2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Permission to make digital or hard copies of this publication for internal use within NATO and for personal or educational use when for non-profit or non-commercial purposes is granted providing that copies bear this notice and a full citation on the first page. Any other reproduction or transmission requires prior written permission by NATO CCD COE.

Strategic Anti-Access/Area Denial in Cyberspace

Alison Lawlor Russell, Ph.D.
Department of Political Science
Merrimack College
North Andover, MA USA
russella@merrimack.edu

Abstract: This paper investigates how anti-access and area denial (A2/AD) operations can be conducted to deny actors access to cyberspace. It examines multiple facets of cyberspace to identify the potential vulnerabilities within the system that could be exploited. This project will also touch upon the policy implications of strategic cyber A2/AD for national security, particularly as they relate to deterrence strategy, coercion, and interstate conflict.

The question of deterrence is particularly important. Given the extensive reliance of modern states and societies on cyberspace, the ability to deny access to cyberspace would threaten the economy, security, and stability of a state. A credible threat of this nature may be sufficient to deter armed conflict or compel a more favorable course of action. Thus, strategic A2/AD in cyberspace may create new options and tools for international relations.

This paper will address strategic A2/AD with regards to the physical aspects of cyberspace (i.e., cables, satellites). It will assess the strengths and potential vulnerabilities of the physical attributes (the architecture) of cyberspace, as they relate to potential A2/AD operations. It will also address the relevant policy and strategy implications of strategic cyber A2/AD for states, including how this may affects the development of cyber security strategy, critical infrastructure protection, and private sector cooperation. The paper will offer conclusions and recommendations to policymakers and scholars.

Keywords: *infrastructure, anti-access/area denial, A2/AD, strategy, deterrence, conflict*

1. INTRODUCTION

The Information Age of the twenty-first century is distinguished by the proliferation of networks of power that transmit information in a variety of forms and have the effect of defining and decentralizing power relationships. The instantaneous transmission of information through vast geographic space has made our current global economic system possible, as it has the operations of modern governments, militaries, and social organizations. Their capabilities

hinge on the accessibility of cyberspace to all participants. To be absent from these networks of information is to be absent from power.[1]

Cyberspace is the modern communications network that underpins global information exchange and services. It is ubiquitous, complex, and much bigger than the internet alone. It underpins the global economic order and is essential to all elements of state power, from military operations to electricity to basic communications. Old networks, such as plain old telephone systems, have been integrated into the newer and more efficient networks of cyberspace. Cyberspace is so ubiquitous that strategic connectivity is rarely questioned.

Nevertheless, connectivity to cyberspace should not be taken for granted, especially by states. Cyberspace is a man-made network to which a state can be connected and disconnected, sometimes against its will. Cyber blockades can occur and states can be denied access to cyberspace[2]. The experience of North Korea in December 2014 illustrated just how quickly and completely a state can be denied access to cyberspace. For nine and a half hours on December 22nd, North Korea suffered a total outage of internet connectivity. At the time of writing, the cause the incident were still being investigated, but the event was consistent with a cyber attack, and it came just days after the U.S. Federal Bureau of Investigation said that North Korea was responsible for a major cyber attack on Sony Pictures. However, experts cautioned that the event could also be attributed to other causes, such as power problems.[3]

Deliberate actions to deny a state access to cyberspace and/or diminish its capacity to operate freely therein may be considered anti-access and area denial operations. The modern understanding of anti-access and area denial operations (or A2/AD operations, as this article will refer to it) specifically means to deny an adversary the ability to bring its operational capabilities into the contested region or to prevent the attacker from operating freely within the region and maximizing its capabilities.[4]

This definition of A2/AD strategy evolved from assessments of anti-access warfare strategies in other domains, that is, on land, at sea, and in the air. The United States Department of Defense has designated cyberspace the "fifth domain" for defensive operations and warfighting, thus it is appropriate and prudent to investigate the extension of strategies, such as A2/AD from the other domains to cyberspace.[5]

The goal of this paper is to examine how A2/AD can occur at the physical layer of cyberspace and understand some of the implications of this for policy and strategy[6]. This article will begin with

1 Manuel Castells, *Communication Power* (New York: Oxford University Press, 2009).

2 Alison Lawlor Russell, *Cyber Blockades* (Washington DC: Georgetown University Press, 2014).

3 Chloe Albanesius, "Internet in North Korea Offline after Apparent Attack," PC Magazine, http://www.pcmag.com/article2/0,2817,2474065,00.asp.

4 Sam J. Tangredi, *Anti-Access Warfare : Countering A2/Ad Strategies* (Annapolis, Maryland: Naval Institute Press, 2013), 1-2.

5 Cyberspace differs from the other domains in three important ways. Firstly, the other domains would exist without human action. Cyberspace was created by humans and will cease to exist and function without continued human interaction and upkeep. Secondly, cyberspace traverses the other domains. Fiber optic cables run along the sea floor, satellites transmit information, wireless signals fly through the air. The other domains touch, but do not rely on each other in the same way that cyberspace relies on the other domains. Thirdly, the topography of cyberspace is constantly changing and being modified by human interaction. As the terrain is constantly changing, it is especially difficult to protect and defend against attacks.

