2014 6th International Conference on Cyber Conflict
P.Brangetto, M.Maybaum, J.Stinissen (Eds.)
2014 © NATO CCD COE Publications, Tallinn

Key Terrain in Cyberspace: Seeking the High Ground

David Raymond
Army Cyber Center
West Point, New York, USA

Gregory Conti
Army Cyber Center
West Point, New York, USA

Tom Cross
Lancope, Inc.
Alpharetta, Georgia, USA

Michael Nowatkowski
Army Cyber Center
West Point, New York, USA

Abstract: In military doctrine, key terrain refers to areas which, if seized, afford an advantage to an attacker or defender. When applied to geographic terrain, this definition is clear. Key terrain might include a hill that overlooks a valley an enemy wants to control or a crossing point over a river that must be traversed before launching an attack. By definition, dominance of key terrain is likely to decide the overall outcome of a battle. While cyber key terrain is similar to geographic key terrain in some ways, there are also significant and often counterintuitive differences. Some consider cyber terrain to be tied to a physical location and to be represented in cyberspace by routers, switches, cables, and other devices. We will argue that key terrain in cyberspace exists at all of the cyberspace planes, which include the geographic, physical, logical, cyber persona, and supervisory planes [1]. In many cases, features of cyber terrain will not be tied to a specific location, or the geographic location will be irrelevant. In this paper we deconstruct and analyze cyber key terrain, provide a generalized framework for critical analysis, and draw parallels between cyber and physical key terrain while providing examples of key terrain in cyber operations. During a cyber operation, an analysis of key terrain will aid in the strategy and tactics of both the offense and the defense. During peacetime, an understanding of cyber key terrain can be employed broadly, ranging from helping a system administrator focus scarce resources to defend his network all the way to allowing nation-state militaries to develop long-lasting and effective doctrine.

Keywords: *cyber operations, terrain analysis, cyber terrain, key terrain*

1. INTRODUCTION

Any military operation requires a thorough analysis of the situation, referred to in the U.S. military as Intelligence Preparation of the Operational Environment, or IPOE [2]. Along with

The views expressed in this article are those of the authors and do not reflect the official policy or position of West Point, the Department of the Army, or the United States Government.

an analysis of the enemy's capabilities and possible courses of action, a fundamental aspect of IPOE is a detailed terrain analysis to identify key terrain. The U.S. Army defines *key terrain* as "any locality or area, the seizure or retention of which affords a marked advantage to either combatant" [3]. Identifying key terrain gives military planners, whether attacking or defending, a physical location upon which to focus their efforts.

Identifying key terrain is straightforward in kinetic conflict; key terrain in cyber operations is likewise critical, but less well understood. In some cases, a hardware device might be cyber key terrain. For example, if your goal is to temporarily deny your opponent access to a tactical network, and if they have a single router connecting them to that network, that router might be key terrain. Some cyber terrain is logical instead of physical. As an example, portions of the Domain Name System (DNS), a distributed, hierarchical, and ever changing database of domain name mappings, might be key terrain in certain situations.

Adding to the complexity is the malleable nature of some cyberspace terrain. The logical structure of a software-defined network (SDN) can change dramatically with no change to the underlying hardware, causing instantaneous shifts in terrain elements such as avenues of approach,[1] obstacles (such as packet filters and firewalls), and key terrain. Battlefield deception is inherently intertwined with key terrain, however in cyberspace deceptive terrain can be easily constructed and moved, a near impossibility on the physical battlefield. Key terrain also has a temporal aspect, a hilltop that is key to a battle might not be so once the battle is over, but in cyberspace these temporal shifts can happen much more quickly, perhaps in milliseconds. Finally, it is not always obvious who controls an element of cyber terrain. While occupation of geographic terrain is often recognized easily by the presence of troops, a cyber operator might be in full control of an adversary's device without them even knowing it.

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. It helps you to focus your defenses, or your attack. It may also assist in your deception effort by informing how to manipulate your network to foil an adversary attempting to penetrate it.

In this work we examine the notion of key terrain in the traditional domains of land, sea, and air, further analyze cyber terrain, and then merge these concepts to study cyber key terrain. We then provide a framework to describe how the concept of cyber key terrain can be applied in both the offense and the defense.

