Spring 2016

Challenges Of Implementing Defense Policies To Deter Hostile Actors In Space And Cyberspace

Stephan Dwayne Bjerring Powers

CHALLENGES OF IMPLEMENTING DEFENSE POLICIES TO DETER HOSTILE ACTORS IN SPACE AND CYBERSPACE

A Masters Thesis

Presented to

The Graduate College of

Missouri State University

In Partial Fulfillment

Of the Requirements for the Degree

Master of Science, Defense and Strategic Studies

By

Stephan D. B. Powers

May 2016

CHALLENGES OF IMPLEMENTING DEFENSE POLICIES TO DETER HOSTILE ACTORS IN SPACE AND CYBERSPACE

Defense and Strategic Studies

Missouri State University, May 2016

Master of Science

Stephan D. B. Powers

ABSTRACT

Space and cyber operations have changed national security for both nations and non-state actors worldwide. The low barriers to entry have allowed less sophisticated nations and actors to have an impact on the U.S. and near-peer nations. The lack of attribution and the ability to obfuscate the source of the space or cyber weapon will make the case for wartime retaliation difficult. The highly proactive antisatellite weapons test conducted by China in 2007 and the alleged employment of Stuxnet against Iran's nuclear program by the United States and Israel illustrates the potentially destabilizing effects to high priority national programs. If a hostile country were to remove the technological advantage, especially concerning space platforms, it could neutralize the conventional weapons advantage of the United States in future conflicts. This thesis will explore the key components of both the space and cyberspace domains. The threat of weapons employment, the unique deterrence characteristics of the space and cyberspace domains, and some case studies where these weapons have been employed. Ultimately, this paper investigates under what conditions deterrence is possible with regard to space and cyberspace technologies. In addition, answers the key question, of whether future enemies can be deterred from attacking U.S. space systems.

KEYWORDS: space, cyberspace, deterrence, space control, effects based operations

This abstract is approved as to form and content

_____

John P. Rose, PhD, Brig Gen (U.S. Army Ret.)
Chairperson, Advisory Committee
Missouri State University

CHALLENGES OF IMPLEMENTING DEFENSE POLICIES TO DETER HOSTILE ACTORS IN SPACE AND CYBERSPACE

By

Stephan D. B. Powers

A Masters Thesis
Submitted to the Graduate College
Of Missouri State University
In Partial Fulfillment of the Requirements
For the Degree of Master of Science, Defense and Strategic Studies

May 2016

Approved:

_____
John P. Rose, PhD

_____
Dana Johnson, PhD

_____
Andrei Shoumikhin, PhD

_____
Julie Masterson, PhD: Dean, Graduate College

ACKNOWLEDGEMENTS

I would like to thank all the people that supported not only my career, but also my education. Without the support of family, friends, professors, and colleagues, I am not sure if I would have been able to accomplish what I have today.

TABLE OF CONTENTS

LIST OF FIGURES

INTRODUCTION

It is difficult to deter nations, rogue states, and non-state actors from employing offensive counterspace and/or cyberspace technologies against the United States. Currently China and Russia either have developed, or are developing robust offensive capabilities to operate against U.S. interests in space and cyberspace. To counter this growing threat, the U.S. is pursuing additional capabilities to increase the resiliency of space systems to provide a level of defense against these developing counterspace technologies. In the case of radio frequency satellite communications jammers and cyber weapons, the technological cost of employing these systems is small enough that regional powers and non-state actors can be effective against more advanced nations like the United States. A fundamental shift in thinking is required to deter nations and other actors from employing offensive space and cyberspace against U.S. interests. Essentially, this should lead to a policy that includes a mechanism that ensures the cost of employing technologies against the U.S. that would outweigh the perceived benefits of their use.

The very nature of today's modern technology, which allows for instantaneous communications and global effective commerce, is also a weakness. This technology is often taken for granted by its users, and there are limited safeguards in these systems to prevent offensive effects employed by a hostile actor. If a hostile actor were to degrade the precise timing provided by navigation satellites, the effects could be devastating to not only commerce but also many other critical facets of everyday life. The need to determine the difference between what is a nuisance intrusion or a sophisticated attack

will require a concerted effort by the U.S. government in order to solve. The complexity of the employed weapon, and the method of employment, affect the ability to detect and attribute the hostile actions. Additionally, these technologies can be used to permanently damage and destroy infrastructure. With space, the technologies begin with radio frequency (RF) jamming for reversible interference and continue to directed energy and kinetic kills vehicles with potentially permanent and irreversible effects, whereas cyber-attacks can range from theft of information of organizations' personnel or intellectual property to the sabotage of national infrastructure. This information can be used to bolster development of weapons that can be acquired much faster and without expending the vast amounts of capital for advance technologies. Additionally, the cyber threat can be used to derail a national program. An example of this was seen in Iran when Stuxnet was discovered in their uranium processing facilities. Few would argue against the fact that the advent of space and cyberspace technologies is having a profound impact in the realm of national security. Both technologies represent new opportunities for warfare outside of the traditional land, sea, and air domains for traditional military power. If any nation were to remove the remarkable advantages provided by both space and cyberspace technologies, it would imperil the conventional weapons dominance observed in both current and future conflicts. This paper will investigate the challenges seen in crafting and applying deterrence principles with regard to space and cyberspace technologies, and the potential course of action to remedy this situation.

CHAPTER ONE – DEFINING THE DOMAIN

Space Defined

In order to examine the issue of deterrence application within the space domain, it is important to define the characteristics unique to space. There are varying definitions on where space begins, but the Karman line commonly represents the boundary between the Earth's atmosphere and outer space. This occurs at 100 kilometers (or sixty-two miles) above sea level.[1] This use of a simple line does streamline the discussion, but it does not constrain the discussion to matters practical to space operations. Building on this concept, Joint Publication 3-14, *Space Operations*, provides a thorough explanation on space as a domain, and the characteristics unique to space. Unlike the domains of land, sea, and air, the space environment's unique characteristics affect not only military operations but also daily commerce. This requires policy makers to have to have a fundamental understanding of the strengths and vulnerabilities of space capabilities. However, with more countries seeing the benefits that space brings to government and commerce, space is becoming increasingly congested, contested, and competitive. While space is vast, there are only limited orbital regimes suitable for use. Furthermore, when coupling the limited orbital regimes with the finite amount of radio frequency (RF) spectrum, requires effective deconfliction for space operations. As more nations and organizations realize the benefits of space this will continue to increase the number of

[1] Dr. S. Sanz Fernández de Córdoba, "100km Altitude Boundary for Astronautics," *Fédération Aéronautique Internationale (FAI)*, accessed December 10, 2015, http://www.fai.org/icare-records/100km-altitude-boundary-for-astronautics.

satellites, and the resulting threat of space debris during a conflict will reach a tipping point potentially threating the ability to launch and operate future space missions.

Space is currently a force enabler to all other military operations, making it unique and different from the terrestrial domains. Integrated military command and control seen today is a direct result of the strengths of space technology enabling near real-time communication from the national command structure to deployed units worldwide. This unparalleled technology has gone through great lengths to shrink the world and provide voluminous data to any country willing to commit the resources to field a robust capability. Space provides not only a global perspective leading some to comment that space is the "ultimate high ground." At a high level, this perspective leverages the ability for satellites in low earth orbit to travel at great speeds to observe any point on the earth over the course of a day, or for satellites in geosynchronous orbits to maintain a persistent overwatch of a third of the Earth. Satellites traverse or watch large areas of Earth by the very nature of how they orbit, and they maintain an additional benefit of not being hindered by international laws for overflight of sovereign nations since space has no geographical borders. This creates an advantage and allows for unrestricted access to denied areas spanning the globe. This capability enables numerous mission areas such as intelligence, surveillance, and reconnaissance (ISR), communications, navigation, and weather monitoring.[2]

To further understand the benefits of satellite overflight, it is necessary to discuss some fundamental laws of physics that govern space operations discovered by Sir Isaac Newton and Johannes Kepler. The laws, Newton's laws of motion and Kepler's laws of

[2] U.S. Department of Defense, "Joint Publication 3-14 Space Operations," May 2013, G1-2, accessed December 15, 2015, http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf.

planetary motion, define how orbital motion occurs around a celestial body.[3] Physics truly makes space different from the traditional laws seen with land, sea, and air. For the most part, the laws are well understood and the changes are observable to those without specialized training and education. Space differs from this since it demands some level of understanding of orbital mechanics. This chapter will explain the fundamentals required to discuss the space domain effectively, but it will not delve deeply into the subject based on the highly technical nature of the math involved. However, it is important to build a foundational language to adequately describe the orbits, capabilities, and limitations of the satellites in use today.

The primary force driving and defining operations in space is gravity. In Low Earth Orbit (LEO), the Earth's gravitational field causes satellites to constantly fall towards Earth's center. This falling is counteracted by the extreme speeds that a spacecraft operates at. From a simplistic point of view, Earth's surface curves downward at a rate of five meters for every eight kilometers horizontally. This requires that LEO satellites cover this same area to remain in orbit, and this requires the satellite to travel at least seven point eight kilometers per second (17,500 miles per hour). As the orbits move away from basic low earth, the speeds for orbital insertion vary based on the altitude and shape of the targeted orbit. The orbital period is defined as the amount of time that a satellite takes to complete one full revolution around the occupied foci of the orbit. From a practical standpoint, orbits are fixed in space. However, they can be manipulated by external forces such as orbital perturbations or to a limited degree from onboard control systems. While the orbit is essentially fixed in space, the Earth rotates beneath the orbit

[3] Jerry Sellers, *Understanding Space, An Introduction to Astronautics*, Third Edition. (McGraw-Hill Companies, Inc., 2007), 38, 111–116.

while the orbits ground track will trace over the Earth over a variable period of time. The large amounts of angular momentum result in a large amounts of inertia to overcome. This inertia leads to a large amount of resistance to making changes to the orbital plane. Contrary to the common misconception about satellites being easy to reposition and maneuver, the very nature of the forces applied to satellites results in limited freedom of maneuver based on restricted onboard resources.[4]

As mentioned earlier, satellites are not very maneuverable based on the high amount of angular momentum that has to be countered to effect any real orbital change. Additionally, maneuvering a satellite for the purpose of changing an orbits size (altitude) or inclination costs fuel and limits the life of the satellite. Based on these limitations it is not possible for satellites to "hover" over a particular point on Earth, nor can they "bend" their planes to a specified point on the planet. A satellite's access to a point on Earth is dependent on time, i.e., time for the Earth to rotate under the satellite's orbit. This orbit rotation is based on the underlying assumption that a satellite's orbital plane must pass through the Earth's center. In addition to the onboard maneuver capability, perturbations will affect an orbit. More specifically, perturbations will alter an orbit depending on the amount of a particular force imparted. For example, atmospheric drag and solar radiation pressure can cause an orbit to decay and force the satellite operators to expend resources to maintain the orbit. The gravitational pull of the sun, moon, and other planets can alter certain types of orbits. These orbital perturbations complicate the orbital propagation and mission planning of satellites. This requires space-faring nations to have the ability to track objects and orbit and develop models. This tracking is not only essential to the

[4] U.S. Department of Defense, "Joint Publication 3-14 Space Operations," G1-2.

operational considerations of space operations, but is important for space situational awareness functions that will be described later.[5]

Describing the various orbit regimes is essential to the overall exploration into space issues. Just as satellites have limited maneuverability, there are specific orbits that utilize unique characteristics for national security and civil missions. Figure 1, shown below, illustrates the various orbit regimes that will be described in more detail throughout this chapter. This illustration details the various orbits and a general set of characteristics for each example. Specifically, the illustration contains data on orbit altitude, orbital velocity, orbital period, and an example mission that would utilize that orbit. The four orbits described in this illustration, while not all-inclusive, represent the major operational orbits in use for most satellites. As each of the orbits will be described in further detail, Figure 1 will be referenced to show the general orbital parameters.

As mentioned earlier, satellites cannot "hover" over a particular spot on the Earth, but that is essentially what geosynchronous and geostationary (GEO) satellites do. The orbital altitude of GEO satellites means they orbit around the Earth at the same rate or rotation as Earth around its axis. These satellites have an orbital period of nearly twenty-four hours, during which the satellite will move one degree along its orbit path shown in Figure 1. The reason these satellites appear to hover is that they are placed at an altitude of 42,164 kilometers from the center of the Earth's. The main benefit of GEO orbit is the ability to cover a third of the orbit with one satellite. This benefit allows for a large field of view (FOV), but this is at the cost of the potential resolution of the onboard sensors to discern small objects. The main difference between a geosynchronous and geostationary

[5] Ibid.

orbit is the geostationary orbit will have an orbit with zero inclination and eccentricity. This will keep the satellite at a fixed point on the equator over the Earth. This contrasts with the ground trace of a geosynchronous orbit which will trace out a figure eight when observed from the ground.[6]

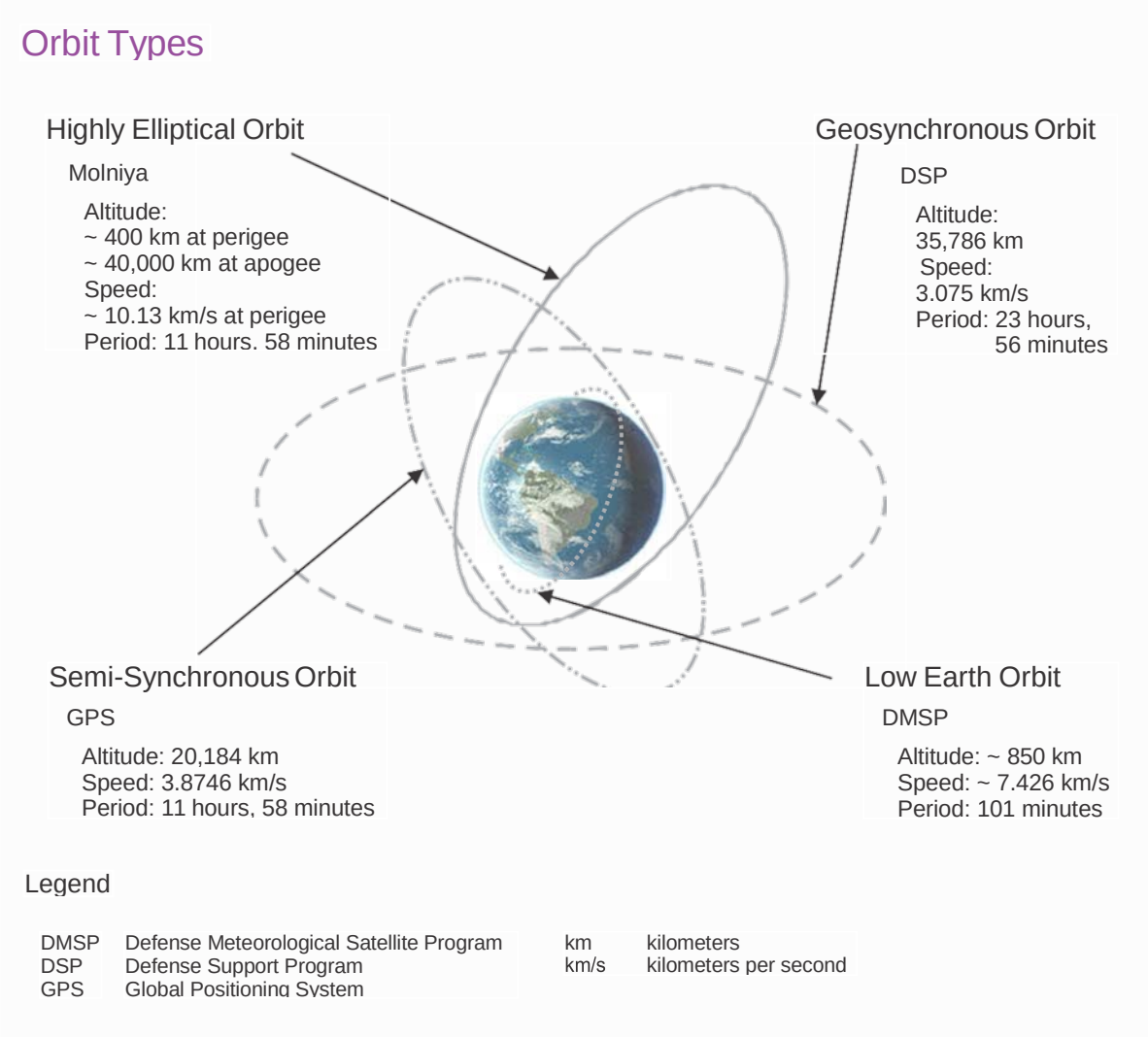

Figure 1. Types of Operational Orbits.[7]

[6] Holli Riebeek, "Catalog of Earth Satellite Orbits: Three Classes of Orbit," *NASA Earth Observatory*, last modified September 4, 2009, accessed April 10, 2016, http://earthobservatory.nasa.gov/Features/OrbitsCatalog/page2.php.
[7] U.S. Department of Defense, "Joint Publication 3-14 Space Operations," G4.

