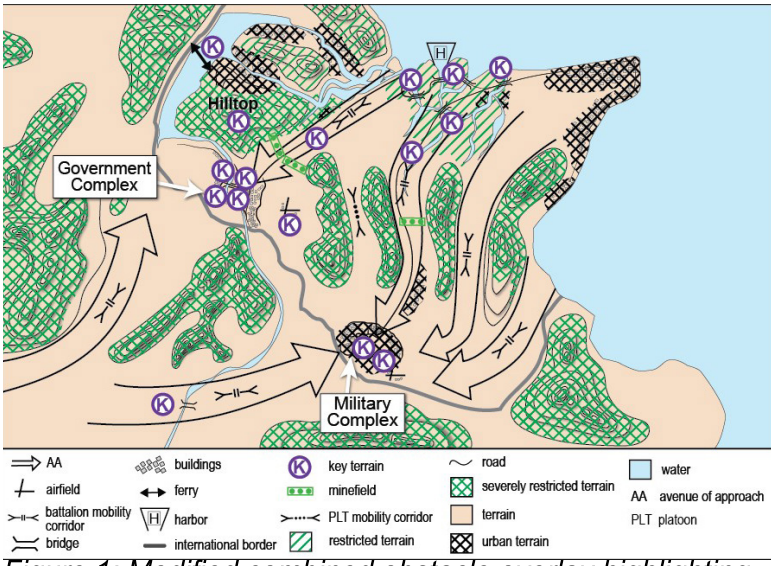

Figure 1: Modified combined obstacle overlay highlighting the key aspects of terrain analysis.

OACOK, OKOCA, or OCOKA? While they may debate the ordering, every Soldier is familiar with the mnemonic for terrain analysis. The concepts of **O**bservation and field of fire, **C**over & concealment, **A**venues of approach, **O**bstacles, and **K**ey terrain, provide a framework through which Soldiers consider the significant aspects of the terrain and their potential impacts to the operation. While OACOK is a natural starting point for Army personnel, the effort required to translate these land domain concepts to computer networks outweighs the convenience of the mnemonic. Cyberspace is a distinct domain of warfare with its own logic. As such, we have no assurance that elements of OACOK can serve as meaningful analogs for the operationally relevant aspect of cyberspace terrain. Instead, this paper proposes features that may be worth considering for operating in cyberspace without attempting to draw a direct comparison. The intent of this contribution is to be a conceptual linkage between military mission analysis and the robust body of cybersecurity resources (e.g. the NIST Cybersecurity Framework, the MITRE ATT&CK Framework, the Cyber Kill Chain) already available for analyzing specific aspects of cyberspace.

Why not OACOK? Unique Characteristics of Cyberspace

Before considering specific features for analysis, it is worth discussing why analysis of cyberspace is unique from terrain analysis in the land domain. Cover and concealment have a direct and personal meaning for Soldiers on the battlefield. They dictate if friendly forces can be seen and shot by the enemy, and, conversely, if they can shoot the enemy. While militaries might cut an undersea cable (Chutel, 2024) or fire artillery rounds at a key transmission node, we do not shoot kinetic munitions within cyberspace. Instead, we primarily manipulate and transmit data in very specific ways to cause effects, gain sensitive information, and defend our use of cyberspace.

The select characteristics below exemplify the unique logic of cyberspace and its unique consequences for a planner's ability to understand the aspects of the cyberspace operational environment. These characteristics are not meant to be a comprehensive description of the fifth warfighting domain but rather illuminate why we must evaluate the operational environment for cyberspace differently than we analyze physical terrain.