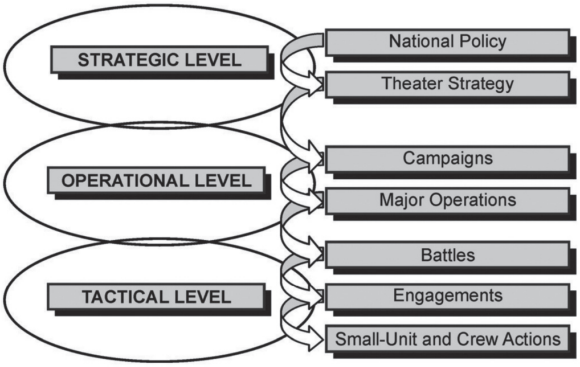
2. KEY TERRAIN IN KINETIC WARFARE

At the tactical level of war, key terrain is a straightforward concept. A hilltop that dominates an enemy's defenses or a bridge across an unfordable river might be key under the right circumstances. Key terrain provides an advantage to a combatant. Therefore, it only exists in a potentially adversarial situation – one in which a place might be attacked and should be defended.

1 An avenue of approach is defined in U.S. Joint doctrine as "[a]n air or ground route of an attacking force of a given size leading to its objective or to key terrain in its path" [8]. In section 3. B. we extend this definition to incorporate elements of cyberspace.

The concept of key terrain is most commonly applied at the tactical level of warfare, however it is relevant at the strategic and operational levels as well. Figure 1 depicts the levels of war from U.S. Army Field Manual 3-0, Operations [4]. The tactical level of war involves individuals and small units engaging in direct hostilities and the above examples of hilltops and bridges apply primarily at this level. The strategic level of war involves nation-states deciding upon national security objectives and using elements of national power (diplomatic, informational, military, and economic) to achieve them. Strategic key terrain might include a nation's capital. For example, the German occupation of Paris in June 1940 caused the French government to flee and put an end to organized resistance against the German invasion, making the city of Paris strategic key terrain. The operational level of war bridges the gap between strategic and tactical and describes a theater of war or a major campaign. An example of operational key terrain is the Khyber Pass, a key supply route between Pakistan and Afghanistan. More than 80 percent of supplies brought in by road to NATO and US forces in Afghanistan is transported through the Khyber Pass [5].

FIGURE 1: FIGURE 7-1 FROM ARMY FM 3-0: OPERATIONS. LEVELS OF WAR.



While applied most often to land-based military campaigns, the idea of key terrain is also useful in naval and aviation contexts. Midway Atoll, an American outpost and airfield 1,300 miles northwest of the Hawaiian island of Oahu, was key terrain in the Pacific theater during World War II. After Japan's attack on Pearl Harbor in December 1941 brought the United States into the war, the U.S. presence at Midway was within Japan's sphere of influence and was perceived by the Japanese as a direct threat to their homeland. This perception was reinforced in April 1942 when Lieutenant Colonel James Doolittle of the U.S. Army Air Corps led a B-25 bomber raid on the Japanese mainland. Admiral Yamamoto was determined to defeat the remainder of the U.S. Pacific Fleet by drawing it into an ambush at Midway. U.S. forces, however, had broken the Japanese naval code and were able to use intelligence gained to ambush and soundly defeat the Japanese fleet, a battle that proved to be a turning point in the Pacific theater.

The term key terrain has been used before to describe non-geographic features of an area of operations. During General David Petraeus' Senate Confirmation Hearing for Commander, International Security Assistance Force (ISAF), U.S. Forces Afghanistan, he stated that in

Afghanistan, as in Iraq, "the key terrain is the human terrain" [6]. In this context, human terrain is defined as "the human population in the [area of operations] as defined and characterized by sociocultural, anthropologic and ethnographic data and other non-geographical information" [7].

3. DEFINING CYBER TERRAIN

The U.S. Department of Defense (DOD) defines cyberspace as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" [8]. 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 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*.

