Key Defensive Terrain in Cyberspace: A Geographic Perspective

Thomas J. Pingel
Department of Geography, University of California
Santa Barbara, CA 93106-4060, USA

ABSTRACT

Current computer network defense strategies explicitly rely on spatial metaphors to create structures that behave similarly to those found within historical physical fortifications. A more historically and geographically informed study of security in general, and fortification in particular, could provide great insight to development of improved defensive structures and strategies. Such a study would have to be based on a theoretical explanation of the translation between the geographic space of everyday life and the topological space of computer networks.

Keywords: Fortification, Cyberspace, Terrain, Security, Firewalls, Information Warfare and Computer Networks

INTRODUCTION

The bulk of the work being done to solve computer security problems comes from the field of computer science as well as industry. In turn, much of these solutions are engineering-related: new and better programs and products with fewer security bugs, patches to repair problems with existing software, and improved theoretical design with security firmly in mind are all quite common approaches to solving the computer security dilemma.

These technology and engineering approaches are invaluable toward easing the security problem. Yet these approaches alone neglect one of the most fundamental aspects of the security problem – namely, that for as long as computer networks are spatial entities, they will be subject to at least some of the same constraints as govern the "real" spaces like the ones humans inhabit in their everyday lives. If this is the case, then it seems natural to look at security problems in real-space, and see how they compare to security problems in cyber-space.

In order to provide a satisfactory explanation of the manifestation of key terrain within cyberspace, it is necessary to first explain the ontological status of the variables in question. Secondly, it is necessary to explore the similarities between real space and the space in which computer networks exist – indeed to justify the very notion that cyberspace is spatial. It is then possible to provide a reasonable definition of what key terrain in cyberspace might be. With this conceptual definition, it becomes possible to look for examples of key terrain within computer security literature.

Physical Security

By studying the evolution of human city fortification, we may be able to apply the lessons learned in human physical space to informational topological space. However, such application can only be done with a thorough understanding of offensive and defensive capability of human constructs. On one level this can be done in a very technical manner by relying on both computer science and military literature within their respective realms. More than this is required, however, for the only way to effectively translate concepts of attack and defense between the two is to first establish a medium of communication. The medium of choice is the philosophical abstraction of violence to contests of force generally, and spatial contests of force specifically. This medium can be established, in part, by relying on the literature of strategy-related computer game design.

In real space, various elements of landscapes, whether created by humans or not, contribute to or detract from the application of offensive force. Examples of these include land cover (plains, deserts, mountains), barriers (rivers, mountains, constructed walls), and transportation routes (rivers, roads, railways). Landforms that reduce or negate the capability of an offensive force are defensively significant landforms.

There are many cases when terrain-scale objects have been created by humans to aid in defense (e.g., moats, walls, ditches). Additionally, the skill of a commander rests largely on his or her ability to master the spatial configurations of landforms and armies. The choice of an advantageous battlefield can have great repercussions on the outcome of any contest of force. All of this is well known in real space, and has been documented by generals, geographers, and historians for thousands of years.

Geographers Patrick O'Sullivan and Jesse Miller have asserted that, "the fundamental strategic and tactical problems are geographical in nature." [9] Certainly this seems true in real space, but what about artificially created spaces like chessboards? Those with the same view as O'Sullivan and Miller have not made a mistake in their assertion, because strategy in games such as chess and go still depends on depth of understanding of spatial

configuration. Still, games like chess and go are explicitly spatial. Do geographic concerns also affect tactical and strategic problems that exist in more abstract spaces?

The abstraction of space in games like chess and go suggest that they do. Although these games are often played in real space, the real game playing takes place in the abstract space of the mind. The manifestation of the games is usually physical, but it need not be. If the fundamental strategic and tactical problems (in general) are geographical in nature, then making the analytical jump from physical contests of force (e.g., traditional warfare) to the contests of force in the pseudo-space of computer networks (i.e. cyberspace) should be possible.

Computer Network Security

Computer networks are spatial simply because they exist in our physical world. Computer workstations, servers, and the physical connections between them (wire, fiber optic, or wireless) exist, and exist in specific locations. More significant than just their locations, though, is that they are connected by physical lines and information switches and protocols to form networks. These networks are arranged in real space and more abstractly in their connectedness or topology.