Where GEO orbits have the ability to monitor large swaths of the Earth at lower resolution, Low Earth Orbits (LEO) will sweep over the Earth at high rates of speed with sophisticated sensors capable of high-resolution data collection. An example of this is seen in Figure 1 where it describes the Defense Meteorological Satellite Program (DMSP). While there is no formalized definition of what comprises a LEO orbit, these orbits usually will not measure more than 1,000 kilometers from the farthest point of its orbit (apogee) to the center of the earth. The relative speeds that are observed in LEO approach seven kilometers a second (roughly 24,600 kilometers an hour) with an orbital period of approximately 100 minutes. Additionally, the amount of atmospheric density has a dramatic impact to the operational life of the satellite. Missions in LEO can be maintained as long as there are no hardware failures, and as long as there is sufficient propellant to continue operations. Propellant is typically the single largest life-limiting item of a LEO satellite. The LEO regime is unique in space operations as the only area where both manned objects, like the International Space Station, and unmanned satellites coexist. However, this is typically lower than 500 kilometers to reduce the need for radiation shielding from the Van Allen radiation belt.[8]

The Van Allen radiation belt exists between layers of the Earth's magnetosphere. This belt is comprised of trapped concentrated charged particles that have escaped those outer layers. This radiation is a concern in satellite design, as well as manned spaceflight missions.[9] These low-earth satellites have the benefit of leveraging lower power transmitters and sensors, but this comes at the cost of reduced time over a target of interest or satellite ground station (access time). This feature necessitates the need to

[8] Ibid., G6.
[9] Sellers, *Understanding Space, An Introduction to Astronautics*, 87–90.

maintain constellations of multiple satellites that are spaced (commonly referred to as orbit phasing) around the orbit to maintain optimum or continuous coverage.

While satellites in both LEO and GEO orbits are the ones that commonly come to mind, there are a couple of other orbits that are germane to the discussion in this paper. Specifically, the Highly Elliptical Orbit (HEO) and Medium Earth Orbit (MEO) are used for various purposes for either northern latitude coverage or positioning, navigation, and timing (PNT) which is better known as the Global Positioning System (GPS). MEO, like other orbits, do not have a formal definition. MEO orbits are near circular, and are also referred to as semi-synchronous and will have an orbital altitude around 20,200 kilometers.[10] However, they will orbit the Earth twice daily with a twelve-hour period and when used with GPS will have an orbital inclination of fifty-five degrees.[11] Both of these orbit types are shown earlier in Figure 1 for reference when compared with both LEO and GEO orbits.

HEO orbits, as the name implies, are a highly elliptical orbit. This varies from the orbits discussed earlier, which are primarily near circular and are described in Figure 1. What makes HEO orbits unique is the difference in apogee and perigee orbit will be quite vast. At HEO orbit's most distant point, the orbit stretch to greater than 40,000 kilometers. The time it takes for the HEO orbit to pass through its furthest point gives these orbits a significant hang time over the poles and can appear to "hover" for a period of time. While there are numerous types of HEO orbits, the most well-known is the Molniya orbit. The word Molniya is Russian for "lightning." The Molniya orbit is inclined at 63.4 degrees, and this will provide for extended communications and ISR

[10] Riebeek, "Catalog of Earth Satellite Orbits."
[11] Sellers, *Understanding Space, An Introduction to Astronautics*, 164.

coverage over high latitude. An example of a Molniya orbit can be seen in Figure 2. Satellites in these orbits are used for providing communications and servicing areas that include Russia, the Nordic countries, and Canada. The specific inclination is used to minimize the propellant expenditure to maintain the Molniya orbit based on the fact that the orbit's perigee will not rotate around the Earth. This allows the orbit's perigee to be maintained in the Southern hemisphere, and ensures the maximum dwell of eleven of the twelve hours in the Northern hemisphere shown in the figure below.[12]

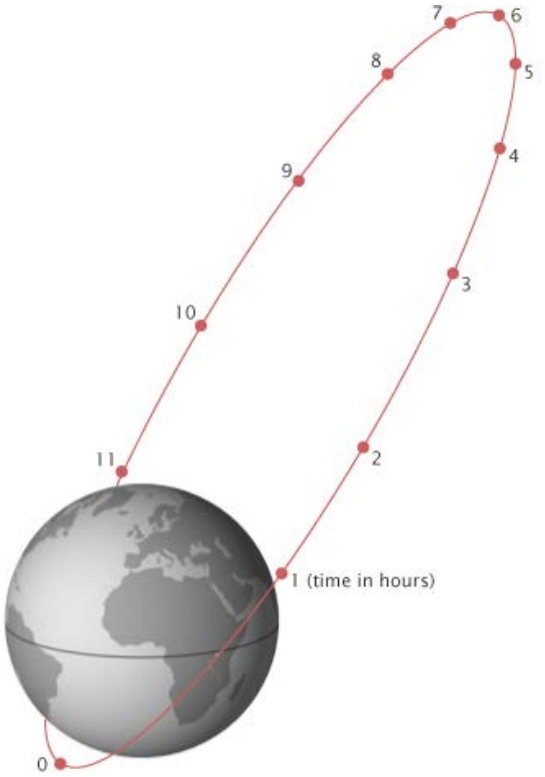

Figure 2. Molniya Orbit.[13]

[12] Ibid., 276.
[13] Riebeek, "Catalog of Earth Satellite Orbits."

Space Operational Considerations

A secondary consideration for any domain is the specific operational planning considerations to employ the technology effectively. A concern to both policy and decision makers is that no asset is ever in the right place at the right time to answer a critical question. Whereas most people, including policy makers, have enough familiarization with sensors hosted on either aircraft or unmanned aircraft systems (UAS) to expect that a near immediate re-tasking is often available for a new high interest event. Unlike airborne systems that retain the capability to maintain a near persistent overwatch of an area of interest, the nature of orbital mechanics necessitates some level of familiarization with how satellites move through space for an individual to understand that a satellite cannot simply reorient or reposition to answer an immediate question.

That leads to the important consideration of satellite revisit rates. These revisit rates refer to the period elapsed between orbits of a given satellite over the same point on the Earth. These rates are highly dependent on the orbit's geometry and orbital period. Typically, the higher an orbit's altitude, the longer it will take a satellite to revisit that point target. The rotation of the Earth factors into this revisit time as it continues to rotate, and the successive satellite pass will be east of the previous ground track. As noted earlier, the altitude is a major component of revisit rate. LEO satellites will maintain revisit rates ranging from ninety minutes to a few hours. Alternatively, you can contrast this with GEO satellites that do not have a true revisit rate. GEO satellites will constantly maintain line of sight (LOS) with the geographic areas under their FOV.[14] Once you understand the revisit rate, the satellite ground track can be modeled to aid in

[14] U.S. Department of Defense, "Joint Publication 3-14 Space Operations," G7.

planning of other portions of the satellite's orbit. The ground track shows the satellite's position with regard to a predicted tack on the Earth. This is easier for most people to visualize instead of the classical orbital elements used in most satellite operations. [15] Either the propagated orbit or the derived ground track will be used to calculate and display satellite access windows. These windows in time are when a given satellite will be able to maintain LOS with a point of interest on the ground. This can be the satellite's ground station for receiving command and tasking to that of ground targets for the onboard sensors to capture. The lower a satellites orbit, the smaller the sensor FOV will be. Typically, a LEO satellite will have access with a particular point on the ground for around ten to fifteen minutes. For better or worse, a satellite's orbit is defined by physics and can be predicted. This is an important factor to note for both planning of day-to-day operations as well as offensive and defensive missions. It is not uncommon for operations to be planned around other nations ISR satellites' access times to maintain some level of deception for ongoing operations. The same can be said of other nations with competing interests with the United States.[16]

The next consideration is important for multiple reasons that will be described later in the paper with regard to the specific application of counterspace platforms. From the standpoint of data, the most important factor is how current the information is on a given satellite. This factor influences every facet of satellite operations, from tracking of all objects in space to the propagation of the data to support tasking for sensor use. As noted earlier, the altitude is one of the largest factors determining the length of the accuracy of a given set of satellite tracks. The lower a satellites altitude, the shorter the

[15] Sellers, *Understanding Space, An Introduction to Astronautics*, 179–184.
[16] U.S. Department of Defense, "Joint Publication 3-14 Space Operations," G7.

period that the data will be within tolerances. Additionally, orbital perturbations mentioned earlier in the chapter will continue to degrade orbital predictions. In addition to data accuracy, there is the presence of Electromagnetic Interference (EMI) or Radio Frequency Interference (RFI). The limiting factor with space derives from the fact that the very use of satellite requires some level of Electro Magnetic Spectrum (EMS) and without Radio Frequency (RF), these capabilities enable ISR, communications, and navigation missions. Space-based assets use RF as their only means of transmitting and receiving data, and once the frequency bands have been built into a satellite they cannot be changed after launch. Consequently, every space mission is subject to some level of EMI, naturally occurring or man-made, and there is often some level of satellite design to mitigate the impacts of the phenomenon. Natural EMI is generated by the Earth's ionosphere, a region of the atmosphere comprised of ionized gases that create noise in the EMS, and is typically not uniform. Additionally, the sun generates electromagnetic energy and that also will react with the Earth's magnetic fields that will strengthen or weaken based on various environmental factors that can be observed both locally and globally. Generally, the environmental EMI can be predicted and mitigated through power management and reducing operations during peak EMI periods. Man-made EMI, or in this case RFI, is usually attributed to another user broadcasting on the same frequency and this is analogous to friendly jamming. However, RFI can be a result of hostile jamming with the intent of degrading the satellite or services that it provides to the end user. This topic will be explored more deeply in subsequent chapters.[17]

[17] Ibid., G7-8.

A separate set of operational environmental concerns deal with some uniquely challenging factors for space – space weather and space debris. Earlier in the chapter, there was some basic description of the Van Allen radiations belts, and satellites operating in those environments can encounter additional radiation. This is further complicated by space weather, which is primarily generated by the sun. Space weather often manifests itself with charged particles, ionospheric interference, like scintillation, solar flares, and cosmic rays. These weather phenomena will have varied effects depending on the particular satellite design and payload. These impacts can range from minor RF degradation to potential onboard electronics failure.[18]

If the complexities of space were not already enough, there is the constant threat of orbital debris. Unfortunately, there is not a mechanism to remove old or defunct space objects from orbit. The complexity and cost of this has so far kept this capability out of reach of the industrial world. An additional consideration on the technology required to remove orbital debris is the very same technology that would be employed for rendezvous and proximity operations (RPO) that would facilitate co-orbital anti-satellite weapons. This debris can be left from rocket bodies used to place satellites on orbit, on orbit explosions, collisions, or micrometeorites. An additional threat of debris is compounded by the extremely small nature of some debris and the inability of systems to track it. As debris occurs, it tends to initially remain in the same orbit as the object it was generated from until some level of force changes that orbit. This leads to the long term process debris dispersal, where debris make take weeks or months, to separate from the source in an operational orbit.

[18] Sellers, *Understanding Space, An Introduction to Astronautics*, 73–89.

Furthermore, the altitude of the debris influences the amount of time it can be a threat. If an object were to break up at a higher altitude, it could take hundreds of years before gravity pulls that object into the atmosphere to where it will burn in. Recent orbital events have left debris clouds in orbits that have taken years to fall into lower portions of space leading to numerous collision avoidance activities by space system owners and operators. In some cases, debris events can lead to collisional cascading of debris that ultimately can destroy other objects in space. Since 2007, this problem has taken on a new sense of urgency with the Chinese anti-satellite test, and the collision of the Cosmos and Iridium satellites in 2009. At the time of the Department of Defense (DoD) Joint Publication on Space Operations, there were approximately 800 active satellites in the satellite catalog (SATCAT). Additionally, the United States Air Force (USAF) tracks more than 21,000 other objects larger than ten centimeters. However, there are over 300,000 items of untracked debris between one and ten centimeters in size that remain a threat to space operations now and well into the future that could lead to a runaway chain of events that leads something known as the Kessler Syndrome, where collision after collision leads to an operational orbit being unusable for centuries.

Figure 3 illustrates the growing trend of objects in space since the initial launch of Sputnik. Additionally, this figure shows the marked increase in orbital objects through 2013. Although this illustration only runs through 2013, is shows the major increase in total objects in space to include two of the more notable incidents of the Chinese anti-satellite weapons test and the collision of an Iridium communications satellite with a defunct Russian communications satellite. Those two incidents alone accounted for an increase of greater than seventy-five percent of orbital debris. If nations were to engage

in full-scale anti-satellite warfare, the increased debris trends seen from 2007-2009 would pale in comparison. This ultimately could make low earth orbit unusable for years and imperil any and all nations future space missions.