A. The Nature of Cyber Terrain

The term *terrain* is almost always used to describe physical locations that can be easily pointed to on a map. Since much of cyberspace is virtual, cyber terrain differs from physical terrain in many fundamental ways [9]. As we will see, cyber terrain spans the cyberspace planes [1], so cyber key terrain often manifests itself logically instead of physically. A router that connects a network to an Internet service provider (ISP) is an example of a cyber terrain feature. While this device resides at a specific physical location, it is not the physical location that might make it key terrain, but the logical location of the device in the network. However, physical location is not irrelevant, in that gaining physical access to take a device offline is still a valid attack vector. What it means to 'control' terrain is also different in cyberspace than in physical space. Traditionally, physical occupation of a piece of terrain is required to control it. Furthermore, it is usually obvious to both sides of a conflict who is in control of certain terrain. In cyberspace, physical proximity is not required to control a given device. System administrators routinely access devices from remote locations, and a cyber criminal might gain access to a company's network through the Internet from hundreds of miles away. A skilled attacker will try to hide his presence and remove evidence of his activities on a compromised device. The network administrator might have the illusion of being in control until the attacker needs to influence a network. In fact, an administrator may never know that one of his devices was compromised; even one that was used to penetrate his network.

The virtual nature of cyber terrain makes it possible to dynamically create, modify, and destroy cyber terrain both quickly and frequently; at machine speed. Software defined networking allows logical network architectures to be modified on the fly [10]. A defender might, therefore, be able to modify avenues of approach and move key terrain dynamically in the face of a network attack. An attacker would need to respond in a highly agile manner to overcome these changes to what is effectively the fundamental fabric of the cyber battlefield. The rate of change could far exceed human capacity and require automated responses reminiscent of

high-frequency trading, which is characterized by algorithmic techniques used to rapidly trade securities in fractions of a second [11].

The potential to practice deception operations in cyberspace is vast. Companies have long deployed deceptive 'honeynets', real-looking network segments designed to divert an attacker's attention away from valuable assets within their networks. Using software defined networking, an organization could move critical nodes from one location to another within their cloud infrastructure and instantly reconfigure the network to support the new architecture. An attacker that is pursuing a certain avenue of approach to a target might then have to abandon that pathway in favor of another, which could also be taken away at any time. This could even be done dynamically in the face of a suspected (or known) attack on, or breach of, a network.

We make a distinction between maneuver and fires in cyberspace. U.S. military doctrine defines *maneuver* as "[a] movement to place ships, aircraft, or land forces in a position of advantage over the enemy," and *fires* as "[t]he use of weapon systems to create specific lethal or nonlethal effects on a target" [8]. In cyberspace, we consider an actor to have maneuvered when he has gained access to a device or system as part of a cyber operation. Such access can be authorized or unauthorized, depending on the owner of the system and the nature of the operation. Cyber fires, such as the launching of a software exploit, or phishing email, might be used to enable cyber maneuver. Other fires, such as denial of service (DoS) attacks, are designed to achieve a specific effect without necessarily attempting to facilitate further maneuver.

B. Cyber Terrain and Cyberspace Planes

The cyber planes suggested by Fanelli [12] and refined by Raymond [1] can be used as a framework to identify terrain at various levels. Here we will introduce cyber terrain at each cyberspace plane. The planes are depicted in Figure 2.

1) Supervisory Plane. The supervisory plane provides oversight and the authority to start, stop, modify, or redirect a cyber operation [12]. Cyber terrain at the supervisory plane is comprised of elements of cyberspace that either perform a supervisory function or provide a conduit for command and control.

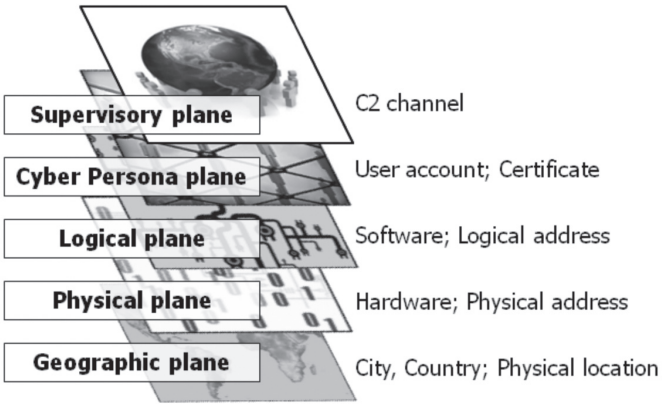
2) Cyber Persona Plane. The cyber persona plane identifies identities in the cyber domain. These identities might have a many-to-one or one-to-many relationship with physical individuals. Here cyber terrain includes such features as user accounts or credentials that provide access to information resources.