6 This article is part of a broader research project to examine A2/AD at all layers cyberspace. To meet CYCON publication requirements, this article will focus solely on the physical layer of cyberspace.

an overview of anti-access warfare and A2/AD strategies. Next, it will examine the elements of the physical layer of cyberspace, specifically cables, satellites, and the electromagnetic spectrum and discuss their potential vulnerabilities to A2/AD operations. Lastly, the article will conclude with a discussion about the implications of this for cyber security and strategy for policy makers and scholars.

2. ANTI-ACCESS WARFARE AND A2/AD

2.1 Anti-Access Warfare

Written records of anti-access warfare strategies date back 480 B.C., when the independent city-states of Greece were menaced by the Persian emperor Xerxes and the largest armed force ever assembled at that time[7]. According to the historian Herodotus, Xerxes' forces numbered 1.7 million troops, and 1,327 warships (although the number of troops was, in all likelihood, much smaller; the larger number may have included warriors as well as camp followers). In contrast, the Greek city-states had only a few thousand defenders each and they had rarely before been united.[8]

The weaker Greek city-states were able to defeat Xerxes and his great army by pursuing a strategy of anti-access. By preventing the necessary supply ships from reaching the soldiers ashore, they turned Xerxes strength into a weakness; his army was too big to live off the land and could not survive without shipments of grain, which could only be brought by sea. The power of the anti-access strategy is that it allowed the weaker force to prevent the stronger force from bringing its resources to bear in the theater of operations; it neutralized the superior force and then waited for time, attrition, and/or extrinsic events to shake the determination of the attacker.[9]

A2/AD operations include a variety of military activities that can occur on land, in the air, at sea, and in space. Traditionally, A2/AD activities have been designed to establish and maintain control of the battlespace—an objective of any military force. The goal is to deny the adversary the ability to enter the area and maneuver freely within the battlespace. Anti-access and area denial are different, but related concepts that offer a nuanced approach to deny the adversary the ability to operate within a contested zone.

Anti-access traditionally refers to the ability to cordon off an area and control entry to it, thus to effectively deny the adversary entry to the contested area. Area denial refers to the ability to diminish, degrade, or destroy the adversary's freedom of action within the contested area. In short, A2 affects movement to a theater, while AD affects movement *within* a theater.

From the U.S. perspective, A2/AD is a contingency for which it must plan for and against. In some cases, the U.S. military may seek to employ A2/AD strategies against an adversary, while in other cases, an adversary may try to use an A2/AD strategy against the U.S. military. Within the U.S. military and policy community, A2/AD is also commonly associated with the "AirSea

7 For an excellent historical analysis of anti-access warfare, see Tangredi, *Anti-Access Warfare : Countering A2/Ad Strategies*.
8 Ibid., 7-8.
9 Ibid., 8-15.

Battle Concept" and other joint operations, it is also applicable to the cyber domain, where access is a necessary precondition to being able to operate from any distance.

2.2 Anti-Access/Area Denial (A2/AD) Operations in Cyberspace

The concept of A2/AD as it pertains to cyberspace is a relatively recent and evolving concept in warfare. Most of the extant literature about anti-access warfare or anti-access and area denial strategies focuses on what has been done historically at sea, in the air, and on land, and what is being discussed now regarding U.S. military planning for future threats, specifically those that might emanate from Asia[10]. Information and communications has long been considered as a key to victory or defeat in conflict, whether it was Sun Tzu's emphasis on intelligence gathering and deception, or more recent decision-making theories such as Boyd's OODA loop theory. A2/AD in cyberspace does not seek to manipulate the information itself, but rather to disrupt and prevent the flow of information.

The capability to conduct A2/AD in cyberspace, or "cyber A2/AD," exists on two levels. At the tactical level, cyberspace can be used as an avenue for conducting cyber attacks that will result in A2/AD of other domains. For example, sophisticated cyber attacks may be designed to destroy specific satellite imagery capabilities, missile targeting, or even navigational equipment to facilitate A2/AD operations at sea or in the air.[11] This level of cyber A2/AD is commonly discussed and relatively well-known by operational planners and cyber tactical teams.

At the strategic level, cyber A2/AD receives very little attention and is relatively under-examined by scholars and policy makers. This strategic cyber A2/AD is the target of this research paper. Strategic cyber A2/AD is defined here as the ability to gain control of the network or infrastructure of cyberspace and manipulate it in such a way as to deny a state the ability to use cyberspace *in any capacity*. Unlike tactical cyber A2/AD, it does not target the functionality of specific weapons or information systems that are connected to cyberspace, but rather targets states' access to the grid itself.[12]

A2/AD in cyberspace is of significant and increasing concern for US national security. In the Joint Operation Access Concept of 2012, U.S. Department of Defense (DoD) identified three trends that directly led to the increase of A2/AD capabilities around the world in recent years. One of these trends is the "*emergence of space and cyberspace as increasingly important and contested domains*" (emphasis added) as a factor affecting the rise of A2/AD threats. In addition to proliferation of advanced technologies and changing US defensive posture, the proliferation

10 There is a dearth of scholarly literature on anti-access warfare, with the notable exception of Sam J. Tangredi's book *Anti-Access Warfare*, while the media and government reports on the subject tend to focus on the specifics of current military planning. Discussions of anti-access warfare and cyberspace in any of the literature are rare and usually quite limited.

11 Harry Kazianis, "The Real Anti-Access Story: Cyber " *Flashpoints: Diplomacy by Other Means* (2013), http://thediplomat.com/flashpoints-blog/2013/05/15/the-real-anti-access-story-cyber/; Nathan Freier, "The Emerging Anti-Access/Area-Denial Challenge," (Center for Strategic and International Studies, May 17, 2012).