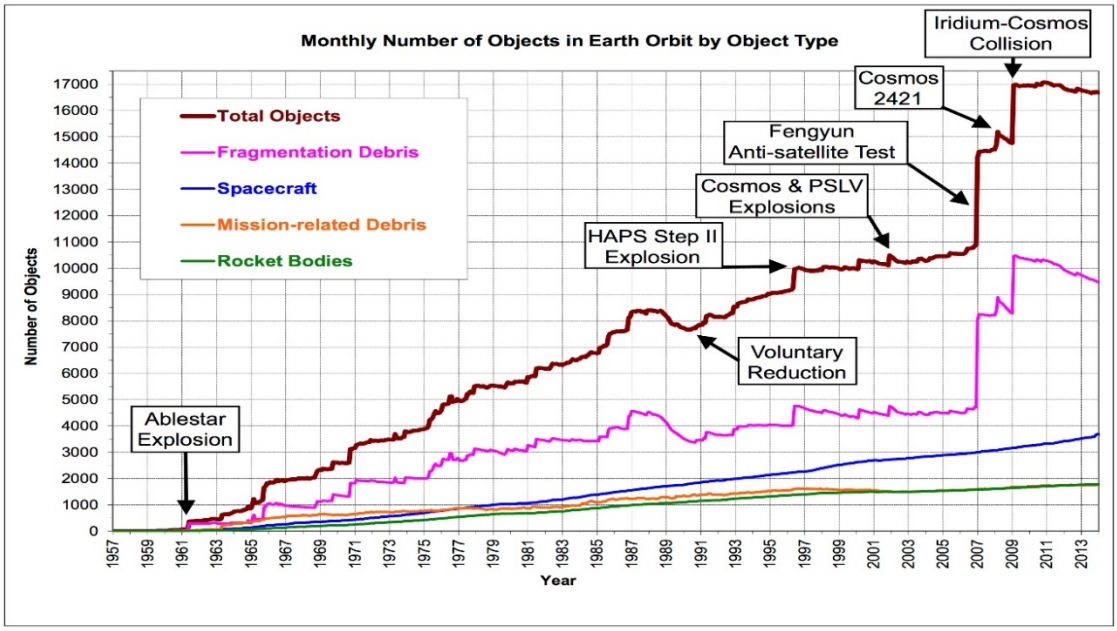

Figure 3. Number of Objects in Earth Orbit by Type.[19]

As with all platforms, one satellite is never enough, and there is no satellite in existence that can support every application. Although there are some constellations of satellites, like GPS, which are comprised of multiple satellites that are designed in similar blocks, most satellites are custom built for a given application. In the case of GPS, the constellation requires a robust constellation to ensure that a user anywhere on Earth with a GPS receiver can track a minimum of four satellites to get an accurate three-dimensional fix on their position. Additionally, ISR constellations will likely be optimized over several altitudes and inclinations to provide the right mix of access times

[19] Mika McKinnon, "A History of Garbage in Space," *Earth & Space*, accessed January 17, 2016, http://space.gizmodo.com/a-history-of-garbage-in-space-1572783046.

and revisit rates to meet the needs of the satellite operators. In addition to the limits on the number of satellites, the final unique consideration for space is the lack of on-orbit serviceability. Satellites are one of the few technologies that you have to ensure they are as close to perfect as possible prior to launch. Because once the satellite is in space, there is virtually no way to fix any hardware issues. A satellite can be designed for robust operations with multiple components and strings of equipment to swap as failures occur, but you cannot replace a bad component with a spare. In some cases, the software can be updated from the ground in a time-consuming and somewhat risky process. This results in limited capabilities when compared to typical terrestrial systems. This lack of serviceability results in tighter constraints being maintained on all satellites, and the mission area requires that each resource by carefully managed to ensure a full and useful design life.[20]

Cyberspace Defined

Like the space domain, cyberspace exists in multiple territories and jurisdictions and that distributed environment leads to complexities for policy makers. Although space is a very important aspect of day-to-day life, there are aspects of life that do not rely on space technology. However, the same is not true with regard to cyberspace technologies. Nearly every facet of everyday life has some component that is reliant on cyberspace. The technology utilized in the cyber domain is vast and often taken for granted. Furthermore, some very specific factors have wide-ranging impacts on national security. Joint Publication 3-12R, *Cyberspace Operations*, defines the cyberspace

[20] U.S. Department of Defense, "Joint Publication 3-14 Space Operations," G6-8.

domain as, “the global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”[21] From a policy standpoint, cyberspace is problematic as it reaches across both geographic and geopolitical borders. Additionally, most of cyberspace is outside of U.S. control and is integrated into critical infrastructure. Cyberspace is also critical to the daily conducting of commerce, governance, and national security. Conversely, the same access to the Internet provides adversaries of the U.S. the ability to compromise the integrity of critical infrastructure and conduct vast cyber espionage campaigns with large impacts of future technologies. This leads to what the authors of Joint Publication 3-12R call the paradox within cyberspace, “the prosperity and security of our nation have been significantly enhanced by our use of cyberspace, yet these same developments have led to increased vulnerabilities and a critical dependence on cyberspace.”[22]

To be more specific, cyberspace is a global domain that relies on an interdependent network of information technology (IT) infrastructure. This infrastructure includes the Internet, telecommunications networks, computer systems, processors, and controllers to manage the data flowing across these networks. Cyberspace Operations (CO) rely on these links and nodes that reside in the physical domains to perform functions in both the physical and cyberspace domains. Cyberspace Operations enable freedom of action for activities in the other domains while utilizing the EMS and physical

[21] U.S. Department of Defense, “Joint Publication 3-12(R) Cyberspace Operations,” n.d., I1, accessed December 16, 2015, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.
[22] Ibid.

infrastructure that each of the other four domains maintains for operational support. Additionally, the relationship between space and cyberspace is very close and space operations are not possible without the infrastructure provided by networks. To the same degree worldwide cyber operations are not possible without the global reach of space technology. Cyberspace is made up of many different and overlapping networks and nodes. These nodes, are devices or logical locations that support an internet protocol (IP) address or identifier. These nodes use routing tables to navigate the layers of cyberspace that will be described in more detail in the next few paragraphs. It is important to note that not all networks are connected or accessible from any other network. From a design standpoint, many networks are supposed to be isolated to prevent any cross talk and to afford some level of security from outside threats. Networks will utilize access controls, encryption, and physical separation to maintain security and data integrity.[23]

Cyberspace Operations can be described as occurring in the terms of three layers and those are the physical network, the logical network, and the cyber-persona shown in Figure 4. The first of these layers is the physical network layer. This layer, shown in the leftmost illustration of Figure 4, is comprised of the geographic component and the physical network hardware where all the data travel. The geographic component is located in the land, air, sea, or space domains where the data are transmitted near the speed of light. This portion of the layer is where the sovereignty issuers are tied to those physical domains. Whereas the physical network component consists of all the hardware, software, and infrastructure (to include the potential RF links) that supports the network and physical connections. The hardware also utilizes logical constructs as the primary

[23] Ibid., I1-2.

method of securing the network. This portion is the primary target for signals intelligence (SIGINT), computer network exploitation (CNE), measurement and signature intelligence (MASINT), open source intelligence (OSINT), and human intelligence (HUMINT). This is the first point of reference for jurisdiction with applicable authorities. Additionally, this layer is the layer that can be exploited by geospatial intelligence (GEOINT) which contributes targeting data for cyberspace operations.[24]

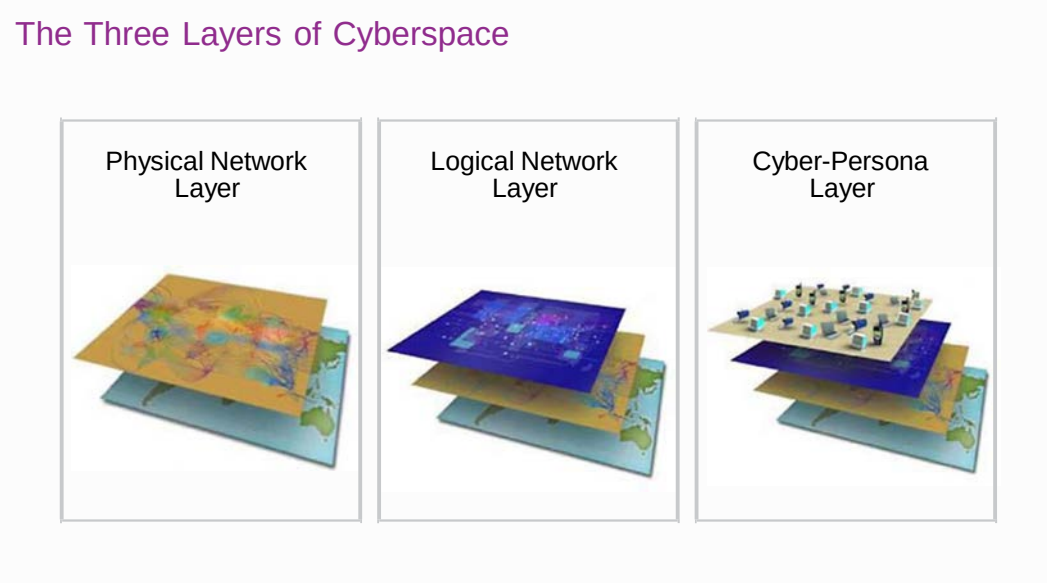

Figure 4. The Three Layers of Cyberspace.[25]

Seen in the second illustration contained in Figure 4, the next layer is described as the logical network layer. This layer consists of the elements of the network that are related to the infrastructure on the physical network layer. This layer is rather abstract when compared to the physical layer. Most people can envision hardware that has been

[24] Ibid., I2-4.
[25] Ibid., I3.

connected to a network, but the logical layer comprises the relationships between the hardware and the connections between various portions of the networks that are not tied to any specific path or network nodes. An example of this is seen anytime an individual uses a web browser to connect to a website. The user does not state how the browser will connect to the various servers between the physical terminal they are sitting at and the server hosting the website at potentially any location in the world.[26]

The final layer shown in Figure 4 is known as the cyber-persona layer. This layer is more abstract than the logical layer described previously. This layer represents the digital persona of a user, or actor, in cyberspace, which consists of the actual individuals on then network. This portion of the cyber domains utilizes the rules applied in the logical network layer for individuals to operate in cyberspace. These cyber-personas can relate to an actual individual or entity; it may incorporate some biographical or corporate data, e-mail and IP addresses, and potentially web pages, and phone numbers. Where this gets complicated, an individual may maintain more than one cyber-persona which may be a representation of the individual. Conversely, a single cyber-persona could have multiple users. This leads to one of the more complex issues with cyberspace. It can be difficult to attribute any actions or responsibility to a particular cyber-persona to the actual group or individual running cyber operations. This cyber-persona's trail may be in multiple virtual locations that are not necessarily linked to a physical location. Networks are globally interconnected, and enable vast amounts of information to be shared between individuals, corporations, and governments.[27]

[26] Ibid., I2-4.
[27] Ibid.

The White House's International Strategy for Cyberspace sums up the importance of cyber space, and lays down some foundational goals to the development of norms for operating in cyberspace. The U.S. strategy declares, "Activities undertaken in cyberspace have consequences for our lives in physical space, and we must work towards building the rule of law, to prevent the risks of logging on from outweighing its benefits."[28] While the internet was developed to aid in collaboration and information sharing, the ability for criminals and state actors to exploit this ability has become a very real cause for concern in the last couple of decades. These threats range from extortion, fraud, and identity theft affecting individual users to concerted efforts to steal intellectual property reducing national competitiveness and innovation. Cyberspace has a unique set of impacts that transcend national borders, and can endanger peace and security if cyber-attacks affect national interests.[29]

The U.S. will operate and defend cyberspace while operating within defined core principles of maintaining fundamental freedoms, privacy, and the free flow of information. The U.S. is committed to the freedom of expression, but not at the expense of public safety and protection of citizens. This is further defined by the incitement of imminent violence, exploitation of children, and organizing terrorist activities not consistent with the rule of law. Additionally, privacy is of paramount importance in cyberspace. The nature of personal data and information requires safekeeping to ensure protection of the individual and the national interests. However, the need for privacy must balance with the ability of law enforcement agencies to investigate and prosecute

[28] The White House, "International Strategy For Cyberspace - Prosperity, Security, and Openness in a Networked World," May 2011, 3, accessed March 30, 2014, https://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf.
[29] Ibid., 4.

those who would misuse information or cyberspace for illicit or violent means. The free flow of information should not be a choice between information and security of the network. National-level filters and firewalls provide an illusion of security, but can dampen growth. Cyberspace is a means of collaboration for individuals, business, and nations alike. The importance of a common access to prevent unfair advantages cannot be understated. The continued technological growth of the twenty-first century requires that cyberspace provides a means for the prosperity of all users.[30]

Chapter one established the foundational language required to discuss operations in both the space and cyberspace domains. It illustrated not only the orbits, but also the unique operational considerations that are required when considering any sort of operation in space. Additionally, the examination of the details that delineate various portions of cyber infrastructure shows areas of connection that may have been overlooked in this exploration of the threat environment. This foundational information is key in the continued exploration of the topic of space and cyberspace threats in the upcoming chapters.

[30] Ibid., 5.

CHAPTER TWO – DEFINING THE THREAT

Both space and cyberspace technologies have become force multipliers for military operations. The difficulty of attributing attacks to space and cyberspace assets hinder the ability to apply deterrence effectively. The continued United States reliance on these technologies makes them an attractive target to both emerging and regional powers. Although these technologies are separate from a policy perspective, both space and cyberspace technologies coexist in their operational employment. Applying deterrence theory in the space and cyberspace domains is not as straightforward as seen previously with nuclear weapons. Cyber technology in particular has become a nearly every day event in the defense and security world. Additionally, there is significant overlap in the technologies associated with both of these domains. For each satellite ground station, numerous computer networks are vulnerable to cyber-attack. It is challenging to find a number to characterize the threat to systems based on space weapons and cyber-attacks. There are very clear and documented trends showing an uptick in activity from the 2007 Chinese anti-satellite (ASAT) weapons test, and a parallel trend in the number of reported cyber incidents as the threat becomes more pervasive.