3) Logical Plane. This plane consists of the operating system, application software, and software settings on a device, and the logical links between networked devices. Terrain at this level includes a wide range of software systems, services, and protocols that keep networks running and computers doing useful work.

4) Physical Plane. The physical plane maps to the physical layer of the Open Systems Interconnect (OSI) model and includes components of a computer system and attached hardware. This plane is comprised of the devices that people often interpret as being cyber

terrain, such as the routers, switches, and other network devices that physically connect devices in a network.

FIGURE 2: CYBERSPACE PLANES AS DEFINED IN [1], WITH REPRESENTATIVE EXAMPLES.



5) Geographic Plane. The geographic plane describes the geographic area in which an information system, or portions of it, resides. It is the most static of the planes – geography changes at an extremely slow rate. While the logical location of a network device in cyberspace is often more important than its geographic position, geography can also be relevant, and failure to recognize geographic impact to operations can be costly. Geography is also important when considering the potential path of a state-sponsored cyber operation. Just like flying over one country enroute to bombing another could cause an international incident, routing attack packets through a neutral third party could have consequences. This poses a particular challenge during cyber operations when the path that data takes across the Internet can rarely be controlled or even accurately predicted.

C. Cyber Terrain Analysis Using OCOKA

Traditional military terrain analysis uses a process represented by the acronym OCOKA, which stands for Observation and Fields of Fire, Cover and Concealment, Obstacles (man-made and natural), Key Terrain, and Avenues of Approach. Hobbs applies the traditional OCOKA analysis to cyberspace [13] and we expand on his observations below.

1) Observation and Fields of Fire. *Observation* refers to the ability to see enemy forces from a particular vantage point; a *field of fire* combines this ability to observe with the ability to engage enemy targets within the maximum range of your weapon. The idea of observing cyber terrain, while different from physical terrain, is still meaningful. Reconnaissance using *whois* lookups provides IP address ranges and Domain Name Server addresses for Internet domains, along with contact information for domain administrators. Scanning a target network will tell you what hosts are accessible from your vantage point and, by scanning ports, what network

services they are running. Tools like *nmap* can be used to determine which type and version of operating system is running on a particular device and may be used to determine some of the software running on the system [14]. Observing traffic entering and leaving a network can also provide a wealth of information about that network. Examination of source and destination IP addresses can help identify individual hosts. Time-to-live (TTL) values in packet headers can tell you how many routers a packet traversed before leaving the network, which helps to help determine the network architecture. This reconnaissance will help determine which cyber weapons might be successful, giving an indication of your 'fields of fire.'

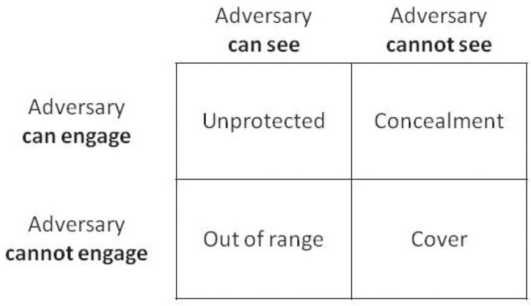
Much like physical terrain, observation is based on vantage point. Someone scanning a network from outside of a firewall will likely get an entirely different result than someone scanning the network from inside. As discussed previously, deception can be used by both attacker and defender. Attackers can hide their source IP address among a flood of false source IP addresses during network scans to hide the origin of the scans. Defenders can use honeynets to draw intruders away from their true network resources. Defenders can also use proxies or network address translation (NAT) to mask their internal network structure.

2) Cover and Concealment. In kinetic terms, *concealment* protects an individual from observation, while *cover* protects one from observation and enemy fire. *Camouflage* is sometimes used to enhance or provide concealment. In cyberspace, as in physical space, a third category exists in which a target can be seen but not engaged and is therefore out of range of an adversary's available weapons. Figure 3 depicts the categories of cover and concealment.