12 This definition specifically focuses on denying *states* the ability to access cyberspace. Non-state actors are exceedingly important actors in the international system and particularly in cyberspace, but anti-access warfare strategies have long been the purview of states, city-states, empires, and other recognized political entities that control territory and raise armed forces. The effort to keep individuals and groups out of cyberspace would more likely fall into the realm of law enforcement and domestic control, as opposed to military operations and international relations.

of and dependence on cyberspace is a leading factor in the A2/AD vulnerability.[13] Furthermore, one of the main precepts identified for achieving operational access in the face of armed opposition is to "protect space and cyber assets while attacking the enemy's cyber and space capabilities."[14] As DoD struggles to address A2/AD, policy makers must come to a greater understanding of how cyberspace works, in order to protect US access and potentially deny it to adversaries.

A preliminary examination of the structure of cyberspace suggests the ways that A2/AD can be achieved in that domain. Cyberspace is a global grid that can be manipulated, expanded, and contracted to increase or decrease accessibility. It is comprised of multiple layers, which means that there are different types of vulnerabilities inherent in cyber A2/AD, depending on the layer of cyberspace. Most scholars agree that there are four layers to cyberspace: the physical foundations, the logical layer, the information layer, and the users.[15] The rest of this paper will focus on A2/AD at the physical layer of cyberspace.

3. THE PHYSICAL LAYER OF CYBERSPACE

The physical layer of cyberspace is comprised of physical elements, from fiber optic cables to cell towers, to computers and servers. Of chief importance are the fiber optic cables that traverse the globe, overland and undersea, that transmit data packages from one location to another. In addition to these cables, there are physical nodes of cables (where cables come together) called internet exchange points, and server farms that centralize the processing of data packages and route them to their final destination. In addition to fiber optic cables, there are satellites that are essential to government and commercial communications, although they transmit only a small fraction of the information that flows through cyberspace. Lastly, the electromagnetic spectrum is a constituent part of cyberspace—essential to its functioning and basic operations.

3.1 Cables

3.1.1 Submarine Cables

Submarine cables traverse ocean, sea, and lake floors carrying about 95 percent of all intercontinental telecommunications traffic, in the form of voice and data. International banking and finance activities are highly dependent on these cables, and government and military traffic uses them also. Data and voice communications can be passed via satellite, but it is significantly less expensive and faster to use fiber optic cables. These cables are the fibers that hug the globe and underpin the modern telecommunications system.[16]

There are approximately 1.197 million kilometers of undersea cables.[17] The longest cable systems connect continents, while shorter systems are laid along coastlines to avoid the

13 U.S. Department of Defense, "Joint Operational Access Concept," (2012), ii.

14 Ibid., iii.

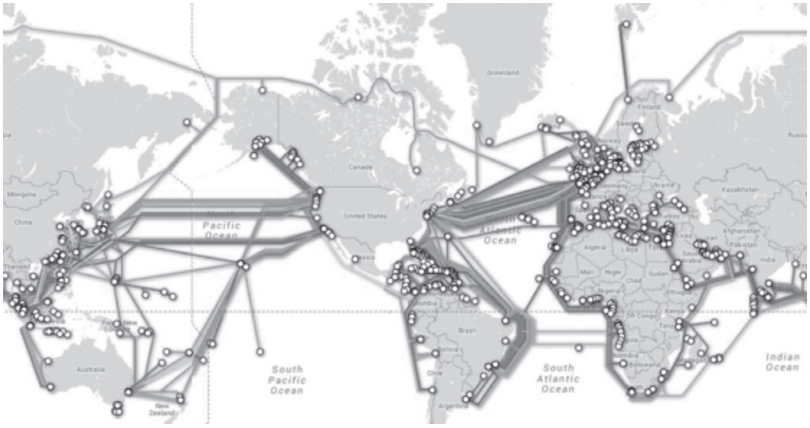
15 Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001); Nazli Choucri and David D. Clark, "Integrating Cyberspace and International Relations: The Co-Evolution Dilemma," in *ECIR Workshop on Who Controls Cyberspace?* (Explorations in Cyber International Relations, Harvard University and Massachusetts Institute for Technology, 2012).

16 Burnett D. Carter L., Drew S., Marle G., Hagadorn L., Bartlett-MacNeil D., Irvine N., "Submarine Cables and the Oceans - Connecting the World," in *UNEP-WCMC Biodiversity Series* (ICPC/UNEP/UNEP-WCMC, 2009), 3.

17 Adam Blenford and Christine Jeavans, "After Snowden: How Vulnerable Is the Internet?," *BBC News* January 27, 2014.

problems of terrestrial cables and provide additional resiliency. The highest concentration of cables connects the east coast of the United States with Europe. The largest capacity cables connect New York and the United Kingdom.[18]

FIGURE 1: SUBMARINE CABLE MAP FROM TELEGEOGRAPHY (HTTPS://WWW.ISCPC.ORG/CABLE-DATA/)



Most submarine telecommunications cables are fiber-optic cables, especially newer cable systems. The older coaxial cables are still in use in some places, but their bandwidth capacity is much more limited. Fiber-optic cables have become the primary cable due to increased demand, changes in technology, and reduced cost.[19]

While fiber-optic cables may be relatively new, submarine telecommunications cables are not. The first underwater cable, a copper-based telegraph cable, was laid in 1850 across the Channel to connect the United Kingdom and France.[20] Likewise, tampering with underwater cables is also nothing new. As far back as the Spanish-American War, undersea telegraph cables were destroyed as part of the campaign to sever trans-Atlantic communications links.[21] During the Cold War, the United States famously tapped into Soviet cables to listen to conversations behind the Iron Curtain.[22] More recently, three men were arrested for trying to cut through an undersea cable off the coast of Alexandria, Egypt in 2013.[23] Whether subjected to tampering or destruction, these cables can suffer from unintentional damage as well as sabotage, which threatens to undermine the efficiency, reliability, and security of the global network.