A 2010 RAND Corporation report supporting Project Air Force used the term "Targets of Growing Attractiveness." This term describes the conditions of space use we see in support of combat operations today. The 1991 Gulf War, opened the eyes of leaders in countries around the world to the level of conventional weapons dominance afforded by a deep investment in space technology. Real-time communications;

intelligence, surveillance, and reconnaissance (ISR) satellites; and positioning, navigation, and timing (PNT) coupled with advanced conventional weapons transformed the U.S. military to a formidable fighting force. This reliance on space by the U.S. makes our space assets valuable resource for targeting. For a country to remove this advantage, it would neutralize our conventional weapons advantage in future conflicts.[31]

This report argues the "infrastructure, policies, and attitudes that both enable and constrain U.S. space operations in the current environment are, in many ways, unchanged from when they were developed during the Cold War. This leaves the United States exposed to the risk of a surprise attack in space unless a deterrence regime can be developed to restore first-strike stability in that domain." This demonstrates the dichotomy in the conventional deterrence thinking of the cold war, and shows the limitations of current systems in this arena.[32]

During an interview conducted for the 60 Minutes segment "The Battle Above," David Martin conducted an interview of General John Hyten, the commander of Air Force Space Command (AFSPC). This segment illustrates the fundamental change in approach from the nuclear world to that of space operations. Journalist David Martin, states in the interview, "Deterrence in the nuclear world was built on weapons."[33] Highlighting the change, General Hyten responds with, "[Deterrence] in the space world has got to be built on a little bit different construct. It's the ability to convince an adversary that if they attack us, they will fail."[34] General Hyten's testimony to House

---

[31] Forrest Morgan, "Deterrence and First-Strike Stability in Space: A Preliminary Assessment" (RAND Corporation, 2010), 13, accessed March 18, 2015, http://www.rand.org/content/dam/rand/pubs/monographs/2010/RAND_MG916.pdf.
[32] Ibid., 16.
[33] David Martin, "The Battle Above," *60 Minutes*, last modified April 26, 2015, accessed April 27, 2015, http://www.cbsnews.com/news/rare-look-at-space-command-satellite-defense-60-minutes/.
[34] Ibid.

Armed Services Committee on the National Security Space Budget for Fiscal Year (FY) 17 provides a few more details on this earlier statement. He noted that, "Not all space faring countries are friendly to the United States or agree to establish and observe international norms in the space domain. Adversaries are developing kinetic, directed-energy and cyber tools to deny, degrade and destroy our space capabilities. They understand our reliance on space, and they understand the competitive advantage we derive from space. The need for vigilance has never been greater."[35]

One of the key initiatives to further the space deterrence posture was the creation of the Joint Interagency Space Operations Center (JICSpOC) initiative. This organization will be located at Schriever AFB, CO, and will facilitate information sharing across the national security space enterprise. The organization has begun operational experimentation and is planning to incorporate any results into standard operating procedures on January 1, 2017.[36] According to General Hyten, "The JICSpOC is focused on space defense, and is developing new space-system operational concepts, and tactics, techniques and procedures in support of both the DoD and Intelligence Community. Fusing the operations of our space systems and intelligence capabilities in real-time will enhance our ability to track, monitor, analyze and predict irresponsible and dangerous activity in space." The JICSpOC was designed to enhance the nation's deterrent posture by demonstrating that the U.S. is prepared to respond should an adversary attempt to

[35] General John Hyten, *National Security Space Budget for FY17: Presentation to the Subcommittee on Strategic Forces of the House Armed Services Committee* (U.S. House of Representatives: U.S. Government Printing Office, 2016), sec. Subcommittee on Strategic Forces of the House Armed Services Committee 11-14, accessed March 16, 2016, http://docs.house.gov/meetings/AS/AS29/20160315/104620/HHRG-114-AS29-Bio-HytenJ-20160315.pdf.
[36] U.S. Department of Defense, "New Joint Interagency Combined Space Operations Center to Be Establish," *U.S. Department of Defense*, last modified September 11, 2015, accessed April 2, 2016, http://www.defense.gov/News/News-Releases/News-Release-View/Article/616969/new-joint-interagency-combined-space-operations-center-to-be-established.

threaten our space capabilities.[37] The initial testing of the JICSpOC initiative has completed two scenarios as of January 22, 2016, and has generated several lessons learned during the process. These two scenarios have begun to look at the problem of characterizing and attributing threats to satellites. Over the years, space leaders have had difficulty determining whether an outage on a satellite is naturally occurring or the result of an attack. The initial testing is working through establishing the various sources of data for decision makers. This will allow each event to be looked at in a consistent and holistic manner and develop options.[38] Although this organization is in its infancy, the benefit of synthesizing data for policy makers to make the right decisions in a time of crisis is or paramount importance.

While General Hyten's comments were informative on the future of space deterrence, it is necessary to investigate the policy statements in the 2010 National Space Policy. This policy states, "The United States will employ a variety of measures to help assure the use of space for all responsible parties, and, consistent with the inherent right of self-defense, deter others from interference and attack, defend our space systems and contribute to the defense of allied space systems, and, if deterrence fails, defeat efforts to attack them."[39]

The U.S. aims to increase stability in space through the development of both domestic and international measures to promote safe and responsible operations in space.

---

[37] Hyten, *National Security Space Budget for FY17: Presentation to the Subcommittee on Strategic Forces of the House Armed Services Committee*, sec. Subcommittee on Strategic Forces of the House Armed Services Committee 12.
[38] Colin Clark, "Two Scenarios Tested: STRATCOM's Haney On JICSPOC Lessons," *Breaking Defense*, last modified January 22, 2016, accessed April 2, 2016, http://breakingdefense.com/2016/01/two-scenarios-tested-stratcoms-haney-on-jicpsoc-lessons/.
[39] The White House, "National Space Policy of the United States of America," June 28, 2010, 3, accessed August 10, 2015, https://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf.

This will be enabled by improved information collection and sharing for collision avoidance to prevent any growth in space debris as well as strengthening measures to mitigate debris. As mentioned in chapter one, space debris is a large threat to space operations, and every effort to reduce this threat should be pursued by all parties involved in space. Additionally, this policy begins to establish the framework for protection of space systems and infrastructures and the interdependence between space and information systems.[40]

Additionally, this policy requires not only the assurance of space systems, but their resiliency as well. Chapter three will describe the various threats to space systems, and the development of resilient space systems is a means to reduce the overall vulnerability of on-orbit space assets. Specifically, the National Space Policy aims to provide guidance to developers and operators of space systems to develop infrastructure that is protected against, disruption, degradation, and destruction from environmental, design, or hostile causes.[41]

The space policy is mirrored by the most recent DoD Cyber Policy stating, "As DoD builds its Cyber Mission Force and overall capabilities, DoD assumes that the deterrence of cyberattacks on U.S. interests will not be achieved through the articulation of cyber policies alone, but through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, capabilities, and the overall resiliency of U.S. networks and

[40] Ibid., 4.
[41] Ibid.

systems."[42] The key difference shown is in the cyber policy's approach to use a totality of actions.[43]

The most prevalent example of deterrence application in space can be observed with the buildup of Chinese counterspace activities, and to a lesser extent Russia. James Clapper, Director of National Intelligence, submitted a report highlighting that both Russia and China are continuing to pursue weapon systems capable of attacking on-orbit satellites.[44] China is developing a full spectrum of counterspace capabilities to include both ground-based and exoatmospheric weapons.[45] "Beijing appears to be developing this array of capabilities to deter U.S. strikes against China's expanding satellite infrastructure; challenge U.S. information superiority in a conflict; and deny, degrade, disrupt, disable, or destroy U.S. satellites if necessary." China has demonstrated the capabilities to threaten every orbit regime from low earth orbit (LEO) to medium earth orbit (MEO) and geosynchronous earth orbit (GEO) with a series of tests in 2007 and 2013 respectively.[46]

In addition to the technological development, China is developing a space deterrence doctrine that reflects how they view the space environment. Like the United

---

[42] U.S. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011, accessed March 27, 2014, http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.
[43] Ibid.
[44] James R. Clapper, *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee* (U.S. Senate: Office of the Director of National Intelligence, 2016), sec. Senate Armed Services Committee 9-10, accessed April 3, 2016, http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.
[45] Kevin Pollpeter et al., "China Dream Space Dream_Report.pdf," *U.S. - China Economic and Security Review Commission*, 86, last modified March 2, 2015, accessed March 17, 2015, http://www.uscc.gov/sites/default/files/Research/China%20Dream%20Space%20Dream_Report.pdf.
[46] Craig Murray, "China Missile Launch May Have Tested Part of a New Anti-Satellite Capability_05.22.13.pdf," *U.S. - China Economic and Security Review Commission*, last modified May 22, 2013, accessed April 17, 2015, http://www.uscc.gov/sites/default/files/Research/China%20Missile%20Launch%20May%20Have%20Tested%20Part%20of%20a%20New%20Anti-Satellite%20Capability_05.22.13.pdf.

States, China views satellites and space technology as essential to military operations. Chinese military theorists also understand the competition between ASAT development and the need for satellite defense (or resiliency in U.S. terms). Writers of Chinese doctrine write, "[T]hat to be prepared for space conflicts, besides having the ability to strike the enemy's satellites, it is also necessary to improve the survivability of one's own satellites."[47] This statement shows striking parallels between Beijing and U.S. development of doctrine. Both countries are going down similar paths to ensure the availability of space systems during times of conflict. This includes resistance to jamming, satellite mobility, enhanced space situational awareness, and disaggregation.[48] Similar to the U.S., China recognizes that protection of ground stations is just as essential as protecting the satellite. Moreover, the technical approaches used by each country are very similar. The need to maintain encrypted links and anti-jamming technologies, as well as minimizing the computer network threat is very important to ensure "the secrecy, validity, and integrity of one's own information system."[49]

Chinese statements place the importance of space deterrence on par with nuclear, conventional, and information deterrence. Although space deterrence is seen as important, it is also still under development in contemporary Chinese thinking. This deterrence theory is being developed along the lines of "People's War of Deterrence," but as with any fledgling technology there is much work to be done. Bao Shixiu, Professor of Military Affairs and Senior Research Fellow at the PLA Academy of Military

[47] Michael Chase, "Defense and Deterrence in China's Military Space Strategy," *The Jamestown Foundation*, last modified March 25, 2011, accessed March 16, 2015, http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews[tt_news]=37699.
[48] Ibid.; Martin, "The Battle Above."
[49] Chase, "Defense and Deterrence in China's Military Space Strategy."

Sciences, posits that the overall deterrence theory will evolve along the overall "active defense" scenario already employed by the PLA. Professor Shixiu writes that, "The basic necessity to preserve stability through the development of deterrent forces as propounded by Mao and Deng remains valid in the context of space."[50]

The deterrence theories put forward by Mao and Deng generally resemble the method of deterrence used during the Cold War by the United States and Soviet Union. Building on this deterrence paradigm, Chinese writers show the need for three conditions to be met for strategic deterrence to be viable. The country must possess a deterrent capability, the country must be willing to use that deterrent, and the country must be able to communicate those capabilities and the determination to use them against an adversary as deemed necessary. However, this is where the similarities to the legacy of nuclear weapons end. According Professor Shixiu, this primary difference is based on, "a taboo on the use of space weapons, the threshold of their use will be lower than that of nuclear weapons because of their conventional characteristics. Space debris may threaten the space assets of other 'third party' countries, but the level of destruction, especially in terms of human life, could be far less than nuclear weapons or potentially even conventional weapons."[51]

This developed method of deterrence developed by the Chinese suggests, "an active defense will entail a robust deterrent force that has the ability to inflict unacceptable damage on an adversary."[52] In addition to this approach, Chinese authors recognize the value of disaggregation of space systems and their associated information

[50] Ibid.
[51] Ibid.
[52] Ibid.

systems. Disaggregation is the means of dispersing missions and payloads on multiple satellite buses to complicate targeting by other nations. By hosting these various payloads on foreign satellites, it poses political and diplomatic challenges to their attack. This requires factoring the impacts of engaging a satellite owned by another country or commercial consortia. Utilizing third-party satellite operators to provide leased transponder space for communications resiliency complicates the intelligence picture required to employ a retaliatory systems against the targeted satellite. In this case, it would likely require using a system that had reversible effects to meet the goals of the attacking country without potentially damaging a leased system of a non-belligerent country. Additionally, the desire to deny the adversaries' use of their own space systems during a conflict leads into the existing nuclear deterrence strategy of China. Beijing's view on the denial of missile warning satellite capabilities to preserve their nuclear deterrent is different from approaches used by the United States.

During the Cold War, missile-warning systems are sacrosanct, and engaging one of those systems would be interpreted as a precursor to an attack. It remains to be seen if China will develop the same view. Professor Shixiu writes that China, "will develop anti-satellite and space weapons capable of effectively taking out an enemy's space system, in order to constitute a reliable and credible defense strategy." And he further states, "under the conditions of American strategic dominance in space, reliable deterrents in space will decrease the possibility of the United States attacking Chinese space assets."[53] The approach utilized by the U.S. would likely be similar, but there are

[53] Ibid.

no official American policy statements to overtly support to what degree of deterrence strategy would be employed.

The interesting approach to the evolving Chinese strategy on deterrence is the lack of conversation on the ramifications of the employment of anti-satellite weapons with regard to space debris. Even in a limited engagement, it is conceivable the amount of debris generated could limit the use of an orbital regime for any space-faring nation. Not only is this a consideration for military payloads, but civil space and manned spaceflight would ultimately suffer. This disconnect could be similar to the 2007 ASAT test where the PLA conducted the test without civilian leadership knowledge. Since that test, there are indications that debris planning has factored into future tests like the 2013 ASAT test.[54]

An illustration of the challenges in applying deterrence to space and specifically cyberspace are seen in the Department of Defense's Cyber Strategy. This policy states that, "Deterrence is partially a function of perception. It works by convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United States, and by decreasing the likelihood that a potential adversary's attack will succeed. The United States must be able to declare or display effective response capabilities to deter an adversary from initiating an attack; develop effective defensive capabilities to deny a potential attack from succeeding; and strengthen the overall resilience of U.S. systems to withstand a potential attack if it penetrates the United States' defenses. In addition, the United States requires strong intelligence, forensics, and indications and

[54] Pollpeter et al., "China Dream Space Dream_Report.pdf," 87–88.

warning capabilities to reduce anonymity in cyberspace and increase confidence in attribution."[55]

This policy shows several key points that will challenge the deterrence value of the United States in these domains. Specifically, the U.S. will need to convince a potential adversary that this attack will result in unacceptable cost. This task will be difficult enough against another nation, which will have an infrastructure of value to be held at risk to prevent such an attack.[56] Additionally, a deterrence strategy must contain elements that can be tailored to support operations against non-state actors, terrorist organizations, or individuals engaged in cyber operations. A National Institute of Public Policy study analyzed various terrorist organizations, and noted non-state actors could be deterred with various measures. The methods fell into two categories. The employment of punishment, both demonstrated and threatened, for operations launched by the non-state actor. The next method was to deny the objectives of the non-state actor. The nature of these methods is outside the scope of this paper, but it is important to note that it is possible to construct a deterrence policy that can be used effectively against these sorts of individuals and organizations.[57] Additionally, the U.S. must be able to display the willingness to engage in a proportional retaliatory strike in the space or cyberspace domains. Whereas the ability to respond is challenging, the most difficult portion of this strategy is the ability to detect and attribute this level of attack to the perpetrator to make the case on why retaliation was required.[58]

---

[55] U.S. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," 11.
[56] Ibid.
[57] Keith B. Payne et al., "Deterrence and Al-Qa'ida" (National Institute for Public Policy, 2012), 5–22, accessed March 8, 2016, http://www.nipp.org/wp-content/uploads/2014/12/Deterrence-web.pdf.
[58] U.S. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," 11–12.