For the network defender, cover is often provided by firewalls that prevent traffic from reaching specific hosts while also protecting those systems from observation. An intrusion prevention system can be used to place hosts out of range of an attack by blocking malicious network traffic, but they do not provide concealment – the hosts behind an intrusion prevent system can still be observed by the attacker through authorized transactions. For an attacker, concealment is used to prevent detection. Polymorphic code and other obfuscation techniques that reduce the potential for signature-based malware detection are often used to camouflage malicious code that could otherwise easily be stopped by intrusion prevention systems. Finally, rootkits can be used by an attacker to conceal the presence of malware on a system [13].

3) Obstacles. In cyberspace, *obstacles* are those technologies or policies that limit freedom of movement within a network. These can include router-based access control lists, air gaps, firewalls, and other devices that are used to restrict the flow of network packets. In cyber terrain, the distinction between obstacles and cover is not always clean. A device installed to limit the enemy's freedom of movement can also provide cover for some network systems. Furthermore, by filtering malicious packets from traffic destined to a system visible on the network, cyberspace obstacles sometimes put target systems out of range of an attackers cyber weapons.

FIGURE 3: CYBER OCOKA CATEGORIES BASED ON ADVERSARY'S ABILITY TO SEE OR ENGAGE TARGET. CONCEALMENT MAY BE ENHANCED BY CAMOUFLAGE.



Other obstacles include user access control systems that prevent network access by all but authenticated users. Even bandwidth constraints that limit traffic flow between two network endpoints can be considered an obstacle. In a kinetic battlespace, obstacles can be either natural (like a ridgeline) or man-made (like a minefield). A similar distinction can be made in cyberspace between intentional obstacles, such as firewalls, and potentially unintentional ones. An example of an unintentional obstacle is a home wireless access point that uses port address translation to map multiple devices to a single IP assigned by an Internet service provider and in doing so, improves security of the network by masking devices inside the network.

4) Key Terrain. Earlier we defined cyber terrain, here we 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. Aspects of cyber key terrain will be analyzed in detail in Section 4.

5) Avenues of Approach. Avenues of approach in cyberspace are composed of the various paths that can be traversed to reach a target. The physical pathways that connect systems such as switches, routers, fiber, and Ethernet cable are often less relevant than the logical connections facilitated and limited by these devices since the devices traversed by Internet flows can change over time. An HTTP connection to a web server can be an avenue into a target network. Avenues of approach in cyber operations might also include multi-pronged attacks such as a phishing attack on an employee followed by a logical connection to resources left open by the phishing attack.

4. KEY TERRAIN IN CYBERSPACE

Cyber terrain exists across the cyberspace planes and there are many features of cyber terrain that can provide an advantage to one side or the other. By understanding this cyber key terrain, a network defender knows where to focus his energy to prevent penetration and an attacker can select a target within a network that provides maximum potential for success.

A. Examples of Cyber Key Terrain.

Here we provide examples of key terrain for each of the cyberspace planes depicted in Figure 2.

1) Supervisory Plane. Key terrain at this level might include botnet command and control servers that are used to supervise large-scale botnet-based cyber attacks. In June 2013, Microsoft and the U.S. Federal Bureau of Investigation coordinated to disable most of the Citadel botnet by cutting off communication between botnet command and control (C&C) servers and the compromised systems under their control [15]. The Citadel botnet is suspected to have compromised more than five million computers around the world and is thought to be responsible for over half a billion U.S. dollars in losses to businesses and individuals. The botnet C&C servers proved to be cyber key terrain in this operation.

2) Cyber Persona Plane. A system administrator's account might be considered cyber key terrain at the cyber persona plane if possession of that account could be used by an attacker to compromise a defender's resources. Even an unprivileged user account could be key depending on the owner of the account. In early 2011 when HBGary CEO Aaron Barr threatened to expose key members of the hacking collective Anonymous, the group attacked HBGary's network to gain access to Barr's email account login credentials, leading to publication of private emails, website defacement, and significant embarrassment to Barr and HBGary [16].

3) Logical Plane. Key at the logical plane might be the Domain Name System (DNS), which provides logical mappings between domain names (such as www.ccdcoe.org) and their Internet Protocol (IP) addresses (such as 195.222.11.253) [17]. Recent attacks by the hacker collective Syrian Electronic Army (SEA) against the New York Times and other organizations highlight the potential vulnerabilities inherent in failing to recognize a key piece of cyber terrain at the logical plane [18]. The SEA achieved its goal of defacing the New York Times website by targeting the domain name registrar rather than directly targeting the websites themselves, which may have been better defended.