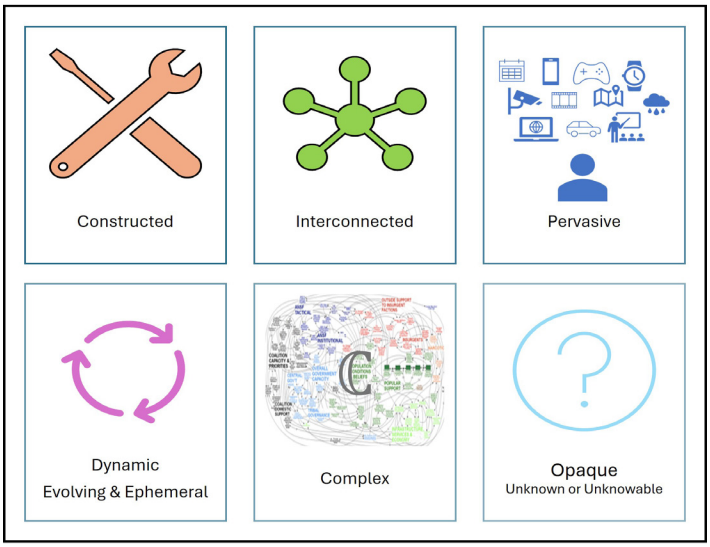

Figure 2: The unique characteristics of cyberspace

First, cyberspace is a man-made, **constructed** domain. Cyberspace comprises a multitude of software and hardware components, produced by a range of companies, organizations, and individuals across decades, and configured together in a variety of ways. This constructed nature contributes to an opaque, dynamic, and complex environment. It also blurs the distinction between terrain analysis and analysis of friendly or enemy forces. The closest military analog is dense urban environments.

Opaque: Because of overhead satellites and global imaging, Army units can generally analyze physical terrain anywhere in the world. However, like the interior of buildings, the cyberspace terrain is often opaque from the outside. Many aspects are known only to those who build and maintain that portion and their design is often confidential intellectual property. Even those who use or interact with the terrain know a limited amount about it.

Dynamic -- Ephemeral and Evolving: While mountains tend not to move and buildings do not change quickly or often, cyberspace changes at the speed of electrons. Change is often an integral part of our use of cyberspace. An IP address assignment may only be relevant for a period of hours, or less. Modern phones maintain connectivity because they can traverse cellular towers and WiFi networks. Similarly, we install new applications and create accounts for new services. Beyond usage, a patch can be pushed out and change networks across the world in a matter of minutes(e.g. CrowdStrike patch in 2024; Burgess), and hardware components are upgraded and replaced. Network diagrams are only one configuration change away from obsolescence.

Complex: Similarly, cyberspace is incredibly complex. Through abstraction, components built by many different people are combined and interoperate together without any one person understanding all the intricacies of each of the elements.

Second, cyberspace is an **interconnected** domain. Logical-layer connections between nodes define proximity in cyberspace, often in ways independent of geographic proximity. Action in one portion of cyberspace can have impacts across the globe, exponentially increasing the scope of the relevant terrain and extending it beyond the authority bounds of the unit, be it defined by geography, organizational ownership, or some other factors.

Finally, cyberspace has become increasingly **pervasive** with a subsequent increase in the diversity and scale of cyberspace terrain that may be relevant for an operation. Internet-connected devices are increasingly prolific throughout society. This pervasiveness also makes understanding the cyberspace terrain increasingly relevant to units and commanders who traditionally only need to concern themselves with the land, sea, or air domains. Because of these characteristics, cyberspace operations involve an environment whose potential scope is both extremely broad and deep, where much about the environment is unknown or unknowable.

Features for Analysis

Given the challenges of understanding the full scope of the cyberspace operational environment, we do not seek to provide an exhaustive list of items for the planner to analyze in order to understand the environment. The breadth and depth of possible analysis quickly dwarfs the staff's capacity to do so, and any exhaustive checklist would be out-of-date before it was finished being written. Likewise, content delivery networks, DNS servers, and similar facets of the domain preclude frameworks that rigidly distinguish between terrain and actors (since the domain is constructed), or rigidly define what is external to the network of interest (given its interconnected nature). Instead, we provide a list of relatively general questions – grouped into three broad thematic areas: **organizational context, network design and functioning,** and **security posture**. Just as the layout of a house may be of little consequence to someone planning a corps envelopment but is of utmost criticality when planning a raid to extract hostages, so too does the mission impact the nature and granularity of analysis appropriate for analyzing cyberspace terrain. Planners may consider these questions in the context of their mission and echelon to decide where deeper analysis is required.

Category	Items of Interest
Organizational Context	• Functions, uses, and business processes • Individual roles and privileges • Standard practices • Providers of services • Security priority
Network Design and Functioning	• Topology • Traffic flow • Hardware and software • Key network services
Security Posture	• Visibility • Tools • Measures and mitigations • Response

Figure 3: Category and analysis questions to help determine OCOKA for cyberspace.