The topology of computer networks creates a "space" that is artificial in much the same way that a "space" is created during the play of a game such as chess or go. The rules that govern network data traffic are not unlike those that govern game play in that not every type of movement is possible. Movement is regulated by the rule structure. Development of strategy and tactics in these artificial spaces (and real spaces for that matter) begins with an understanding of the rules, limitations, and capabilities of pieces within the sphere of the space created by the game.

Computer networks are now interlinked to the point that together they form the Internet. Although very large and quite dynamic, the Internet itself has its own topology. As people and data interact on the Internet, a virtual space is created. It is this virtual space that many authors and people think of as cyberspace.

Cyberspace, since it has its own topology and rules, could be thought of in much the same way as a game. Given that people, groups, and states have interests that are manifested in cyberspace, it is no wonder that conflicting interests have manifested themselves as contests of force. These contests of interest with respect to computers and networks are studied as Information Security. Information Security addresses the issues of information confidentiality, integrity, availability, and privacy.

If we have in cyberspace a spatial configuration (topology) and a contest of interest (leading to a contest of force) we may wonder whether, in such a complex structure such as the Internet, local variability in spatial arrangement may yield offensive/defensive advantages in the same way as does similar variability in real landscapes.

ANALYSIS

Terrain and Key Terrain Defined

Terrain, used in the context of security, refers to the irregularity of the land and configuration of the landscape. While most often the term refers to the relief and composition of the land surface or near subsurface, terrain (like *space*) can also refer to other types of physical configurations as well as cultural variability. [4] Such a broader definition of the term makes sense when one considers that conflict does not occur within the physical realm alone, but that spatial variability in culture also has a strong influence over the preferred method of military deployment.[1] Put more simply, the term *terrain* encompasses the irregularities and configuration of the medium of conflict in whatever forms it may take.

The United States Army Operations Manual defines *key terrain* as "any feature, locality, or area which affords a marked advantage to the combatant who controls it." [11] The Operations Manual also reminds soldiers that key terrain is "situational" and depends on the mission. Depending on the scale of conflict, key terrain (sometimes called critical terrain) varies considerably. Again, it is important to reiterate that, following the conception of terrain above; key terrain should not be thought of purely as areas or locations. Often, it is the function of these locations that distinguishes them as key. While key terrain can be something as intuitively obvious such as a geographic choke point, it can also be an important structure, road junction, or transit zone. [5]

Fortification as Key Terrain

Fortification is an attempt to control the space surrounding a settled community. The point was (and is) to limit movement and fire. The oldest form of fortification was a ditch and palisade with a gate. [5, 7] In some cases, the siting of the city itself was done so as to take advantage of the natural terrain. Walls provided cover – protection from observation and fire - and thus acted in much the same way as a portable shield. [7] Ditches and other earthwork defenses were explicit modifications of the landscape, but so too were walls, as they modified and thus defined the terrain in ways that the builders hoped (one assumes) were defensively significant.

It is helpful to briefly discuss how fortifications act as key terrain in the physical realm before delving into how

[1] Consider, for example, the significance of the political organization or state of conflict of a region and how it affects military and diplomatic deployment.

key terrain is constructed in cyberspace. First, fortifications themselves offer protection to an immediate community – the city, fort, or other settlement that the fortifications enclose. Since key terrain is identified by the marked advantage that possession of it affords, it seems logical to conclude that walls and other defensive outworks are in some way key.

At an even finer level of detail, certain portions of the defensive structure may be more key than others. For instance, as gates are intended to be selectively permeable (e.g., keeping enemies out while allowing freedom of movement for one's own troops and allies) they are also (generally) weaker than the surrounding wall. Thus as gates became the focus of an offensive force, fortification plans were adjusted to develop means to focus fire on any group attempting to storm the gates. Towers, crenellations, and bastions were all attempts to control the space surrounding the walls such that defensive fire could be directed toward an opponent with relatively much less risk of damage to the defender. [5]

Moving to a smaller scale over greater area, fortifications were a means to exert control over marginal territory far from the core area. The Roman *limes* and the Great Wall of China are both examples of such a strategy. Further, systems of forts and fortified villages also served the same purpose, though for different reasons. Examples of this abound, but as a prototypical example one may note the network of castles designed to exert power on the periphery during the Norman conquest of England. [1, 2] In these cases, key terrain becomes the fortified settlements that can bring the surrounding area under central control.