4) Physical Plane. Key terrain on the physical plane might be a poorly configured wireless device that uses an obsolete security protocol. Starting in July 2005, criminals gained access to networks belonging to TJX Companies, Inc., through wireless networks operating at some of their department stores. The stores were using Wired Equivalent Privacy, or WEP, to secure their wireless networks, a protocol that was known to be insecure as early as 2001. Attackers were able to gain access to the company's database servers and steal as many as 200 million customer credit- and debit-card numbers over four years [19].

5) Geographic Plane. The geographic location of infrastructure supporting cyber operations, such as power stations and HVAC controls, could be key terrain. During Hurricane Sandy in October 2012, storm surges surpassed a two-century old record, reaching 14 feet in lower Manhattan. When saltwater rushed over the 12.5 foot seawall at a key substation near Battery Park, 3 million New Yorkers lost power for four days, including the financial district, contributing to the estimated damages of over $20 billion [20] [21].

B. Cyber Key Terrain and the Levels of War

Tactical cyber key terrain are those features that provide tactical advantage to someone attacking or defending a network. Examples might include wireless networks or physical links that allow communication at the local level, firewalls or similar devices that control traffic in a network, or local administrator privileges that could be used to compromise a network. Since tactical actions could have operational or strategic consequences, these examples could also be key terrain at higher levels depending on the context.

Operational key terrain includes features that might give an adversary an advantage in a specific campaign or major operation. A key component of Stuxnet, for example, involved software driver files signed by legitimate digital certificates from two companies that were apparently compromised as part of the development of this malware [22]. The computer systems that those companies used to store their digital certificates constitute operational key terrain. The creators of Stuxnet were able to obtain an asset from those computers that provided them an advantage when they went after their primary objective.

An example of cyber key terrain at the strategic level might be components of a supply chain that produces network devices used by a target entity. A supply chain attack that inserted vulnerable firmware in a government's network routers allowing unauthorized access, for example, could provide an adversary a significant strategic advantage.

Table 1 lists cyber key terrain across the cyberspace planes and the levels of war.

TABLE 1. REPRESENTATIVE CYBER KEY TERRAIN EXAMPLES BY CYBERSPACE PLANE AND LEVELS OF WAR

	Tactical	**Operational**	**Strategic**
Supervisory Plane	• Wireless channel used for C2 communications	• Security systems located in a Theater Network Operations and Security Center (TNOSC)	• Nuclear launch systems
Cyber persona Plane	• Local System administrator account	• Network credentials for theater commander	• Email account and password for presidential candidate, Supreme Court justice, or other key figure.
Logical Plane	• The operating system of desktop computer in a targeted organization	• The authoritative DNS server for a popular website	• The software running a regional cellular network
Physical Plane	• A USB key • A cellular phone • An Ethernet switch	• Regional communications cables • Air Defense Artillery Radar/early warning network	• Data center for government agency or major industry
Geographic Plane	• Physical location of network devices providing service to edge network	• Power plant providing electricity to a capital	• Building housing nation's offensive cyberspace operations capabilities

C. A Framework for Leveraging Cyber Key Terrain

Just like in a kinetic scenario, the identification of key terrain is often in the eye of the beholder and depends heavily on context. Two tacticians might look at a defensive sector and, based on experience and their approach to defending an area, identify different key terrain in the sector. Both the defender and attacker must analyze cyber terrain in the context of what he or she considers to be a 'successful' defense or attack and then identify the terrain they perceive will give them an advantage in order to focus their efforts. A general framework for identifying cyber key terrain as a **defender** is given here. This process is reminiscent of the process a tactical commander might take to identify and defend physical key terrain, but our approach is tailored to the realities of cyber terrain.

1. Identify potentially targeted assets. Defenders should start their terrain analysis by identifying the information systems or data that may motivate attackers to target the organization. It is important to keep in mind that the assets that are most valuable to an organization are not always the assets that are most valuable to attackers. Although prudent organizations always consider the risks to their "crown jewels," attackers may be interested in other assets as well, such as an administrative assistant's logon credentials. Therefore it makes sense to work from a model of different threat actors, their motivations, their capabilities, and their tactics in attempting to identify the assets that they may decide to target.