While the DoD Cyber Strategy lays out the most thorough definition of deterrence of the space and cyberspace domains, it is important to note with regard to attribution, that this paper will focus on a subset of weapon systems. Specifically, it will apply to cyber-attacks, jamming, and potential co-orbital ASAT weapons. These methods do require some level of technological sophistication, but they will maintain some level of deniability versus that of a China's demonstration during the 2007 test direct ascent ASAT.[59] The inherent capabilities of some of these new technologies to degrade or destroy a satellite complicate the deterrence posture. Without clear attribution, how can deterrence work?

Attribution is fundamental to deterrence, but attribution requires a significant investment in intelligence, indications[60], and warning. This requires a mechanism for all sources of intelligence collection as well as effective dissemination of information to reduce the anonymity of both state and non-state actors alike. Detecting an event is only the first step, the attack must be tracked to the point of origin, and if possible the perpetrators of the attack must be determined. This can be done by comparing against known tactics, techniques, and procedures (TTPs) and employment methods observed during testing and real world events.[61]

The DoD Cyber Strategy mentions the benefits that public and private attribution can play in dissuading a cyber-attack. Additionally, the policy addresses whether a military strike in retaliation is warranted in the event of an attack in cyberspace by a state or non-state actor. In the event that military action is not used, the government may

[59] Ibid., 11.
[60] Indicators are defined as an event or events that suggest mobilization of forces is in progress for pending military operations.
[61] U.S. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," 11.

leverage a combination of diplomatic and law enforcement actions. The U.S. employed this method to attempt to deter future cyber economic espionage actions by China. The U.S. used "verifiable and attributable" data to establish a dialog with Beijing expressing concern with the amount of intellectual property stolen from U.S. companies. This concern is based on the reduction in competitiveness in the business markets by the loss of this intellectual property, and the resulting strategic threat and reduced stability. The Justice Department indicted five members of the People's Liberation Army (PLA) for these thefts. It remains to be seen if this action will have any measureable deterrence value in the cyber domain.[62]

A final consideration for deterrence challenges deals with common understanding. It is unknown if the PLA and the civilian leadership of the People's Republic of China (PRC) subscribe to a common deterrence theory. Most of the publications are from the PLA, and reflect the current approach to strategy from that portion of the government. As was mentioned earlier, this was seen in the civilian leadership's lack of understanding of world leaders' opinions after the 2007 ASAT test. The PLA suggests that future ASAT tests remain unpublicized to foster uncertainty.[63] As seen from research from the Cold war era, there were significant disconnects between the U.S. and the Soviet Union on deterrence application. It is important to understand the Chinese views on deterrence to ensure whatever posture is implemented will be effective. The U.S. views on deterrence could be flawed, there are more factors in deterrence than lethality or mutual

[62] Ibid., 11–12.
[63] Dean Cheng, "China's Space Program: A Growing Factor in U.S. Security Planning," *The Heritage Foundation*, last modified August 16, 2011, accessed April 30, 2015, http://www.heritage.org/research/reports/2011/08/chinas-space-program-a-growing-factor-in-us-security-planning.

threats, what is rational to the U.S. may not be rational to China, deterrence could be far less predictable than anticipated, and finally adjusting the weapons posture may have limited impacts on stability.[64]

To maintain the overpowering conventional capabilities of the United States and to minimize the economic threat of a significant loss of space systems, it is necessary to form an effective form of deterrence for space and cyberspace. According to Dean Chang, a Senior Research Fellow of the Asian Studies Center, the writings of the PLA posit, "a military must be able to exploit space. Only the high ground of space can provide the opportunity to gather information; transmit it rapidly, securely, and reliably; and exploit it promptly. PLA writings describe space as essential for reconnaissance and surveillance, communications, navigation, weather forecasting, and battle damage assessment. A military that is capable of effective joint operations can also deter an opponent. Thus, space capabilities strengthen conventional deterrence as well as deterring in their own right."[65] The Chinese strategy is remarkably similar to that of the U.S. in the sense that these systems will be used to possibly deter future conflicts, and if necessary, fight and win in future conflicts.

This statement made by Mr. Cheng mentions that effectively operating in a joint environment will also deter an opponent. This seems to mirror a statement made by the U.S. Department of Defense in the Deterrence Operations Joint Operating Concept (JOC) that, “deterrence requires a grand strategy that considers adversary-specific deterrence on a global scale, incorporates cross-[area of responsibility (AOR)] effects, and factors in

[64] Keith B. Payne, *The Fallacies of Cold War Deterrence and a New Direction*, First Edition. (Lexington, Kentucky: The University Press of Kentucky, 2001), 30.
[65] Cheng, “China’s Space Program.”

second and third order effects. This deterrence strategy must be integrated within a national deterrence strategy that integrates and brings to bear all elements of national power: diplomatic, information, military, and economic."[66] Effectively China will employ these sort of joint operations to increase deterrence capabilities as the PLA continues to develop and employ anti-access and area-denial (A2/AD) technologies in their sphere of influence to deter the U.S. from interfering in operations that China feels important. The Chinese employment of anti-satellite weapons is the latest extension of A2/AD into warfare with the intent of holding U.S. space assets at risk.

Space systems will continue to advance with new technology, and their importance will continue to increase. For space deterrence to remain viable, the United States will have to make changes to ensure deterrence viability. First, the U.S. must continue to maintain a robust space capability. This includes modernizing sensors and technology, communications capabilities, and focusing on the enhancing the resiliency of ground stations and links that are required for command and control of space missions to be possible. Furthermore, an investment in enhanced spacecraft monitoring to deter command intrusions and early detection of jamming is paramount. As mentioned earlier, "attribution—knowing who is performing what kinds of action—is essential for successful deterrence." This will require a larger investment in situational awareness platforms.[67]

Mr. Cheng notes that China's space program is a growing factor in U.S. space planning. As counterspace capabilities mature, it is no longer acceptable to operate under

[66] U.S. Department of Defense, "Deterrence Operations Joint Operating Concept," December 2006, 7, accessed February 20, 2016, http://www.dtic.mil/doctrine/concepts/joint_concepts/joc_deterrence.pdf.
[67] Cheng, "China's Space Program."

the pretense that space is a neutral zone. The U.S. should increase investment in alternatives to space systems. The DoD must be able to operate without space support. This requires a re-learning of wartime skills, but by reducing the reliance on space systems this will send the message to other countries that negating space assets will not prevent effective military action. To build on the approach of disaggregation onto commercial satellites, more unmanned aerial vehicle (UAV) communications linked should be moved off dedicated military assets to reduce the likelihood of jamming. This will retain the benefits of battlefield surveillance systems while complicating an adversary's counterspace targeting.[68]

The final area for improvement is increasing intelligence on foreign counterspace capabilities. Currently China has invested huge amounts of resources along the space deterrence lines, and that does not mean other countries will not make similar investments in the future. China's lack of transparency in the development of capabilities causes uncertainty. This lack of understanding of Beijing's policy works to their advantage. This allows China to influence other governments with stated policies describing detailed deterrence strategies during peacetime and conflict. The U.S. government needs to prioritize intelligence collection and expand the pool of experts to bolster the translation of documents.[69]

In closing, the importance of space cannot be overstated. Not only does space technology allow for rapid communication, it affords the opportunity for great scientific and economic growth. The space and cyberspace environments will continue to be contested by the U.S. and near peer nations, and overtime new nations and capabilities

[68] Ibid.
[69] Ibid.

will enter those domains. As stated by the National Security Strategy, "The world is connected by shared spaces—cyber, space, air, and oceans—that enable the free flow of people, goods, services, and ideas. They are the arteries of the global economy and civil society, and access is at risk due to increased competition and provocative behaviors. Therefore, we will continue to promote rules for responsible behavior while making sure we have the capabilities to assure access to these shared spaces."[70] The space and cyberspace domains are critically important to the national security of the United States and its allies, and serious attention is needed to maintain the space systems that ensure conventional warfare dominance when needed for operations around the globe.

The overall threat of space and cyberspace weapons employment will continue to grow, and that will influence policy development for the United States. The next chapter will focus on the different weapon systems that could be employed in these domains, and the specific deterrence challenges of these systems. This continues to build on the language that is specific to both the space and cyberspace domains working toward the real-world application of these systems in chapter four.

[70] The White House, "National Security Strategy," February 2015, 12, accessed March 18, 2015, https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

CHAPTER THREE – UNIQUE DETERRENCE CHARACTERISTICS OF SPACE AND CYBERSPACE

There is enough uncertainty in space and cyberspace where it will be difficult to prove the source, the agency, or the nation conducting hostile operations against U.S. platforms. Space control is the means that the U.S. will use to protect space assets through defensive operations as well as conduct offensive operations. China and Russia may be developing similar capabilities, but they may be listed under different terminology. From the perspective of the U.S. National Space Policy, "The United States will employ a variety of measures to help assure the use of space for all responsible parties, and, consistent with the inherent right of self-defense, deter others from interference and attack, defend our space systems and contribute to the defense of allied space systems, and, if deterrence fails, defeat efforts to attack them."[71]

As mentioned earlier, adversaries of the United States will develop and employ capabilities with the intent to neutralize U.S. space advantage. Those nations employing offensive space control technologies will leverage a series of tactics that will range from reversible effects to the destruction of a space asset. These capabilities will target space systems, forces, information links, and any potential third party space capabilities. These are commonly referred to as the "Five Ds," uncluding:[72]

- Deception operations leverage, "the manipulation, distortion, or falsification of information to induce adversaries to react in a manner contrary to their interests."[73]

[71] The White House, "National Space Policy of the United States of America," 3.
[72] U.S. Air Force, "Air Force Doctrine Document 3-14 Space Operations," June 19, 2012, 45, accessed December 15, 2015, http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-14/afdd3-14.pdf.
[73] Ibid.

- Disruption operations will force, "temporary impairment of some of all of a space system's capability to produce effects, usually without physical damage."[74]
- Denial will force, "temporary elimination of some of all of a space system's capability to produce effects, usually without physical damage."[75]
- Degradation will cause, "permanent impairment of some or all of a space systems capability to produce results, usually with physical damage."[76]
- Destruction is the, "permanent elimination of all of a space system's capabilities to produce effects' usually with physical damage."[77]

Counterspace Weapons Technology

Several technologies could be employed against U.S. space assets to reduce their effectiveness. For this paper, we will focus on electronic attack weapons, directed energy weapons, and kinetic kill vehicles. Some space weapons involve the use of electromagnetic energy and directed energy to attack an adversary. Typically, this is referred to as electronic attack (EA) or jamming. Jammers emit signals powerful enough to override the system generated signals to a satellite to prevent the reception of authentic data on the satellite. All space systems are susceptible to uplink and downlink jamming, but the jammer must be in the same band as the targeted satellite. Over the next few pages, I will explain the differences between jammers. At a high level, uplink jammers must be nearly as powerful as the satellite ground stations emitter to ensure jamming. On the other hand, ground-based downlink jammers do not need as much power to be effective since they are relying on just overpowering the already diminished signal that has traveled from space and through the Earth's atmosphere. Jammers leverage the fact that satellites require constant upkeep from the ground to maintain operations. It is often taken for granted that the

[74] Ibid.
[75] Ibid.
[76] Ibid.
[77] Ibid.

command and control of satellites occurs without a large team of people and a sophisticated system to uplink those command to ensure payload management, station keeping, and state of health services. Attacking the uplink during critical periods can degrade the mission performance, but jamming effectiveness can be mitigated by further automation of satellites and ensuring satellite ground stations are placed in ways to mitigate the fielding of a jammer in the satellite footprint. This mitigation leads to the need for downlink jamming.[78]

Uplink signals come in two varieties, signals for retransmission like communications signals, and command uplinks to the satellite for mission operations. Conducting uplink-jamming against the satellite payload is an attractive strategy. From an attribution standpoint, the jammer can be located anywhere in the satellite's footprint making it difficult to locate, and the jammer can indirectly affect all the users that rely on the retransmission of that signal. Uplink jamming requires that the jamming signal be approximately the same frequency as the target signal. This signal will be transmitted to the target satellite on the same transponder as the target signal that will lead to the onboard transponder to not be able to distinguish the jamming signal from the target signal. This inability to distinguish between signals results in the loss of or corrupted downlink to the affected users. This type of jamming does require the support of intelligence agencies to provide SIGINT and OSINT support to this sort of jamming.[79]

Whereas uplink jamming targets the satellite itself, downlink jamming is geared toward affecting ground based users exclusively. Downlink jamming is typically used to

[78] Brian Garino and Jane Gibson, "AU-18 Space Primer: Space Systems Threats" (United States Air Force, September 2009), 274–276, accessed January 15, 2016, http://www.au.af.mil/au/awc/space/au-18-2009/au-18_chap21.pdf.
[79] Ibid.

disrupt GPS and in some cases satellite communications (SATCOM) broadcasts. Similar to uplink jamming, downlink jamming requires knowledge of the signal to closely match the parameters to be effective. This will either be done via an aircraft over a regional area or by using ground based jammers to accomplish the desired EA mission. The benefit of utilizing an aircraft is based on the altitude that it can operate. The higher the aircraft's altitude, the larger the affected area. Additionally, this can help jam around terrain that would otherwise mask the jamming signal. In some cases, downlink jamming would be considered to impact satellite command and control. In most cases, satellite operators do not like to "command in the blind" since most systems require some level of command verification to send the next command. Downlink jamming would prevent the ground station from receiving the telemetry link and would cause the very scenario mentioned previously. With regard to GPS downlink jamming, the Russians market a system roughly the size of a pack of cigarettes that can deny GPS users access out to eighty kilometers, and a slightly larger one can push that number out to nearly 200 kilometers.[80]

The final type of RF weapon would rely on spoofing. This is the capability to capture, alter, and retransmit a signal in a way to mislead a recipient. This is primarily seen with sophisticated GPS downlink jamming. Certain systems will capture and retransmit the GPS signal just a few seconds later than it would receive them at higher power leading to a large position shifts. If spoofing were to be used on a satellite, it would take a sophisticated intelligence operation sponsored by a nation. This would require resources to capture, decrypt, and exploit the end-to-end satellite command and telemetry links. This

[80] Ibid.

could lead to commands being inserted into a system leading to component failure, and would be exceptionally discrete and deniable.[81]

The most important thing to understand with regard to weapons systems employing jamming, is that those systems are primarily concerned with generating effects that are hard to attribute to a point of origin and that are also reversible. These systems operate with the intent of deceiving, disrupting, and denying the use of a particular asset. Additionally, these systems are relatively inexpensive to field and many nations without sophisticated space programs could acquire and employ them to interrupt space communications in there are of operations.