There are approximately 100-150 cable faults or damages every year. Most of the damage that submarine cables suffer is accidental, such as a ship dropping anchor in the wrong place and

18 U.S. Department of Homeland Security, "Characteristics and Common Vulnerabilities Infrastructure Category: Cable Landing Stations," (Draft - Version 1, January 15, 2004), 2-3.
19 Ibid., 1.
20 Carter L., "Submarine Cables and the Oceans - Connecting the World," 3.
21 Charles Cheney Hyde, *International Law, Chiefly as Interpreted and Applied by the United States*, 2nd rev. ed., 3 vols. (Boston, MA: Little, Brown and company, 1945), 1956.
22 Sherry Sontag, Christopher Drew, and Annette Lawrence Drew, *Blind Man's Bluff : The Untold Story of American Submarine Espionage* (New York: Public Affairs, 1998).
23 "Egypt Arrests as Undersea Internet Cable Cut Off Alexandria," *BBC News*, March 27, 2013 2013.

damaging the cables as they run through shallower waters. Fishing gear such as trawlers are the most common culprit for damage to cables, accounting for roughly half of cable cuts. Over the past five decades, fishing gear and anchors combined represent approximately 70 percent of damage done to submarine cables.[24] As a result, the location of submarine telecommunications cables and their landing stations are often marked on nautical charts and coastal maps, so that ship operators and others may avoid them. These cable cuts happen frequently but most of them are minor and result in little disruption in service.

Submarine cables may also be damaged due to natural disasters and earthquakes. These events represent approximately 12 percent of damage to cables.[25] These events are relatively rare, but they can render catastrophic damage to telecommunications systems. On May 23, 2003, Algeria experienced an earthquake that damaged its telecommunication cables and its satellite ground stations, thus severing almost all of its international telecommunications services. Furthermore, the recurring aftershocks from the earthquake impeded repairs of the submarine cables, which were not completed until June 21, 2003.[26]

Finally, deliberate state action and other human action accounts for approximately 8 percent of cable damage.[27] Human actions may include dredging (such as that associated with beach replenishment), pipeline construction, oil and gas extraction, dumping, and scientific research. Fortunately, cuts near the shore can be repaired relatively quickly because the cables are more accessible. Damage to cables farther out at sea, and at depths of more than 4,000 meters, takes longer to repair and requires specialized equipment.[28]

There is no force tasked with protecting submarine cables, and the responsibility to avoid the cables falls to individual mariners, who are expected to consult the latest charts and abide by local laws to protect cables. In some places, coast guards and navies focused on littoral operations may have an increased responsibility to protect this critical infrastructure because these cables are most vulnerable as they come ashore on the beach head, where they ultimately meet pipes that protect them as they run inland. Thus, maritime military and law enforcement forces (i.e., navies and coast guards) potentially have a role to play in monitoring and protecting critical infrastructure for cyberspace.

3.1.2 Terrestrial Cables

Cable networks that run over land consist of physical lines, transmission line amplifiers, network protection equipment, wavelength termination equipment, and supervisory circuitry.[29] Submarine cables come ashore at cable landing stations, where they are then connected to communications networks on land. Some of these stations are located in densely populated areas, such as New York City, while others are in more remote locations, such as Nedonna Beach, Oregon. At the landing stations, the cables (or fibers, as they are sometimes called) are encased in protective tubes or casings and trenched (i.e., placed in a trench dug for this purpose)

24 Carter L., "Submarine Cables and the Oceans - Connecting the World," 45.
25 Ibid.
26 U.S. Department of Homeland Security, "Characteristics and Common Vulnerabilities Infrastructure Category: Cable Landing Stations," 7-8.
27 Carter L., "Submarine Cables and the Oceans - Connecting the World," 45.
28 Ibid., 44-47.
29 U.S. Department of Homeland Security, "Characteristics and Common Vulnerabilities Infrastructure Category: Cable Landing Stations," 6.

or routed along existing rights of way, such as railroad tracks and bridges. Cables, protected by these tubes, bring connectivity inland.[30]

Terrestrial cables are most exposed at the cable landing sites, where they are vulnerable and can be subject to accidental or intentional damage. Common threats to cables include attacks that target the fiber itself, the switching/network control equipment to which it attaches, and the electrical power system that supports it. The cables that are exposed above ground (for instance, from the shoreline to a building or along a right of way) and those that are subterraneous but easily accessible (i.e., below a manhole cover), are most vulnerable to damage.[31]

Cable landing sites often consist of one building with telecommunications equipment. Localized damage to cables and equipment at landing stations is relatively easy to repair, unless the area is unreachable (due to debris, flooding, contamination, or other conditions which may be created by an attack or a natural disaster). The primary security of the cables lies in the resiliency and flexibility of the network. First, the network has "self-healing" powers to reroute traffic away from nodes or pathways. Thus, damage to one cable or landing station is unlikely to have a noticeable effect on routine operations. Second, the cables, landing stations, and other stations are not permanently tied to specific locations and they can be relocated to another place that is more secure.[32] Cyberspace is a partially man-made network, thus we have the ability to change elements of its geographical configuration.