2. Enumerate avenues of approach. What are all of the different vectors that can be used to access each potentially targeted asset? It is important to consider all of the interfaces that the asset has to the outside world that the attacker could leverage on each cyberspace plane, whether they are direct network interfaces, or indirect interfaces such as removable media, or key personnel with physical access.

3. Consider observation and fields of fire. From what locations can the attacker gain access to each interface into the potentially targeted asset? At this point, the analysis may become iterative – if the attacker can reach an interface to the targeted asset from a particular system or network, it is important to enumerate the avenues of approach to that secondary system or network, and determine the locations from which those avenues of approach can be reached, and so on.

It is through this iterative analysis that a picture of key terrain begins to emerge. Are there particular vantage points that provide an attacker with a field of fire that includes many potentially targeted assets? In most networks there are infrastructure components that could provide an attacker broad access to many systems in the network, such as identity and access management systems, core firewalls, network backup systems, and end-point management systems. All of these may be considered key terrain.

It is important for defenders to avoid limiting this analysis to terrain that they control. How might an attacker target other organizations or infrastructure in order to obtain a tactical advantage? Attackers might target suppliers, business partners, service providers, or even third party websites. For example, a "watering-hole attack" is a tactic that involves compromising a website that is frequented by the intended target. Once the website has been compromised, the

attacker has an improved field of fire into their intended victim's computer network, as they can directly access the victim's web browser and provide code for it to execute. All of these vantage points should be considered.

4. Place obstacles, cover, and concealment. Once key terrain has been identified, a defender can begin to take steps to protect it. The most basic step is to limit avenues of approach. Interfaces to key terrain that are unnecessary should be deactivated. Firewalls are often used to limit the number of access vectors into a key asset in a computer network.

Of course, in order for most computer systems to work, they have to be interconnected either directly or indirectly, so it is impossible to close off every access vector. Access vectors that must remain open should be protected. Known vulnerabilities should be patched and weak passwords identified and changed. Intrusion prevention systems have been used for years to block attacks across interfaces that cannot be closed off.

The fact is that neither firewalls nor vulnerability management nor intrusion prevention systems have proven effective in practice against advanced attackers, and this is not merely because defenders have failed to perform a comprehensive terrain analysis. Attackers have proven that they can craft attacks that target vulnerabilities that defenders are unaware of, and they can conceal their attacks in such a way that they cannot be detected.

In light of the effectiveness that attackers have demonstrated at subverting traditional kinds of cover, defenders might benefit from giving more consideration to deception as a part of their defensive posture. As previously discussed, cyber key terrain can be moved, and it can be reorganized in such a way that it ceases to be valuable. A defender could lure an attacker into targeting a piece of key terrain that seems to provide access to a valuable asset, and then change the nature of that terrain once it is compromised. This approach expends attacker resources and forces him or her to reveal capabilities and techniques.

Although honeypots have been a part of defensive approaches to protecting computer networks for a long time, traditional approaches to constructing them have not always kept up with modern attackers and their tactics. It is important to design honeypots that are truly attractive to the kinds of adversaries an organization is most concerned with. A good honeypot should appear to be a key piece of terrain in order to attract an attacker's attention.

An **attacker** has a slightly different perspective as they typically operate with imperfect information about the terrain of the environment they are targeting. Often, cyber terrain cannot be observed until it is accessed, so attackers are forced to engage in a constant process of reassessment of key terrain as they progress deeper into a network. This assessment mirrors the iterative analysis that was (hopefully) performed by the defender.

A careful analysis of avenues of approach, observation points, and fields of fire can provide an attacker with a complete view of his or her options at each stage of the attack. Because attackers may be operating with imperfect information, they may have to make assumptions about the capabilities that controlling a particular asset will afford them, based on how that sort of asset

is typically used by network operators or end users. It is also important for the attacker to try to enumerate the protection technologies employed by the defender. If the attacker can reproduce the defender's complete toolset, he or she can ensure that exploits, malware, and command and control channels are not detected by that toolset.

Of course, attackers need to take care to conceal the reconnaissance used to collect their picture of the cyber terrain, as noisy reconnaissance may result in the attack being identified. Also, attackers must take care to assess whether or not the terrain is what it appears to be, as defenders may have placed honeypots or other deceptive features onto the battlefield.