The next category of space weapons are directed energy (DE) weapons, and more specifically lasers. The employment of standoff directed energy weapons would utilize either ground or air based platforms. The benefit of these platforms it the ability to engage multiple targets as well as obfuscate the attack origin. Under ideal conditions, with good geometric access, these weapons can complete an engagement in seconds. This highlights the benefits to the sunk cost of these platforms. Directed energy attacks likely do not give off many external intelligence indicators that would lead to a definitive engagement time. With these sort of weapons, the degradation may not be immediately apparent leading to difficulty tracing the attack time to a definitive point in the orbit.[82]

Laser systems include coherent radiation, aligned waveforms, and other devices operating near the optical wavelengths. These systems operate by delivering energy to the surface of the targeted satellite. The gradual or rapid absorption of the laser energy will lead to the buildup of heat leading to thermal damage to the payload or satellite bus. From

[81] Ibid.
[82] Ibid., 277–278.

a practical standpoint, anti-sensor lasers could be used against targets against satellites at various altitude. These systems require a great deal of power to focus the laser to propagate the wave over hundreds or thousands of kilometers to deliver lethal energy to the target. Some of the system capabilities for these systems include megawatt class lasers for long range weapons would require a high degree of beam quality, a high quality beam director, and a very high precision pointing system. Several factors impact the operational effectiveness of the laser, these mainly concern the ability to condition the beam to compensate for varying atmospheric effects. There is some research concerning space based lasers, however, most testing and operational systems to date have been ground and air based laser systems.[83]

Unlike the jammers described earlier, directed energy weapons would be employed to cause degradation or destruction of a space system. Additionally, these systems will be difficult to detect and determine the point of origin leading to the possibility a satellite would have failed for electrical or environmental reasons instead of from hostile employment of directed energy. These weapons require a significant amount of technology and resources to develop, and that would limit their employment to nations such as Russia or China.

Anti-Satellite (ASAT) Kinetic Kill Vehicles (KKVs) have existed since the Cold War, and were in development by both the U.S. and Soviet Union. The development of these weapons did seem to slow down or stop after the Cold War. With regard to KKV platforms, the interceptors can be divided into various categories. Primarily, I will speak to the direct ascent and co-orbital variants. These weapons are launched either from the

[83] Ibid.

ground or from aircraft into an intercept trajectory or orbit that will pass in close proximity to the target satellite. Either the onboard guidance systems or the interceptor, ground based sensors and control, or a combination of the two will be used to steer the weapon to the target.

In recent history, China completed a successful ASAT test in 2007 and the United States used this capability to destroy a failed satellite before it re-entered Earth's atmosphere over Canada with a one thousand pounds of hydrazine propellant. Operation Burnt Frost occurred on February 20, 2008, and this utilized a sea launched Standard Missile-3 (SM-3) from the USS Lake Erie. This operation resulted in the destruction of the defunct satellite preventing the toxic propellant from entering the atmosphere. Additionally, the intercept occurred at an altitude where the majority of orbital debris re-entered within forty-eight hours, and the remaining debris within a few days.[84]

The next group of interceptors falls into the co-orbital variety. These interceptors will launch from Earth into a temporary phasing orbit to allow the interceptor to align with the target satellite in a different orbit. Based on the need to conduct an on orbit intercept, these systems are more complex to develop and field. They involve having on-orbit capabilities to maintain systems in the phasing orbit for some number of hours before they maneuver to the intercept point. This also requires a larger booster to loft the satellite into orbit to account for the additional propellant needed for conducting the final maneuver to intercept. These systems could be used to attack a satellite a few hours after launch, or could remain in orbit for years before being utilized for an attack. These interceptors have

[84] U.S. Department of Defense, "Aegis Ballistic Missile Defense, One-Time Mission: Operation Burnt Frost," *Missile Defense Agency*, accessed April 9, 2016, http://www.mda.mil/system/aegis_one_time_mission.html.

the potential to engage a satellite out of view of a sensor field and mimic an orbital collision, leading to some level of question on what happened. These ASATs could be designed to look like a functioning satellite with some sort of small satellite launcher embedded into the satellite. This makes it difficult to assess the point of origin of the attack.

The core premise behind a KKV is the weapon will close and engage the target with either a hit to kill or explosive warhead. These weapons can be utilized as a direct ascent (DA) or co-orbital weapon after launch. What that really means with a DA ASAT, is the interceptor would be launched from the ground on an intercept course with the target satellite. This sort of employment would have a relatively short engagement timeline and if other nations did not have sensors watching, could be missed by intelligence agencies. This could lead to some level of deniability that the targeted satellite either exploded or broke up on-orbit for reasons that are not explained. Conversely, the co-orbital ASAT would be launched into a similar orbit as the target, then execute a rendezvous with the target, and finally engage with the target by colliding or utilizing another form of kinetic attack. Further engagement options with co-orbital ASATs could include launching smaller micro satellites from a host satellite that could be utilized for more untraceable style of attacks.

An example of this sort of satellite could be seen from China's testing of the BX-1 microsatellite. This satellite measures approximately forty centimeters on each side and weighs around 40 kilograms. This type of satellite can be further developed and its size reduced to under space surveillance tracking levels, making it a very real threat in the future. This satellite was primarily used to inspect an orbital body, test data relay

functionality, and conduct some limited proximity operations. Some would argue that these are the same capabilities required to field a co-orbital ASAT.[85]

However, the only recent testing, development, and fielding of these capabilities is being seen with the People's Republic of China. As recent as July 23, 2014, China has conducted space launches on similar profile as the January 2007 test that resulted in the deliberate destruction of a weather satellite that was no longer in service. This results in hundreds, if not thousands, or pieces of orbital debris. Unlike the 2007 test, the 2014 test did not contain an impact. It was however, a suspicious profile that has alarmed countries concerned with continued space operations. Additionally, May 13, 2013, China launched an object into a ballistic trajectory with an altitude of greater than 30,000 kilometers. This resulted in an orbital track that approached near the geosynchronous belt where numerous communications and weather satellites reside. What is interesting about this "peaceful" demonstration is the vehicle re-entered the Earth's atmosphere nine and a half hours after launch without being observed dropping off nay payloads on orbit. This test is especially a concern based on the expanded capability to threaten satellites in both MEO and GEO orbits. Furthermore, a kinetic engagement at those altitudes could lead to a catastrophic debris incident rendering whole swaths of the GEO belt unusable for space missions.[86] To date, China has not publicly acknowledged any additional anti-satellite programs, but PLA writings emphasize the need of, "'destroying, damaging, and interfering with the enemy's reconnaissance ... and communications satellites,'" which suggests that MEO and GEO,

[85] Brian Weeden, "China's BX-1 Microsatellite: A Litmus Test for Space Weaponization," *The Space Review*, accessed January 31, 2016, http://www.thespacereview.com/article/1235/1.
[86] U.S. Department of Defense, *Annual Report to Congress - Military and Security Developments Involving the People's Republic of China 2015* (Washington D.C.: Office of the Secretary of Defense, May 2015), 13–15, accessed January 10, 2016, http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf.

specifically navigation and early warning satellites, could be among the targets of future attacks designed to "'blind and deafen the enemy.'" This is consistent with reports from PLA analysis of U.S. and coalition military operations that "'destroying or capturing satellites and other sensors ... will deprive an opponent of initiative on the battlefield and [make it difficult] for them to bring their precision guided weapons into full play.'"[87]

All of the kinetic kill vehicles described represent some of the most complex systems that could be developed for space warfare. These systems are limited to nations that have their own space programs, and can invest significant resources into the development of these systems. Similar to the directed energy systems, these platforms would primarily be used to degrade or destroy other satellites. Furthermore, they would be difficult to detect based on their potential size, and the level of sophistication of the targeted nation's satellite to maintain a high level of space situational awareness to track these potential weapon systems in space.

Space Stability

The RAND report *Deterrence and First-Strike Stability in Space* raises several points that are germane to this topic. The U.S. depends on the use of space systems for all facets of national security. This includes satellite communications systems for real-time communications and collaboration anywhere in the world, GPS for precision timing and navigation, and ISR systems for intelligence collection and targeting.[88] Space systems are inherently vulnerable and very little is currently available to harden existing systems against attack. The United States Fiscal Year 2016 budget has allocated fund to

[87] Ibid.
[88] Morgan, "Deterrence and First-Strike Stability in Space: A Preliminary Assessment," iii.

further the development of resilient space systems to continue space mission assurance. Space Mission Assurance is the means of securing space-based services so that U.S. forces will have those capabilities whenever they are required.[89] That stems from unknown requirements to address the upcoming space threats, and the practical matter of cost to build a robust satellite that can operate in a congested and denied environment. Forrest Morgan, a twenty-seven year veteran of the U.S. Air Force and a senior political scientist at the RAND Corporation specializing in crisis stability, preemptive and preventive attack, escalation management, deterrence, information operations and the operational resilience of U.S. airpower in the Asia-Pacific Theater, asked a simple question that I hoped to be able to answer with this paper – "Can future enemies be deterred from attacking U.S. space systems? To what degree is deterrence reliable, and under what circumstances might it fail?"[90]

The United States is heavily reliant on space assets for real-time communication, ISR, PNT, and too many other services to list that a loss would be catastrophic to say the least. Dr. Morgan characterizes the threat in which an adversary would weigh the risks and benefits of conflict with the U.S. based on the belief that attacking our space systems would degrade our capabilities enough to attain operational objectives with an acceptable cost. This is a case where a failure in space deterrence could lead to failures in general deterrence based on superior conventional advantage. Conversely, if the cost of attacking

[89] Douglas Loverro, *Statement of Douglas Loverro Deputy Assistant Secretary of Defense (Space Policy) Before the House Committee on Armed Services Subcommittee on Strategic Forces on Fiscal Year 2016 National Defense Authorization Budget Request For National Security Space Activities* (U.S. House of Representatives: U.S. Government Printing Office, 2015), sec. U.S. House of Representatives Strategic Forces Subcommittee 4, accessed April 6, 2016, http://docs.house.gov/meetings/AS/AS29/20150325/103106/HHRG-114-AS29-Wstate-LoverroD-20150325.pdf.

[90] Morgan, "Deterrence and First-Strike Stability in Space: A Preliminary Assessment," iii.

U.S. space systems is too high, not only is space deterrence maintained but general deterrence as well.[91]

That ability to maintain a credible defense and retaliatory capability creates a viable deterrent. It would be an exceptional situation where the U.S. would retaliate against an ASAT test by destroying an adversary's satellite. The potential debris from the ongoing engagement would threaten all future space missions to include commercial and manned missions. The important topic of space debris has been an ongoing topic in this paper. Additionally, going one for one with an adversary would quickly work against the U.S. and its numerous satellites. At a certain point, there would be no more viable targets to leverage. Conversely, an argument can be made that destroying terrestrial capabilities is not only a credible threat but easier with the existing military capabilities at the disposal of the United States. As noted throughout this paper, it is hard to directly attribute a space attack. The resultant retaliatory strike used to destroy ground facilities without some level of irrefutable proof would quickly earn the condemnation of the international community. This also brings up the question of the relative value of targeting a terrestrial target in retaliation against a loss of satellite. If the U.S. were to lose a single high-value, low-density ISR satellite, what would be an appropriate terrestrial target to destroy to ensure punitive deterrence? Additionally, when striking terrestrial targets, a scenario exists where escalation quickly occurs and the retaliatory strikes become irrelevant.[92]

It goes without saying that our adversaries will attempt to "level the playing field" against U.S. capabilities in any domain that is feasible. Glenn Kent, a retired Lieutenant

[91] Ibid., xii.
[92] Ibid., xiii.

General of the U.S. Air Force and a Senior Research Fellow of the RAND Corporation specialized in strategies and analysis concepts in national security, and David Thaler, a senior defense analysts at the RAND Corporation specializing in strategy and force planning, first put the concept of first-strike stability forward in 1989 to examine the dynamics of mutual deterrence between nuclear states. They define the term first-strike stability as the two-sided calculus of each side's cost of striking first compared with the cost of striking second. Essentially that in a conflict, each side has the ability to limit potential damage on itself by striking an opponent's strategic assets first. This strategy leads to the added benefits of denying an opponent's objectives in a first or second strike by inflicting damage on that nations valued assets.[93] This concept is similar to the concept described by Charles Glaser, a former member of the Pentagon's Joint Staff and a specialist in international relations relating to security, defensive realism, and the offense-defense balance, "as a measure of the countries' incentives not to preempt in a crisis, that is, not to attack first in order to beat the attack of the enemy."[94]

Where this issue varies with space stability is that nuclear forces are not directly involved in maintaining stability in space, but they influence strategic stability utilizing capabilities such as space based missile warning. As a result, space is seen as an environment where offensive capabilities will dominate. This coupled with the inherent difficulty in creating satellites to operate in a contested environment, there is the destabilizing factor of striking space assets first to assure your military objectives. A further consideration for deterrence in space is the costly nature of the infrastructure to

[93] Glenn A. Kent and David E. Thaler, "First-Strike Stability: A Methodology for Evaluating Strategic Forces" (The RAND Corporation, August 1989), 24–26, accessed February 22, 2016, https://www.rand.org/content/dam/rand/pubs/reports/2008/R3765.pdf.
[94] Morgan, "Deterrence and First-Strike Stability in Space: A Preliminary Assessment," 1–2.

support orbital operations.[95] In addition to the infrastructure, how much global commerce would be affected by attacks in space? The global impact of such an attack would result in most nations shouldering some cost of any consortium-owned satellites as well as the ramifications if GPS was damaged and the banking industries were degraded with the lack of accurate timing. Similar to a nuclear exchange, the resulting amount of orbital debris would be catastrophic if it took key orbits away from future use. A final concern where there is a parallel to nuclear and space deterrence is that once the threshold for use is met, retaliation would likely rapidly escalate the conflict to unforeseen levels.

Bruce MacDonald, former Special Advisor for Nonproliferation and Arms Control, gave a succinct representation of the end state for the U.S. He stated that, "Our overall goal should be to shape the space domain to the advantage of the United States, and to do so in ways that are stabilizing and enhance U.S. security. The U.S. has an overriding interest in maintaining the safety, survival, and function of its space assets so that the profound military, civilian, and commercial benefits they enable can continue to be available to the United States and its allies."[96] I agree with the sentiment, and the goal should be expanded to include all countries in creating stability in space. Although advances in conventional warfare and precision guidance have led to these weapons being the preferred option in U.S. warfare, the threat of nuclear weapons still exists today.

---

[95] Ibid., 2–3.