Damage to the landing stations themselves can be conducted directly through a physical attack on the building (such as a bombing or armed assault), indirectly (such as an attack on the power supply), and through internal sabotage (such as a computer virus or worm, fire, or physical damage). Indirect attacks on power sources are unlikely to be successful because landing stations have battery back-up power generator systems, but they are still possible. More likely, a disruption of power to a cable landing station would be part of a larger interruption of service (attack or otherwise) on the regional area.[33]

There are typically minimal forms of physical protection for cable landing sites, making a physical attack possible. Many cable landing sites are completely unprotected, simply small buildings on a beach somewhere. Of those that have some protection, they typically have chain-link fences and basic video surveillance equipment. Thus, as a small area with limited physical barriers it is relatively easy to conduct physical damage to this infrastructure.

Another challenge to managing the vulnerabilities of the physical infrastructure is that the information about the location of cables landing ashore is publically knowable in many places. In the United States, the Federal Communications Commission (FCC) mandates the public availability of licenses for all cables that touch its shores.[34] Furthermore, there are numerous articles discussing risk to critical infrastructure, including cyber infrastructure, which provide

30 Ibid., 4-6; Andrew Blum, *Tubes: A Journey to the Center of the Internet*, 1st ed. (New York: Ecco, 2012).
31 U.S. Department of Homeland Security, "Characteristics and Common Vulnerabilities Infrastructure Category: Cable Landing Stations," 7.
32 Ibid., 6-7.
33 Ibid., 7.
34 Sam Biddle, "How to Destroy the Internet," Gizmodo.com, http://gizmodo.com/5912383/how-to-destroy-the-internet.

specific information about the location of some of the infrastructure.[35] In addition, it is not difficult to obtain the equipment to find a cable line underground and destroy it–a line tracer and an axe will suffice. Despite this, the interconnectedness of land networks provides resiliency for the system.[36]

3.2 Satellites

Satellites are another essential part of cyberspace, but they transmit only 5 percent of voice and data telecommunications. When compared with fiber optic cable networks, they are five times slower and have 0.3 percent of the capacity. They are also more than 50 times more expensive per megabits per second. Furthermore, the design lifespan of satellites is 10-15 years, whereas it is 25 years for cables.[37]

TABLE 1: COMPARISON OF SATELLITES AND SUBMARINE FIBER OPTIC CABLES ACROSS SEVERAL KEY FACTORS IN TELECOMMUNICATIONS.[38]

Comparison Factor	Satellite	Optical Subsea
Latency	250 milliseconds	50 milliseconds
Design Life	10-15 years	25 years
Capacity	48,000 channels	160,000,000 channels
Unit cost per Mbps capacity	$737,316 US	$14,327 US
Share of traffic: 1995	50%	50%
Share of traffic: 2008	3%	97%

Private sector communications satellites provide an array of service, including voice and internet service. These satellites usually orbit in Middle Earth Orbit, a distance of 200 to 930 miles from Earth. The larger the satellite, the greater the power capacity, and thus the higher an orbit it is capable of achieving. The major players in private sector communications satellites are ViaSat, Space Systems/Loral, O3b, Eutelsat, and IntelSat.[39]

Satellite access faces several challenges for end users, in particular: high cost, signal latency, signal strength, and interference. With regards to the economics of satellites, they have high upfront costs ($50 to $400 million dollars for a large satellite)[40] and marginal returns, particularly communications and internet satellites that are competing with the more efficient cables that have much faster rates of transmission.[41] Signal strength and integrity are also an issue; due to interference and power requirements for satellites, signal reliability can be unstable.

35 Paul Saffo, "Disrupting Undersea Cables: Cyberspace's Hidden Vulnerability," International Relations and Security Network (ISN), http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=162869.

36 Blenford and Jeavans, "After Snowden: How Vulnerable Is the Internet?."

37 John K. Crain, "Assessing Resilience in the Global Undersea Cable Infrastructure" (Naval Postgraduate School, 2012), 3.

38 Ibid. Adapted from C. Donovan, "Twenty thousand leagues under the sea: A life cycle assessment of fibre optic submarine cable systems" Masters Thesis, The Royal Institute of Technology, Stockholm, Sweden, 2009.

39 Alistair Barr and Andy Pasztor, "Google Invests in Satellites to Spread Internet Access," *The Wall Street Journal* June 1, 2014.

40 "The Cost of Building and Launching a Satellite," http://www.globalcomsatphone.com/hughesnet/satellite/costs.html.

41 Latency is the measure of response time, but the "speed" of a network commonly refers to throughput/bandwidth.

Additionally hardware capability is particularly important for satellites. Satellite manufacturing is a time-consuming process and it requires significant lead time, such as five to ten years for larger satellites. Following Moore's Law, rapid improvement in technological capabilities means that by the time satellites are launched, their hardware may already be out-of-date. Microsatellites, which can be developed in one to two years at a cost of only a few million dollars, may be a solution to this problem.[42]

Satellites face vulnerabilities in space and on the ground. In space, their primary challenges include missiles, space debris, and hacking. On the ground, their control stations are physical targets that can be compromised by deliberate action, accidental causes, or acts of nature.