There are many different possible names or features that could be selected and groupings for each. However, with any grouping there are edge cases and interrelated aspects. Our concern was not that we had the perfect list of individual questions, but rather that the aggregate list would prompt the planner to consider the salient aspects for their operations and the corresponding implications.

Organizational Context:

Functions, Uses, and Business Processes: For what does the organization use cyberspace?

• What is the significance of each use? Which uses are most important? What happens if it breaks? Are there redundancies within or outside cyberspace?

• How are these functions performed? What steps, components, and individuals are involved in the different uses?

Individual Roles and Privileges: Who does what, with which authorities?

• Who has privileges for the network, content, devices, applications, etc.?

Standard Practices: What are the standard practices?

• Are there standard naming conventions for users, systems, sites, and organizational units?

• Are there standard times, locations, or people for certain tasks?

Providers of Services: How are the cyberspace capabilities provided and maintained?

• What is provided “as service” and under what conditions? (service level agreements (SLA), responsibilities)

• To what degree does change occur and what is the process for it?

• Are individuals providing their own devices (bring-your-own-device, BYOD)?

Security Priority: How is security valued by the organization and its individuals?

• Are there regulatory, legal, or other security and notification requirements?

• Has the network been compromised in the past?

Network Design and Functioning:

Topology: What are the different portions of the network and what are they used for? (subnets/IP space, VLANs, DMZs, user space – wireless, wired, VPN)

• What is the public-facing footprint? (Across layers: applications, domains, IPs, servers, etc.)

Traffic Flow: What is the network traffic and how does it flow?

• How does it flow between internal/public facing servers, internal/external hosts, and the Internet?

• What is the volume, type (applications, services, protocols), and patterns (in time and direction)?

• What additional factors impact or complicate traffic? (VPN concentrators, DNS, routing rules, traffic prioritization, caching, load balancing, failover, etc.)

Hardware and Software: (host and network; public-facing and internal)

- What hardware and software are used on the network? (version, patch level, configuration)
- Where are they?
- What purpose are they used/authorized for?
- What is the process for approval, patching, and updating?

Key Network Services: What are they and how do they function?

Security Posture:

Visibility: What data is collected about traffic and endpoints and what is its lifecycle? (Collection, transmission, storage, access, removal)

Tools: What endpoint and network security solutions are present?

- What are the settings for endpoints and network traffic?
- What are the capabilities, gaps, and limitations of the implementation?

Measures and Mitigations: What technical and policy mitigations are in place?

- What system and user behavior is explicitly permitted or prohibited?
- What rules are in place for network traffic?
- How does authentication occur for users and services?
- How is data protected within the organization?

Response: How does the organization respond to alerts and incidents?

- What are the business response actions and the technical incident response actions?

These questions allow the planner to connect the broader operational context to the multitude of guides, techniques, procedures, and other resources available for analyzing specific aspects of networks and cybersecurity. In particular, the organizational context helps planners understand the significance of the cyberspace terrain and its integration with the broad joint or national context. When answering the questions, planners should consider all aspects - physical, human, and technical - holistically, rather than focusing exclusively on one domain, to ensure a more complete understanding of the implications.

Existing Frameworks and Approaches

Industry and the military offer various models that informed our selection of the above features and can complement their analysis. They provide insights into the questions we should ask, the processes we should use to ask them, and the details we should consider when answering them.

First, we proposed that cyberspace, as a complex constructed terrain with a significant human presence, is more closely analogous to a dense urban environment than wooded or rural environments. Given this premise, ASCOPE (Areas, Structures, Capabilities, Organizations, People, and Events) provides a related conceptual framework. Just as a planner cannot exhaustively analyze these elements in a large urban setting (ATP 3-06), so also do the characteristics of cyberspace preclude exhaustive analysis of the environment. However, we must view the concepts of areas and structure differently in cyberspace. Similarly, the relevant capabilities, organizations, people, and events in cyberspace may differ from those in an urban environment. Key people may include network administrators, while events may include holidays (when no one is working), but also scheduled downtime and upgrade periods.