Despite the attractiveness of the concentrated wealth of the core, centers of authority were not often fortified to the same degree as the periphery. [7] Although the capitol cities of major civilizations often had some wall structures, most typically relied on defense by means of an army rather than fixed fortifications. [8]

Key Terrain in Strategic Games

Strategy games are among the most widely cherished of all games that humans play. In fact, it is difficult to imagine games that have no element of strategy whatsoever. Still, one would acknowledge that some games are more strategic than others. Those games that meet some, albeit ambiguous, threshold are termed strategy games. A further subset of these is *spatially* strategic –that is location plays a crucial part in the game. Thus we might differentiate non-spatial strategy games like poker from spatial strategy games like chess and go. Of the spatial subset of strategy games, some are conducted on (or in) metric spaces while others require no metric distance at all, but merely topological spaces.

Chess and go are both spatially strategic games that rely on topological, not metric spaces. A chessboard may of course be any size, but more importantly it may be any shape as well, so long as the "squares" are all connected in the same way. In fact, as important to the space of chess as the physical connections of the "squares" is the preservation of the movements of pieces. In chess, terrain in generated by the irregularity of space between the edges and the center, but also by the relative positions of the pieces, whose differing movement rules create an almost limitless set of possibilities for placement.

With the rise of modern powerful multimedia computing, a new set of spatial strategy games has emerged. An extremely high number of these are based on premises of contests of force. The strategic problem in these games seems to be focused on a vary particular kind of opposition – states of war between groups.

Of the most popular of these is the series of Warcraft games produced by Blizzard Entertainment. Blizzard boasts the most active multiplayer network[3], where thousands of competitors daily compete against one another in mock battle scenarios. In this case the spaces of conflict are pixilated versions of battlefields, where users can download but also create maps on which others can play. Most fascinating about this is that users are given the opportunity to *create* terrain with a map, instead of simply describe or interpret it. Now instead of enhancing terrain, and building key terrain piecemeal, where opportunity arises, humans create a (strongly) geographic terrain from scratch. In one sense, users are creating terrains every bit as much as they are creating maps.

Another interesting aspect of computer strategy games is that experienced map creators seem to incorporate key terrain into many maps. The variability of the terrain in the maps coupled with the wide variety of troop capabilities enables an even larger set of possibilities of position that chess or go. But map creation is not haphazard. Maps seem to be created with the idea of a few important spots on the map that are important to hold. The strategic description of the maps that accompany the game Starcraft, one of the latest in the Warcraft series, uses language that does not differ substantially from military science texts. It admonishes players to seize strategic sites and areas, and outlines key locations on a map where players should place defenses. [6]

The surprising part of this is not that players are taught to seize key spots, but that these spots are created with this in mind. For although key terrain is situational, given the known (or likely) capabilities of possible opponents, one can find, build, or augment important terrain, or arrangements of pieces in a game like chess, so that they can be reliably expected to afford one an advantage.

Key Terrain in Computer Networks

Computer networks are similar in many ways both to real cities and spatial strategy games. The security of a network rests on a variety of factors, among them the topological design. The topology of a computer network is influenced by physical connections between hardware, but also the implementation of software, particularly routing and firewall rules sets. The success of an attack on, or defense of, a network depends heavily on how well key terrain of the network is understood and incorporated.

There are several broad types of spatial entities often employed in the defense of a computer network, and many of the names of these categories give some intuitive understanding of how they perform. Firewalls are one primary type of spatial defense that typically attempts to restrict and define network traffic between networks, usually a small network and the Internet. Although specific types vary, it is essentially a filter, such that all traffic bound in or out of the network must pass through the firewall. Traffic is inspected (in a variety of ways) and compared against a set of rules specified by a security plan. In practice, there may be several routes in to and out of a network. For a firewall-type defense to be successful, it must be employed in all routes.

The deployment of firewalls highlights the similarities between the topological space of computer networks and the geographic space in which human settlements exist. During the deployment of a firewall, the space surrounding a network is occupied and a new structure interferes with "normal" traffic and movement. This corresponds quite closely to the construction of walls and gates around settlements.

Another method of spatial defense is the construction of a "bastion host", a public face and the most heavily fortified element. [12] In one of the original formulations of the bastion host, it was identified as "a critical strong point in the network's security" [10] The assumption behind this defense strategy is that the most public face of a network (e.g., the host that offers services such as web hosting, file servers, or terminal access) is the most likely to be attacked. Thus one can focus one's security efforts on a single host rather than distributing one's efforts among many hosts.