Anti-satellite missile systems have been a threat since the 1950s and they continue to be developed today. In 2007, China demonstrated its anti-satellite missile capability by destroying a defunct weather satellite at 537 miles above Earth. Similarly, the United States destroyed a spy satellite in 2008 at 150 miles above Earth.

Space debris is also a threat to satellites. Debris is created by man-made objects in space, including old satellites, spent rocket stages, and fragments from erosion, collision, and disintegration of items in orbit. In 2009, the U.S. Iridium 33 communications satellite collided with a defunct Russian military communications satellite Cosmos 2251. The collision caused a significant increase in debris, requiring the International Space Station to execute avoidance maneuvers.[43] Likewise, the aforementioned Chinese weather satellite that was destroyed in 2007 resulted in significant debris due to the way in which it was shot down.[44]

Satellite hacking has already been reported.[45] Given that satellites are often sent up with outdated technology, vulnerabilities are likely to grow over time. The technological expertise required to hack a satellite may be found within state resources and armed forces, as well as within the hacking community. Indeed, China was accused of hacking into U.S. weather satellites in 2014[46], but there are also claims of blackhat and whitehat hackers hacking satellites.[47]

Satellite communications relies on ground stations to receive information and track satellites moving through orbit. The ground stations function as a hub to receive information from the satellite and connect it with terrestrial communication networks, such as the internet. Ground stations can also be used to upload computer programs or issue commands to the satellite. These stations are susceptible to physical attack as well as natural events, such as earthquakes, tornadoes, and tsunamis.

42 Conrad de Aenlle, "U.K. Firm Finds Niche in 'Discount' Satellites" *The New York Times* June 19, 2001

43 "International Space Station Again Dodges Debris," *Orbital Debris Quarterly News, National Aeronautics and Space Administration* 15, no. 3 (July 2011).

44 "Chinese Asat Test," Center for Space Standards & Innovation, http://www.centerforspace.com/asat/.

45 Mary Pat Flaherty, Jason Samenow, and Lisa Rein, "Chinese Hack U.S. Weather Systems, Satellite Network," *Washington Post* November 12, 2014.

46 Ibid.

47 Stephen Northcutt, "Are Satellites Vulnerable to Hackers?," http://www.sans.edu/research/security-laboratory/article/satellite-dos.

4. IMPLICATIONS FOR CYBER SECURITY

It is clear from the previous assessment that the physical infrastructure of cyberspace can be degraded or destroyed in a way that would prevent an adversary from accessing the contested area (in the case, cyberspace) and/or, if the enemy is already present, to diminish its capacity to maximize its capabilities.

In order to completely deny an enemy access to cyberspace, the opposing force would first need to drive the enemy out of cyberspace. In this way, cyber A2/AD is significantly different from A2/AD in other domains because of its compression of time and space. Countries already have a presence in the domain and have immediate access to all parts of cyberspace. This is in stark contrast to the maritime domain, for example, where a ship launched in the Atlantic Ocean does not have immediate access to Straits of Malacca. Thus, A2/AD in the maritime domain would involve preventing entry to a specific region within the domain; in cyberspace, it is necessary to cut off their access to the domain entirely.

States can be cut off from cyberspace through attacks on the physical infrastructure that connects them to the grid. The cables that connect them to other countries, whether terrestrial or submarine, must be damaged or destroyed and satellites and/or their ground stations must be compromised and rendered non-functional. At this point, the country would be isolated from the international community and A2/AD could be maintained by preventing the country from re-establishing connectivity. For those who wanted to go further and prevent a country for communicating internally, domestic internet exchange points and server farms would be the next targets.

The decision to stop at isolation or continue to domestic communications depends on the goal of the attack and the broader context. If it is part of a military campaign that is expected to be quick, then isolation would likely be sufficient to degrade military capabilities and diminish command and control. If the goal requires a more extensive campaign that will likely meet with significant resistance, then attacking domestic infrastructure will weaken the state by attacking the centres of gravity, and accelerate the collapse of the state.

4.1 Strategy Implications

Cyberspace communications nodes are centres of gravity in the modern era. The ability to hold cyberspace infrastructure and communication nodes at risk is a significant factor in a conflict environment. Governments rely on cyberspace communications for command and control of military forces, economic stability, and societal well-being. Without access to cyberspace, the economy would immediately come to a halt, with millions of dollars lost each day of non-connectivity. Government, law enforcement, and security forces would have a difficult time functioning and protecting the population from domestic or foreign threats. Societal functioning would grind to a halt as people would need to develop alternate methods of doing just about everything.

Because of the serious impact of a cyber A2/AD strategy for society as a whole, it is likely that it would be applied during a military conflict, as one element of a larger campaign. At any threshold lower than armed conflict, cyber A2/AD presents the risk of potentially escalating the existing crisis to the level of armed conflict, as states could perceive the A2/AD strategy as a threat to their defences, economies, and societies.

Traditional deterrence strategies are useful to consider for preventing A2/AD in cyberspace. Deterrence is intended to convince an adversary not to take an action by leading the adversary to believe that the costs required to take the action would exceed the potential benefits derived from the action. Deterrence can be accomplished by three different means: punishment, denial, and cooperation.[48]

Deterrence by punishment occurs when the actor signals that the costs inflicted in retaliation for being attacked would outweigh the potential gains derived from launching an attack. Successful deterrence therefore depends on the actor being able to credibly threaten offensive actions in order to ensure the desired response.