5. CONCLUSION

An understanding of cyber terrain, and specifically cyber key terrain, is an important part of emerging cyber operations doctrine. It is important for operators to understand that key terrain in cyberspace can have completely different features than key terrain in the traditional sense. A much more robust technical understanding of the cyber landscape is required for a cyber operator to be able to identify and leverage key terrain in cyberspace, but developing this insight could be instrumental in allowing cyber operators to focus limited assets on the most likely path to success during offensive or defensive operations.

BIBLIOGRAPHY:

[1] D. Raymond, G. Conti, T. Cross and R. Fanelli, "A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons," in *5th International Conference on Cyber Conflict*, Tallinn, Estonia, June 2013.

[2] Department of Defense, Joint Publication 2-01.3: Joint Intelligence Preparation of the Operational Environment, 2013.

[3] Headquarters, Department of the Army, Field Manual 3-90-1: Offense and Defense Volume 1, 2013.

[4] Headquarters, Department of the Army, Field Manual 3-0: Operations, 2011.

[5] S. Masood, "Bridge attack halts NATO supplies to Afghanistan," New York Times, 3 February 2009. [Online]. Available: http://www.nytimes.com. [Accessed 29 November 2013].

[6] A. Garfield, "Understanding the Human Terrain: Key to Success in Afghanistan," Small Wars Journal, 16 July 2010. [Online]. Available: http://smallwarsjournal.com. [Accessed 17 October 2013].

[7] J. Kipp, L. Grau, K. Prinslow and D. Smith, "The Human Terrain System: A CORDS for the 21st Century," *Military Review*, pp. 8 - 15, September-October 2006.

[8] Department of Defense, Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms, 2010.

[9] M. Miller, J. Brickey and G. Conti, "Why Your Intuition About Cyber Warfare is Probably Wrong," Small Wars Journal, 29 November 2012. [Online]. Available: http://www.smallwarsjournal.com. [Accessed 15 October 2013].

[10] Open Networking Foundation, "Software-Defined Networking: The New Norm for Networks," ONF Whitepaper, April 2013.

[11] Wikipedia, "High-frequency trading," [Online]. Available: http://en.wikipedia.org. [Accessed 16 November 2013].

[12] R. Fanelli and G. Conti, "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict," in *4th International Conference on Cyber Conflict*, Tallinn, Estonia, June 2012.

[13] D. Hobbs, "Application of OCOKA to Cyberterrain," White Wolf Security White Paper, Lancaster, PA, June 2007.

[14] G. Lyon, “nmap.org,” [Online]. Available: http://nmap.org. [Accessed 11 November 2013].
[15] J. Ribeiro, “Microsoft, FBI disrupt Citadel botnet network,” Infoworld Security Central, 6 June 2013. [Online]. Available: http://www.infoworld.com. [Accessed 16 November 2013].
[16] P. Bright, “Anonymous speaks: the inside story of the HBGary hack,” Arstechnica, 15 February 2011. [Online]. Available: http://arstechnica.com. [Accessed 16 November 2013].
[17] Wikipedia, “Domain Name System,” [Online]. Available: http://www.wikipedia.org. [Accessed 17 October 2013].
[18] K. Poulsen, “Syrian Electronic Army Takes Down the New York Times,” Wired, 27 August 2013. [Online]. Available: http://www.wired.com. [Accessed 13 September 2013].
[19] J. Pereira, “How credit-card data went out wirless door,” Wall Street Journal, 4 May 2007. [Online]. Available: http://www.wsj.com. [Accessed 17 February 2014].
[20] J. Donn, J. Fahey and D. Carpenter, “NYC Utility Prepped for Big Storm, Got Bigger One,” Associated Press, 31 October 2012. [Online]. Available: http://bigstory.ap.org. [Accessed 17 October 2013].
[21] C. Burritt and B. Sullivan, “Hurricane Sandy Threatens $20 Billion in Economic Damage,” Bloomberg, 30 October 2012. [Online]. Available: http://www.bloomberg.com. [Accessed 17 October 2013].
[22] N. Falliere, L. Murchu and E. Chien, “W32.Stuxnet Dossier, v1.4,” Feb 2011. [Online]. Available: http://www.symantec.com. [Accessed September 2012].