Second, doctrine and industry also provide several common models to conceptualize cyberspace at higher levels of abstraction. JP 3-12 (OJCS, 2018) defines the interrelated layers of cyberspace – physical, logical, and person – while the Open Systems Interconnection (OSI) model (Day & Zimmerman, 1983) or the related Transmission Control Protocol/Internet Protocol (TCP/IP) model (History of Computer Communications, 2021) defines protocol layers to promote the understanding of networking. While extremely useful, the layers of these models are not features of the terrain itself but rather a lens through which to view an element of cyberspace. They are layers of abstraction that provide scope and context. While not a direct analog, they provide

similar utility to the land domain practice of analyzing terrain before, on, and after the objective. For example, in cyberspace, one might consider the physical device(s) running a web service in addition to the MAC address(es), IP address(es), and URL(s) of the server(s). Planners can consider the different layers when asking the questions proposed earlier.

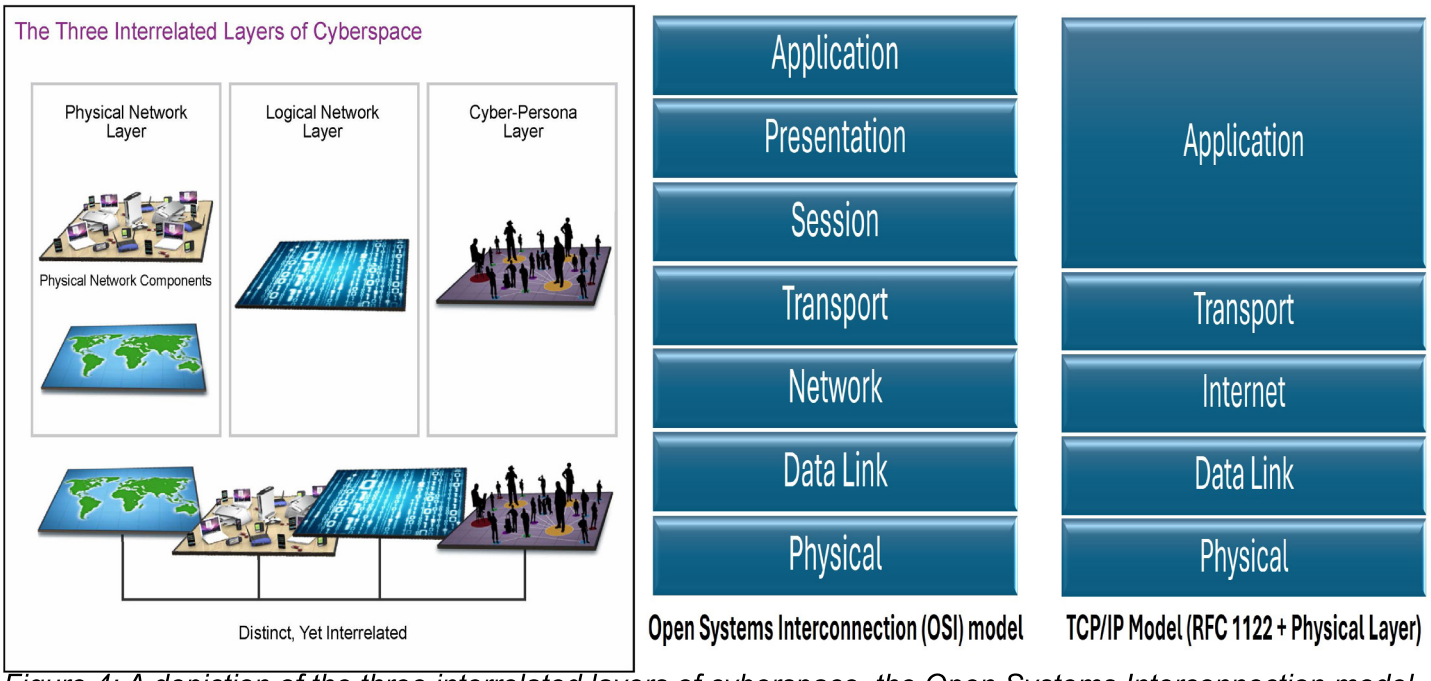

Figure 4: A depiction of the three interrelated layers of cyberspace, the Open Systems Interconnection model, and the Transmission Control Protocol/Internet Protocol.