In cyberspace, attribution poses a significant problem for deterrence by punishment. It is essential that states have the capability to correctly attributing the attack in order to deter potential adversaries. Without the ability to attribute the attack, there would be no way to punish the attackers. Attribution is difficult in cyberspace, but it becomes more achievable in certain contexts and when traditional intelligence methods are also utilized.[49] However, if A2/AD in cyberspace takes place during a military conflict, then attribution is no longer a problem.

A second challenge for deterrence by punishment for cyber A2/AD is that punishment itself may be difficult to achieve precisely because cyber technologies underpin the many of the capabilities that military forces may use to retaliate. A likely reason for a state to attempt cyber A2/AD against the state like the United States would be to degrade its overall military capacity, as well as prevent it from launching cyber operations. As a result, military retaliation for an A2/AD attack in cyberspace may not a viable option, and punishment may have to come from a source that was not cyber-dependent, such as political or economic sanctions.

If a state retains the capability to retaliate through kinetic or non-kinetic means, there is the issue of credibility—whether or not state seeking to deter has the capabilities to harm the adversary through kinetic or non-kinetic means. In addition, there may be a question of whether a state would follow through with a kinetic attack in response to a non-kinetic, cyber attack.[50]

Deterrence by denial is defensive and deterrence is preventive, but they both have the same ultimate goal of seeking to deny benefits of attack. Deterrence by denial is achieved through a display of capabilities that suggest the probability of succeeding in the attack is quite low. It can be achieved by reducing the vulnerabilities through hardening, redundancy, training, and continuous vulnerability analysis.[51]

48 Christopher Wrenn, "Strategic Cyber Deterrence" (Tufts University, 2012), 166-68.
49 Richard J. Danzig, "Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependecies," (Center for a New American Security).
50 Charles L. Glaser, "Deterrence of Cyber Attacks and U.S. National Security," (Cyber Security Policy and Research Institute: The George Washington University, 2011).
51 Wrenn, "Strategic Cyber Deterrence," 171.

Deterrence by denial has some advantages in cyberspace. The infrastructure of cyberspace since its earliest days has been designed for resiliency. While much of the physical infrastructure of cyberspace is relatively unprotected, located on beaches, along railways, and in buildings in densely populated areas, very little of that critical infrastructure is critical by itself. The nodes and cables may be relatively exposed and potentially vulnerable, none is singularly important to the entire system.

The infrastructure consists of redundant cables and satellites for private sector communications and military operations. The logic programming of the data and telecommunications was designed to adapt to changing circumstance, to automatically route traffic through an alternate route when the first route is unavailable. This "self-healing" property of cyberspace makes it difficult to cause substantial damage without launching a full assault against the infrastructure.

A full assault on the physical infrastructure of cyberspace would require substantial effort to target satellites and their ground stations, cables, servers, internet exchange points, and any activities within the electromagnetic spectrum. The difficulty of conducting this type of assault varies depending upon the target country. For a country that connects to cyberspace in relatively few places, such as North Korea, this may be achievable. However, for countries with a greater number of connections, such as the United States or the United Kingdom, it would be much more difficult to target all of their cables and satellites.

The downsides of deterrence by denial is that it is expensive to harden vulnerabilities and create (and maintain) redundancies. Many states or private industries may be unable, unwilling, or reluctant to invest resources in redundant capabilities instead of other more profitable ventures.

Deterrence by cooperation seeks to prevent an attack through interdependencies, norm creation, international law, and international agreements. Interdependency create networks that can be leveraged to influence the costs and benefits of a cyber attack. Norms can create a common standard for conduct that can help keep up with the rapid pace of technological development. International laws can deter, while international agreements can help to regulate cyber matters between and among states.[52]

Successful deterrence in cyberspace requires all three elements: punishment, denial, and cooperation. These elements work together to increase the costs (and difficulty) of a cyber attack beyond the desired benefit of the attack. Conversely, if there is little to no real cost to the adversary if the attack fails, then it has very little to lose by attempting attacks.[53] Fortunately, states do not need to deter all potential cyber attackers, only those that can cause the most harm. There may not be one formula of deterrence for all actors, but rather deterrence may need to be tailored to the threat or adversary. For some actors, punishment may need to play a more prominent role, whereas denial or cooperation may need to be more prominent to deter other actors.[54]

52 Ibid., 172.
53 Glaser, "Deterrence of Cyber Attacks and U.S. National Security."
54 Wrenn, "Strategic Cyber Deterrence," 166-72.

5. CONCLUSIONS AND RECOMMENDATIONS FOR POLICY MAKERS

This paper has demonstrated that strategic A2/AD at the physical layer of cyberspace is possible and would pose significant problems for military and economic power of the targeted state. Deterrence would require the threat of credible punishment, denial, and cooperation to be most effective. Each element of the triad has costs and weaknesses associated with it, but collectively they provide for the most robust deterrence.[55]

Given that several states have already issued policies articulating their potential responses to cyber attacks, or they have already engaged in actions that make their policies clear, deterrence by punishment is already underway. Further actions by policy makers may include articulating clearly defined "red lines", establishing thresholds to issue and carry out threats, and consideration for retaliation and resistance to attacks.