[96] Bruce W. MacDonald, *Space and U.S. Security: Hearing before the Strategic Forces Subcommittee of the Committee on Armed Services, House of Representatives* (U.S. House of Representatives: U.S. Government Printing Office, 2009), sec. House Armed Forces Committee 2, accessed March 18, 2015, https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg51760/html/CHRG-111hhrg51760.htm.

The core limitation to applying conventional deterrence to the space domain is explained by dissecting the approach of the old, "if you shoot ours, we'll shoot yours" model.[97] When dealing with ground-based targets, this approach is not only reasonable but easily explained and understood. However, the U.S. space inventory and reliance on space assets quickly shows where this model is no longer as effective. This is solely based on the number of U.S. satellites that can be attacked when compared to other nations. While the total number of active satellites cannot be ascertained, research shows the U.S. as operating more than three times the number of satellites as China.[98] Potential enemies of the U.S., such as Russia or China, are likely going to conduct operations in regions where they have good knowledge of the area, a limited use of space based ISR, and in some cases indigenous PNT systems that the U.S. cannot access. In that case, the trading shots at satellites is not practical.

In the case that the hostile nation does not employ a space weapon that destroys a satellite, but relies on systems with reversible effects the threshold for retaliation is different. That likely will not break the threshold that dictates a hostile response where space assets will be paced in jeopardy. If the conflict were to escalate, the addition of strikes against high-value, low-density ISR assets could enable military success of the attacking country. An example of this would be for China to target U.S. ISR assets before mounting a campaign in the South China Sea. There is a school of thought that the U.S. should punish space aggressors with punitive terrestrial strikes. This lends some credibility based on the asymmetric U.S. conventional advantage. Nevertheless, this

[97] Morgan, "Deterrence and First-Strike Stability in Space: A Preliminary Assessment," 26–28.
[98] "UCS Satellite Database," *Union of Concerned Scientists*, last modified February 25, 2016, accessed April 10, 2016, http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database.

threat may not be enough to deter aggression in space. Some argue that despite the capabilities of advanced conventional weapons, they cannot generate the effects necessary in a short period to have a credible retaliatory strike. Current capabilities would have to leverage cruise missiles launched from either submarines or aircraft to fill this role. Moreover, the amount of damage generated may not be adequate for deterrence.[99] However, if the United States were to launch cruise missiles against a country's high value asset or assets, this would make for an effective and credible retaliatory capability in the event of an attack against a U.S. satellite. The U.S. does have an associated cost with the development, deployment, and operation of each of the satellites in its inventory. The value of a given space asset could be used to determine a strategy on what terrestrial targets to strike if needed. This would tie into a counter-value strategy for deterrence with regard to space assets.

Mr. Morgan makes an argument against attacking terrestrial targets in retaliation of a space asset. His argument's central premise is that if another nation is attacking the space assets of the United States, that conflict may be a foregone conclusion. He posits a scenario where the targeting of those space enablers would negate the space advantage of the U.S. and limit the advanced conventional weapons capability in a pending conflict. An example of this could be seen if China were to invade Taiwan. In this case a preemptive strike on U.S. ISR assets would allow for China to execute a limited campaign in Taiwan with a degraded U.S. military trying to project power into that theater. In this case it would be more costly to attack Taiwan without striking the space assets first. In this scenario, it becomes an exercise of damage limitation. The benefit of

[99] Morgan, "Deterrence and First-Strike Stability in Space: A Preliminary Assessment," 26–28.

negating the space assets far outweighs the potential loss of some number of terrestrial assets in a retaliatory strike. Or in the case of Taiwan invasion, the retaliatory strikes would be anticipated as part of the expanded conflict.

His secondary argument leverages on the fact that for a threat to be credible, a nation must be willing to carry out the attack. What level of credibility loss would the U.S. suffer if it failed to retaliate for the loss of capability relating to national technical means (NTM)? He further argues that in destroying a satellite that there was no loss of life, and a terrestrial attack is not a credible response. That argument fails to account for the significant amount of resources countries have invested in their space assets. If a country is not punished in some form for attacking a satellite then you fundamentally have a deterrence failure.

Contrasting with the opinions of Dr. Morgan are those of Mr. Peter Marquez, a Fellow of the George C. Marshall Institute. He argues in his essay *Space Deterrence: The Prêt-á-Porter Suit for the Naked Emperor* that, "Recently posited theories of space deterrence misuse the term deterrence; they do not grasp the intent of deterrence, the full range of other security constructs, and, most importantly, what should be done when, not if, deterrence fails. Compounding this situation is the growing belief that deterrence is an element of defense."[100] For deterrence to work, it requires three elements. Attribution, signaling, and credibility. To apply this to effectively, the U.S. requires a demonstrated capability to attribute an attack on a satellite. Next, the U.S. would need to provide clear signals that attacking an American satellite is not in the attacking nation's best interest.

[100] Robert Butterworth et al., "Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century" (George C. Marshall Institute, November 16, 2011), 15, accessed April 2, 2016, http://marshall.org/wp-content/uploads/2013/08/Butterworth-et-al-Returning-to-Fundamentals-Deterrence-and-U.S.-National-Security-in-the-21st-Century-Roundtable.pdf.

And finally, the U.S must develop, maintain, and exhibit a willingness to punish a hostile act to establish that the U.S. will act when one of its satellites is threatened or attacked.[101]

Both China and Russia are involved in developing counterspace weapons, and both countries have shown a political willingness to use these weapons. Mr. Marquez makes the argument that the U.S. does not have a deterrence relationship with either of those countries in space, but rather a compellence relationship. The weapons under development by China and Russia are a threat to the United States' ability to project power, and for this to change the U.S. must compel those nations to cease their activity on those programs. However, as long as the U.S. is heavily reliant on space capabilities, China and Russia would likely not see the benefit in abandoning those weapons programs. To change this relationship, the U.S. must have the ability to deny the use of hostile counterspace weapons by potentially denying China and Russia from meeting their national objectives.[102]

Cyberspace Weapons Technology

There is limited writing on specific cyberspace weapons employed by various countries. In this section, I will define documented cyberspace weapons that were reportedly employed against other countries. Specifically, I will speak to the nature of why these particular weapons are hard to locate and attribute to a particular user. One of the most common weaponized forms of cyber-attack is the Distributed Denial of Service (DDoS) attack. This attack was used by the Russian Governments against Estonia in 2007.

[101] Ibid., 16.
[102] Ibid., 21.

DDoS attacks occur when an attacker sends a stream of packets to the target computer. This process consumes some resources, and subsequently renders those same resources unavailable for users of the targeted computer system. A similar approach would employ malformed packets that would confuse a software application or protocol on the targeted computer leading it to freeze or force a reboot. This technique is scalable and can be used to deny services to multiple computers in a targeted network. This attack vector can ultimately lead to a point where the targeted network's users cannot access internal or external services. A DDoS attack would be executed in several phases. First, the attacker would recruit a sizeable number of agent machines. These machines could be from multiple locations around the world, which lends itself to the definition of the distributed attack. These machines are selected based on underlying security issues with the machines being exploited to conduct the attack. This phase is typically automated, and often leverages previously infected machines. Once the network of exploited computer has been created, the attack will use these computers to generate a high volume of bad information packets with the sole intent of jamming the targeted network with an excessive volume of traffic to render it unusable.[103]

The next major cyber weapon is the advanced persistent threat (APT). The computer anti-virus provider McAfee describes this as, "APTs [are] sophisticated, covert attacks bent on surreptitiously stealing valuable data from targeted and unsuspecting companies [that] can inflict serious harm to your business. Their relentless, persistent intrusions typically target key users within organizations to gain access to trade secrets,

[103] Jelena Mirkovic and Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms" (University of Delaware - Computer and Information Sciences Department, 2003), 1–5, accessed February 1, 2016, https://www.eecis.udel.edu/~sunshine/publications/ccr.pdf.

intellectual property, state and military secrets, computer source code, and any other valuable information available."[104]

Building on the earlier APT description, APT's use many of the conventional techniques employed by organizations employing cyberspace weapons. However, where they begin to differ from botnets and malware is the specific intent of the APT. Organizations who employ APTs are targeting strategic users with the aim of gaining unfettered and undetected access to sensitive information on a targeted network. The very nature designed into this threat highlights the level of damage that can be perpetuated by this sort of weapon while it operates undetected. A contemporary example of this can be observed with the employment of Stuxnet in Iran's nuclear enrichment facilities.[105]

Once an APT has been loaded onto the targeted system, it will evade conventional detection by disguising itself as legitimate network traffic. The strategic goal of an APT is to establish a covert and long-duration mission of exfiltration of sensitive data to the organization employing the weapon. An APT infiltration will begin by targeting the weakest link in any network security – the user. That infiltration can be accomplished through e-mail with a hostile attachment designed to look like a real message. This type of technique is commonly referred to as spear-phishing. Other cases leverage infecting USB devices that are plugged into networks then loading the APT directly. In recent

[104] McAfee, An Intel Corporation, "Combating Advanced Persistent Threats - How to Prevent, Detect, and Remediate APTs" (McAfee, An Intel Corporation, 2011), 3, accessed February 1, 2016, http://www.mcafee.com/us/resources/white-papers/wp-combat-advanced-persist-threats.pdf.
[105] Ibid., 3–5.

years, the USB standard has been compromised to contain bootable code that resides in the firmware that escapes most virus scanners.[106]

While not an all-encompassing list, APTs typically operate in several phases of operation. The first phase is the social engineering period to target an individual to unknowingly infect the network. Once that person has inadvertently loaded the APT into the network, the malicious code will establish for all practical purposes a cyber beachhead. This phase is where the hostile code will execute and establish communications with the organization that is executing the cyber-attack and await further instructions. The next phase is the real network infiltration. This phase builds on the previous success of building the beachhead on the network. During this point, the attackers will begin designing custom, objective-specific code to operate on the targeted network. There typically is not a one-size fits all network configuration, so some level of customization is required to successfully operate without being detected. Once the custom application has been loaded into the system, the APT moves into the persistence phase. During this phase, it will passively monitor the network, and look for opportunities to execute the attack based on the systems maintenance or operations schedule. The final phase endures until detection. During the final phase, the APT will receive remote commands to gather and exfiltrate the data to the organization conducting the cyber operation. Additionally, this phase could be used not for what is essentially espionage but for sabotage as well. This will be explored a bit later in this thesis.[107]

[106] Ibid.
[107] Ibid.

Cyber Deterrence Observations

As noted earlier, the networks and infrastructure of the cyber domain are tangible things, but the cyber domain itself does not entirely exist in the physical world. Whereas deterrence with regard to space weapons may be possible with an effective framework to ensure that space remains a sanctuary, the same cannot be said on the cyber front. Under no leap of the imagination will it be possible to maintain control of cyber weapons from being employed operationally. The best hope is to disincentive the use of those weapons against programs of national interest like power grids. An argument can be made that an attack on infrastructure, even if conducted via cyber-attack, is tantamount to an act of war if there is loss of life. In this case, an attack of that magnitude is likely to be a pre-cursor to a major regional conflict or operation. Paul Davis, a professor of policy analysis in the Pardee RAND Graduate School, has researched extensively in the cyber domain. Specifically, he notes a study conducted by the RAND Corporation that determined that cyber-attack is fundamentally different from any earlier forms of conflict that has been recognized.[108]

Aside from the obvious benefits of using cyber-operations as a means of intelligence collection, there are limited other uses in peacetime. The Stuxnet incident highlights what is possible with cyber-attacks, but it can be argued that the employment of that weapon was outside the scope of intelligence operations, and delved into the arena of offensive operations to sabotage another nation's national project. This again brings up the obvious point of cyber-weapons as offensive weapons, and the cyber domain as an enabler of intelligence operations. Cyber-attacks will not capture territory, and the

[108] Paul Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar," *New York University Journal of International Law and Politics* 47, no. 2 (November 13, 2015): 334.

effects will likely be temporary in the sense that equipment and infrastructure are not destroyed. This is contrasted against a concerted effort against a target such as a national power grid, but ultimately cyber operations will enable operations in the sea, air, and land domains.[109]

Will a nation under a cyber-attack know who committed it?[110] This question is difficult on multiple levels. One, even if the country has definitive proof of a cyber-attack, most governments would be reluctant to speak to the sources and methods used to develop that proof. The intelligence cost of going public may outweigh the benefit of doing so. Additionally, if the intelligence was garnered from some level of cyber-operation to gather intelligence it will be difficult to use this collected information in the public arena. On the other hand, the cyber-attack could be quite complex and result in not enough information to allow a nation to do anything other than publicly acknowledge a developing situation. Additionally, what level of retaliation is appropriate for a cyber-attack? From a practical standpoint, the response needs to be proportional. Launching an airstrike in response to a cyber-intrusion is not an effective strategy, and that will further damage world opinion in future dialogue in this area. However, if a cyber-attack were to damage some level of infrastructure, or have the intent of an precursor to a larger operation a retaliatory attack would be warranted.

This leads to the question of holding assets at risk. In the case of the OPM breach, is there a similar organization in China that keeps their personnel records on an unencrypted server? I would imagine that is very doubtful, and even if the U.S. could conduct a retaliatory operation, the cyber infrastructure may not be in place to target

[109] Ibid., 335.
[110] Ibid.

similar information. That would lead to targeting of other information, potentially leading to a tit for tat series of cyber exchanges. In this case, could the U.S. employ a capability with reversible effects to degrade communications or commerce for a limited period.? Eventually, the cyber-operations could lead to unforeseen levels of escalation leading to additional national issues. In the case of the OPM cyber-attack, would it be appropriate to try and levy sanctions against the attacking country? That would lead to a discussion on what the information lost was worth, and can that be quantified in such a way that is acceptable on the world stage. In this example, would the sanctions beget a reciprocal set of sanctions from China for previous cyber-incursions? This example shows how a simple question can result in even more questions that do not advance the issue.

Building on the question of holding a nation's assets at risk over a cyber-attack brings up the question of can that be done repeatedly. Along those lines, can the cyber-attacks disarm cyber attackers?[111] These questions are related in the sense that if you are going to retaliate over a cyber-attack a possible option would be to go after the means of the opposing countries cyber-operations. If the response were covert or overt, this is equivalent to a counter-battery attack and could be repeated to reduce the net cyber-capability of the attacking nation. Whether or not these attacks were aimed at reversible effects or permanent effects would have to be discussed based on proportionality. In the case of overt retaliation in the cyber domain, this sort of retaliation would have some deterrence value. The amount of resources a nation commits to a given set of weapons is usually a significant amount of capital. Potentially, this could be the cyber equivalent of

[111] Ibid.

a counter value target. Even under the circumstances of cyber counter-battery attack, it would be near impossible to disarm a cyber attacker. The focus would need to be on having capabilities to degrade the capabilities of an attacking nation to limit their effectiveness for follow on cyber-operations. The net capabilities could be reduced, but short of shutting down the Internet to the entire region, it would be difficult to carry out. In the case of denying a nation's Internet, again the question would be raised on the proportionality of the attack. An attack of that level would have significant harm to a nation's commerce even under a limited retaliatory strike.