Given the answers to questions proposed earlier, planners may determine additional analysis is required. They can turn to the rich body of cybersecurity resources from industry and government sources to dive deeper into specific aspects, such as configuration of endpoint agents, vulnerabilities of certain software, penetration testing web applications, and technical security controls.

Finally, JP 3-0 introduces the concept of a "systems perspective" for understanding the operational environment. This perspective and the related concepts of functional mission analysis (FMA), mission threads (TC 3-12.2.90), failure modes and effects analysis (FMEA), and dependency analysis, provide an approach that planners can use to focus their analysis and guide their selection of which elements to analyze.

Concluding Thoughts

We would be remiss if we failed to acknowledge that cyberspace operations do not occur in a vacuum. People use and depend on cyberspace for a variety of functions, but there can also be analog alternatives to cyberspace. The physical layer of cyberspace resides in the domains of land, sea, air, and space. It can be destroyed and impacted by power outages, extreme temperatures, electronic attack, and other physical factors. The information within cyberspace is part of the information environment and can interact with the cognitive dimension as it shapes human thoughts and behaviors - which may have subsequent impacts on users' activities in cyberspace. To conduct joint, multi-domain operations that achieve synchronized effects in time and space, cyber planners must not only understand the cyberspace terrain but also how it fits into the broader operational environment and operational objectives. The organizational context provides the means for planners to do just that.

About the authors

Maj. JC Fernandes is an active duty Cyber Officer at the Army Cyber Institute. He conducted defensive cyber operations while assigned to the Cyber Protection Brigade. He was initially commissioned as an infantry officer and served with the 173rd IBCT(A).

Maj. Alexander Master is an active duty Cyber Officer at the Army Cyber Institute and an Assistant Professor in the Electrical Engineering and Computer Science department at the United States Military Academy at West Point, New York. His research interests focus on privacy and digital operations security (OPSEC). Maj. Master has served on a National Cyber Protection Team, and spent three years supporting offensive cyberspace operations in the Cyber National Mission Force. He was initially commissioned as a field artillery officer and deployed in support of Operation Resolute Support in 2015 as part of the conflict in Afghanistan

References:

Burgess, M. (2024). Microsoft outage caused by CrowdStrike takes down computers around the world. WIRED. https://www.wired.com/story/microsoft-windows-outage-crowdstrike-global-it-probems/

Chutel, L. (2024). Finland Says Vessel Suspected of Cutting Cable May Be Part of Russia's 'Shadow Fleet'. The New York Times. https://www.nytimes.com/2024/12/26/world/europe/finland-estonia-cables-russia.html

Day, J. D., & Zimmermann, H. (1983). The OSI reference model. *Proceedings of the IEEE, 71*(12), 1334–1340. https://doi.org/10.1109/PROC.1983.12775

History of Computer Communications. (2021). The Department of Defense, OSI, and TCP/IP. https://historyofcomputercommunications.info/section/14.5/The-Department-of-Defense-OSI-and-TCP-IP/

Strom, B., Applebaum, A., Miller, D., Nickels, K., Pennington, A., & Thomas, C. (2018). MITRE ATT&CK: Design and philosophy. MITRE Corporation. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

Lockheed Martin. (2011). Cyber kill chain. Lockheed Martin Corporation. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Office of the Joint Chiefs of Staff. (2018). Joint publication 3-12: Cyberspace operations. U.S. Department of Defense. https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/

OWASP. (2025). The OWASP Risk Assessment Framework. Open Worldwide Application Security Project (OWASP). https://owasp.org/

Ullrich, S., & Moriarty, S. (2024). Lessons learned from the Ukrainian Territorial Defense Forces: Command post survivability. United States Army. https://www.army.mil/article/273510/lessons_learned_from_the_ukrainian_territorial_defense_forces_command_post_survivability

U.S. Army. (2022). ATP 3-06: Urban Operations. U.S. Department of the Army. https://armypubs.army.mil/ProductMaps/PubForm/ATP.aspx

U.S. Army. (2024). TC 3-12.2.90 Mission Thread Defense. U.S. Department of the Army. https://armypubs.army.mil/ProductMaps/PubForm/TC.aspx