The next recommendation for policy makers is to invest in resiliency and redundancy to counter a potential A2/AD strategy. This recommendation is particularly important in an era of fiscal constraints and persistent budget cuts within defence departments in many countries. Despite budgetary concerns, investment in redundant and resilient physical infrastructure is a key element to ensuring that all other military capabilities are able to operate as planned. Assured access to cyberspace underpins nearly all activities of advanced militaries. Investment in infrastructure will also have several non-military benefits. There is an immediate economic benefit to the private sector companies that make satellites, cables, and server farms. In addition, it can spur innovation and upgrades for government and civilian networks alike.

The final recommendation for policy makers and scholars alike is to define the norms for codes of conduct for states and their citizens to follow. States may agree to cooperate with each other at the international level, but norms embedded in values and social structures are essential to bring the society in line with to the official policies, so that states can effectively deter their own populations from engaging in counter-norm behaviour.[56] In particular, norm generation paired with redundancy can provide for much great resistance and lessen vulnerability to A2/AD in cyberspace.

REFERENCES

Aenlle, Conrad de. "U.K. Firm Finds Niche in 'Discount' Satellites " *The New York Times*, June 19, 2001

Albanesius, Chloe. "Internet in North Korea Offline after Apparent Attack." PC Magazine, http://www.pcmag.com/article2/0,2817,2474065,00.asp.

Barr, Alistair, and Andy Pasztor. "Google Invests in Satellites to Spread Internet Access." *The Wall Street Journal*, June 1, 2014.

Biddle, Sam. "How to Destroy the Internet." Gizmodo.com, http://gizmodo.com/5912383/how-to-destroy-the-internet.

55 Ibid., 170.
56 Ibid., 169.

Blenford, Adam, and Christine Jeavans. “After Snowden: How Vulnerable Is the Internet?” *BBC News*, January 27, 2014.

Blum, Andrew. *Tubes: A Journey to the Center of the Internet*. 1st ed. New York: Ecco, 2012.

Carter L., Burnett D., Drew S., Marle G., Hagadorn L., Bartlett-MacNeil D., Irvine N. “Submarine Cables and the Oceans - Connecting the World.” In *UNEP-WCMC Biodiversity Series* ICPC/UNEP/UNEP-WCMC, 2009.

Castells, Manuel. *Communication Power*. New York: Oxford University Press, 2009.

“Chinese Asat Test.” Center for Space Standards & Innovation, http://www.centerforspace.com/asat/.

Choucri, Nazli, and David D. Clark. “Integrating Cyberspace and International Relations: The Co-Evolution Dilemma.” In *ECIR Workshop on Who Controls Cyberspace?*: Explorations in Cyber International Relations, Harvard University and Massachusetts Institute for Technology, 2012.

“The Cost of Building and Launching a Satellite.” http://www.globalcomsatphone.com/hughesnet/satellite/costs.html.

Crain, John K. “Assessing Resilience in the Global Undersea Cable Infrastructure.” Naval Postgraduate School, 2012.

Danzig, Richard J. “Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America’s Cyber Dependecies.” Center for a New American Security.

“Egypt Arrests as Undersea Internet Cable Cut Off Alexandria.” *BBC News*, March 27, 2013 2013.

Flaherty, Mary Pat, Jason Samenow, and Lisa Rein. “Chinese Hack U.S. Weather Systems, Satellite Network.” *Washington Post*, November 12, 2014.

Freier, Nathan. “The Emerging Anti-Access/Area-Denial Challenge.” Center for Strategic and International Studies, May 17, 2012.

Glaser, Charles L. “Deterrence of Cyber Attacks and U.S. National Security.” 8. Cyber Security Policy and Research Institute: The George Washington University, 2011.

Hyde, Charles Cheney. *International Law, Chiefly as Interpreted and Applied by the United States*. 2nd rev. ed. 3 vols Boston, MA: Little, Brown and company, 1945.

“International Space Station Again Dodges Debris.” *Orbital Debris Quarterly News, National Aeronautics and Space Administration* 15, no. 3 (July 2011 July 2011): 1.

Kazianis, Harry. “The Real Anti-Access Story: Cyber “ *Flashpoints: Diplomacy by Other Means* (2013). Published electronically May 15, . http://thediplomat.com/flashpoints-blog/2013/05/15/the-real-anti-access-story-cyber/.

Northcutt, Stephen. “Are Satellites Vulnerable to Hackers?” http://www.sans.edu/research/security-laboratory/article/satellite-dos.

Rattray, Gregory J. *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press, 2001.

Russell, Alison Lawlor. Cyber Blockades. Washington DC: Georgetown University Press, 2014.

Saffo, Paul. “Disrupting Undersea Cables: Cyberspace’s Hidden Vulnerability.” International Relations and Security Network (ISN), http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=162869.

Sontag, Sherry, Christopher Drew, and Annette Lawrence Drew. *Blind Man’s Bluff: The Untold Story of American Submarine Espionage*. New York: Public Affairs, 1998.

Tangredi, Sam J. *Anti-Access Warfare: Countering A2/Ad Strategies*. Annapolis, Maryland: Naval Institute Press, 2013.

U.S. Department of Defense. "Joint Operational Access Concept." 2012.

U.S. Department of Homeland Security. "Characteristics and Common Vulnerabilities Infrastructure Category: Cable Landing Stations." Draft - Version 1, January 15, 2004.

Wrenn, Christopher. "Strategic Cyber Deterrence." Tufts University, 2012.