Bastion hosts were so-named because they "overlook critical areas of defense". [10] In the Renaissance forts in which they originated, bastions were an attempt to provide protected means to defend gates by focusing interlocking fields of fire such that the adjacent two bastions could target any attacker trying to breach a gate or wall. Any bastion, which was itself targeted, could be similarly defended by its two adjacent bastions. [5]

One final spatial security element sometimes employed in network defense is the construction of a perimeter demilitarized zone (DMZ) network, on which the bastion host might operate. [12] The physical separation afforded by the DMZ (sometimes called a perimeter network) prevents intrusion by creating a space between two barriers. One barrier exists between the Internet and the perimeter network while another barrier exists between the perimeter network and the internal network. Thus if an attacker successfully penetrates the first barrier he or she must still overcome another barrier before he or she is able to access the sensitive information restricted to the internal network. The DMZ essentially provides greater depth of defense so that there is not a single point of failure, but rather several reinforcing security mechanisms.

The names for these components of network security (firewalls, bastion hosts, and DMZs) are misleading, and this drives a wedge between the translation of security concepts developed for physical space to those developed for use in network security. For instance, there is some ambiguity in the literature as to whether a firewall is a component of defense or a description of a network's defenses in total. Notwithstanding this, the term *firewall* is a security term in the physical realm, but not a military one. Although it does represent a compartmentalization, it certainly isn't principally a protection from *attack*. Bastions, in military history, were certainly heavily fortified, but not because they were to serve as an entry point or exit point for distribution of services. Finally, formal demilitarized zones in military history have been defined in a number of treaties, perhaps the most famous of which is that created near the 38th Parallel between North and South Korea. While such a region can and does serve as a buffer or frontier, stipulations in the treaty (as in the 1919 Treaty of Versailles after World War One) dictate that fortifications and military assembly or maneuver are strictly forbidden within a certain defined area. This seems quite counter to the admonition in network security manuals to "pay special attention to the [bastion] host's security" and that it should be "the most fortified host" given also that bastion hosts should be located in a network DMZ. [12]

Despite the differences in terminology, however, there are astounding similarities between the methods of securing computer networks and fortifying cities. This stems from the fact that both are faced with a similar problem to overcome: they have to develop a system that can keep attackers out while allowing legitimate traffic to flow. The metaphor of space and movement permeates through computer terminology as a whole and so network security engineers are on to something when they spatialize the problem they try to solve. By doing so, they tap in to a wealth of knowledge that physical security engineers have been dealing with for thousands of years.

The fortifications employed in network security are one example of how key terrain is created in cyberspace. Like strategic games, the topological space of networks is filled in by various structures that influence how movement flows. The computer security engineer, then, tries to create fortification designs that seem to transcend most situational variability.

REFERENCES

[1] Addington, L.H., *The patterns of war through the eighteenth century*. 1990, Bloomington: Indiana University Press. xii, 161.

[2] Beeler, J.H., *Castles and Strategy in Norman and Early Angevin England.* Speculum, 1956. Volume 31(Issue 4): p. 581-601.

[3] Blizzard Entertainment, *Company Profile*. 2003, Blizzard Entertainment.

[4] Collins, J.M., *Military geography for professionals and the public*. 1st Brassey's ed. An AUSA Institute of Land Warfare book. 1998, Washington D.C.: Brassey's. xxiv, 437.

[5] De la Croix, H., *Military considerations in city planning: fortifications.* 1972, New York: G. Braziller. 128.

[6] Farkas, B. and Blizzard Entertainment (Firm), *StarCraft : Prima's official strategy guide*. 1998, Rocklin, Calif.: Prima Pub. vii, 246.

[7] Keeley, L.H., *War before civilization*. 1996, New York: Oxford University Press. xiv, 245.

[8] O'Brien, P., *L'Embastillement of Paris: The Fortification of Paris during the July Monarchy.* French Historical Studies, 1975. Volume 9(Issue 1): p. 63-82.

[9] O'Sullivan, P.M. and J.W. Miller, *The geography of warfare*. 1983, London: Croom Helm. 172.

[10] Ranum, M., *Thinking about Firewalls*. 1993, Digital Equipment Corporation.

[11] United States. Dept. of the Army, *Operations.* Department of the Army field manual; FM 100-5. 1986, Washington DC: Headquarters Dept. of the Army.

[12] Zwicky, E.D., S. Cooper, and D.B. Chapman, *Building Internet firewalls*. 2nd Ed 2000, Beijing; Cambridge Mass.: O'Reilly. xxi, 869.