The mere threat of a cyber-attack on Wall Street resulted in panic selling. On April 23, 2013, an event occurred that is a real-world example of just this – an unknown actor hacked the Associated Press's (AP) Twitter feed and announced that two explosions had hit the White House injuring President Obama. This "tweet" resulted in a 143-point free fall, and caused the high-frequency trading (HFT) to start selling off billions of dollars in stock.[112] This example shows the power of a minor cyber-attack, and you can imagine the enormous impact that is possible if a nation were to commit to a concerted cyber-attack in retaliation. This case is used only to illustrate the potential power of a rumor acted on by poorly informed stock traders. This shows that people will act irrationally under a set of circumstances where too much truth is placed into a source on the internet that is inherently unsecure.

The framework established by the RAND Corporation asked whether third parties would stay out of the way, and if retaliation would send the wrong message. There is a

[112] Heidi Moore and Dan Roberts, "AP Twitter Hack Causes Panic on Wall Street and Sends Dow Plunging," *The Guardian*, April 23, 2013, sec. Business, accessed February 5, 2016, http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall.

very low probability of third parties staying out of a public cyber dispute. The Russia-Georgia example demonstrated this earlier. It goes without saying that if a large scale cyber-attack was going on against a nation patriotic hackers would enter the fray. In addition to patriotic hackers, there are several communities on the internet involved in hacking targets of opportunity like the groups Anonymous and LulzSec.[113] Groups like this have been attributed to hacking news websites for their own amusement or their view of justice. One of the more well-known campaigns launched by these groups was in support of Julian Assange and Bradley Manning for their sharing of secrets on the website WikiLeaks. The view of many of these hacking groups is that information should be free and this was an opportunity for them to push their agenda in a public forum. In this case, the hackers were engaged in support of what is essentially a criminal act. Although this may not seem related to national security, it is important to note that many of the same individuals involved in these hacking groups will mobilize in support of events with national security ramifications. After the November 2015 terrorist attacks in Paris, the hacking group Anonymous launched cyber-operations against the Islamic State of Iraq and al-Sham (ISIS). The group declared their intent to hunt down the militants and utilize their hacking to weaken ISIS.[114] This campaign primarily focused on destroying the Twitter accounts utilized by ISIS for recruitment and propaganda purposes. Additionally, they are attributed with determining the identity of a high-ranking ISIS recruiter living in Europe. This campaign forced ISIS to abandon many of their websites and traditional messaging means to maintain operations on the dark

[113] Lulz is internet slang for amusement.
[114] Tara John, "Anonymous Launches 'Biggest Operation' Against ISIS in Response to Paris Attacks," *Time*, last modified November 16, 2015, accessed March 12, 2016, http://time.com/4114182/anonymous-paris-attacks/.

web.[115] It is not a large leap of the imagination to imagine groups like this being involved in any large-scale cyber-attack against another nation, but the question would remain for whose benefit?[116] This leads to the discussion of whether or not retaliation is sending the wrong message. There is a definite chance that the wrong message will be sent. The message of retaliation could be lost in translation to observing nations who did not view the cyber-attack in the same light as the country launching a retaliatory cyber-strike. This could lead to further actions on the international stage that would impact the attacking of retaliating countries.

Whether or not states can set thresholds for response or avoid escalation is harder to answer.[117] Placing a value on information stolen from a cyber-attack is challenging. Moreover, without some level of value it is difficult to establish a threshold for a response. In the case of loss of life, resulting from a cyber-attack is an area where this might be possible, but again you have to approach the problem of attribution of the cyber-attack. This highlights the need to separate the terminology associated with cyber-attacks. Every single cyber incident is highlighted as some sort of cyber-attack, and that is only partially true. It is important to delineate between intelligence operations in the cyber domain versus hostile cyber-attacks. The nature of intelligence operations will continue regardless of what the public perception of the cyber-attack is. From General Hayden's comments with regard to the OPM hack, an intelligence organization would

---

[115] Jack Fenwick and Oli Smith, "Anonymous Destroy ISIS Twitter Accounts in Campaign US Officials Take 'Secret Pleasure' in," *Express.co.uk*, last modified November 19, 2015, accessed March 12, 2016, http://www.express.co.uk/news/world/620184/ISIS-anonymous-paris-attacks-ISIL-IS-islamic-state-Abdelhamid-Abaaoud-scott-terban.

[116] Parmy Olsen, "Interview With PBS Hackers: We Did It For 'Lulz And Justice,'" *Forbes*, accessed February 5, 2016, http://www.forbes.com/sites/parmyolson/2011/05/31/interview-with-pbs-hackers-we-did-it-for-lulz-and-justice/.

[117] Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar," 335.

always strive to collect the information, and that should be separated from the retaliatory attack and that is an area where escalation would likely be avoided. With regard to the nation attacking a power grid, you can argue that escalation has already occurred and that is likely the first stage of a major attack.

This series of questions shows how viewing cyber-operations through the prism of previous intelligence and military operations is not going to lead to easy answers. Ultimately, the need for norms and policy for cyber becomes more important every day, and as the threat grows, it will reach a tipping point where action will be taken. I would image in the near future there will be accords to normalize the behavior, and that will likely include some carve out for intelligence operations.

Chapter three focused on the various technologies either under developed, or utilized in operations today. These technologies represent only what is currently imagined, and is by no means an all-encompassing explanation of the space and cyberspace threat in existence. The speed observed in technological development only illustrates how fast the technology and the threat is developing, and that continued evaluation is required to ensure that future missions are designed to operate in contested environments. In the next chapter, I will examine various cases observed during the past few years where nations employed these weapons to demonstrate that they can hold satellites at risk or employ cyber technology to further national aims.

CHAPTER FOUR – CASE STUDIES

Chapter four examines the employment of the various space and cyber weapons technologies to further the development of these capabilities or to augment ongoing operations of those nations. These examples illustrate not only the theoretical use of the weapons, but also the real world ramifications of their employment.

2007 China ASAT Test

Easily the most provocative space weapons test in recent history was conducted by China on January 11, 2007 against their defunct FENGYUN 1C polar-orbiting (sun-synchronous) weather satellite. This anti-satellite weapon was launched from a road mobile Dong Feng-21 Intermediate Range Ballistic Missile (IRBM) transporter erector launcher (TEL) shown in Figure 5.[118] The intercept was conducted between 852 and 864 kilometers which is consistent with the altitudes of most reconnaissance satellites. This test was not announced prior to execution, but was later publicly acknowledged by the Chinese government after the large amounts of international outcry by the large amounts of debris generated by the test. The initial debris field from the ASAT engagement can be observed in the lower right portion of Figure 6. [119] This illustrates the devastating effect of a kinetic weapon impacting a satellite at speeds greater than seven kilometers per second. The resultant debris field continues to be a threat to low earth objects today.

---

[118] T.S. Kelso, "AGI USER Exchange 2007: Chinese ASAT Test Analysis," *Analytical Graphics, Inc. (AGI)*, accessed January 5, 2016, https://www.agi.com/downloads/events/2007-agi-user-exchange/Chinese_ASAT_Analysis_CSSI.pdf.

[119] Global Security, "SC-19 ASAT Test," *GlobalSecurity.org*, last modified January 2007, accessed January 5, 2016, http://www.globalsecurity.org/space/world/china/sc-19-asat.htm.

Figure 5. Dong Feng-21 Road-Mobile IRBM.[120]

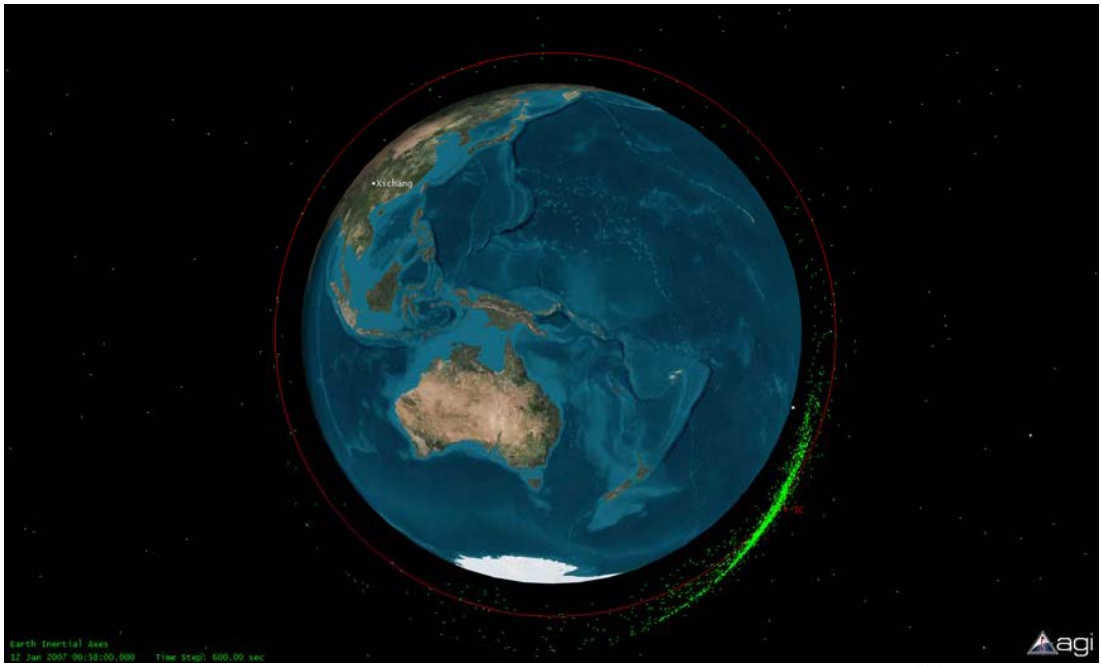

Figure 6. FENGYUN-1C Debris Track Post Engagement.[121]

[120] Kelso, "AGI USER Exchange 2007: Chinese ASAT Test Analysis."
[121] Kelso, "CelesTrak: Chinese ASAT Test."

Jonathan McDowell, a Harvard astronomer who tracks rocket launches and space activity noted that, "This is the first real escalation in the weaponization of space that we've seen in 20 years. It ends a long period of restraint."[122] Prior to this test, both the United States and Soviet Union had been involved in ASAT development and testing. The amount of debris generated from the Chinese test varies from the various reports. However, it is estimated that there are greater than 3,000 objects generated and those objects will remain on-orbit for a period ranging from two to over ninety years before that debris encounters the Earth's atmosphere.[123] This engagement shows the power of such weapons in space, and the true impact to deterrence is still being determined. I would argue that China's space weapons development program designers understands the deterrence nature of these weapons when applied to the U.S. and the vast array of military technology that relies on space based information to ensure conventional weapons dominance. The threshold for use of ASAT weapons is likely lower than that of nuclear weapons, and the threat of use against the U.S. would likely lead to some level of discussion or coercion to meet China's goals.

This is consistent with the writings of Professor Bao Shixiu of the PLA Academy of Military Sciences mentioned in chapter two. He is quoted as saying, "[There] will be a taboo on the use of space weapons, [and] the threshold of their use will be lower than that of nuclear weapons because of their conventional characteristics. Space debris may threaten the space assets of other 'third party' countries, but the level of destruction,

[122] William J. Broad and David E. Sanger, "China Tests Anti-Satellite Weapon, Unnerving U.S.," *The New York Times*, January 18, 2007, accessed January 5, 2016, http://www.nytimes.com/2007/01/18/world/asia/18cnd-china.html.
[123] T.S. Kelso, "CelesTrak: Chinese ASAT Test," *CelesTrak:*, last modified June 19, 2007, accessed January 5, 2016, https://celestrak.com/events/asat.asp.

especially in terms of human life, could be far less than nuclear weapons or potentially even conventional weapons. Therefore, the threshold of force capability required to launch an effective deterrent will inevitably be higher than for that of nuclear weapons. This unique nature of space weapons will affect the determination of the quantity and technical level of a 'deterrent capability' in space."[124]

This shows the dichotomy of this sort of weapon. For countries heavily reliant on space, the mere presence of these weapons will lead to a large change in strategic planning. The perspective of Professor Shixiu is merely one facet of the People's Republic of China (PRC), but he does represent the thinking of the PLA's Academy of Military Sciences. This assertion speaks only to the employment of KKVs as a conventional weapon, but does not describe the likely calamitous economic effects of a limited of prolonged conflict in space. As mentioned in chapter one, the threat of space debris in space conflict has the chance of causing a cascading series of collisions leading to increased space debris denying the use of low-earth orbit for years to come.

Stuxnet Employment In Iran

The Stuxnet virus was the first cyber weapon seemingly employed by a nation against another with the intent of affecting its core interests.[125] Stuxnet, an unconfirmed joint U.S./Israeli venture, was employed against Iran's Natanz nuclear facility that damaged nearly a fifth of the country's nuclear enrichment centrifuges. The deployment of this virus mirrored typical warfare where initial reconnaissance is conducted prior to

[124] Bao Shixiu, "Deterrence Revisited: Outer Space*," *China Security Journal*, no. Winter 2007 (January 1, 2007): 7–9.
[125] Ralph Langner, "Cyber Weapons: Stuxnet's Secret Twin," *The Brookings Institution*, accessed April 1, 2014, http://www.brookings.edu/research/opinions/2013/11/19-stuxnet-secret-twin-langner.

an attack. Stuxnet developed a blueprint of the nuclear facility that allowed the tailoring of the attack vector. Once an operational understanding had been developed of Natanz, the virus was designed to command the centrifuges to operate in a way to damage the controllers while providing an expected operational status to the technicians monitoring the equipment.[126]

The cyber-attack itself utilized two methods. The first method utilized the overpressure of the gas control system, and the second capability to change the rotor speeds of the centrifuge to damage the centrifuges. This control system and the associated instrumentation do not serve any operational process, but detects any anomalies for the overall safety and protection of the system and the operating environment. The centrifuges used by Iran are controlled by the amount and pressure of gas used to control the spin during the enrichment process. The gas centrifuges used by Iran are configured into groups to maximize enrichment efficiency. These groups share the same input gas piping, product, and output gas piping and this process is designed to cascade from one centrifuge to the next. The input pressure controls the overall efficiency of centrifuges, and the high sensitivity of the device is dramatically impacted by moderate variations of pressure. An increase of inlet pressure will cause more uranium hexafluoride entering the centrifuge resulting in higher mechanical stress on the rotor. Rotor wall pressure is impacted by the velocity and operating pressure that can result in solidification of the gas driving the centrifuges resulting in uranium enrichment being halted and possibly destroying the equipment. This meets the intent of delaying

[126] Michael B. Kelley, "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought," *Business Insider*, accessed April 1, 2014, http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

enrichment, but the overt nature of this attack will ensure detection of a malicious intent.[127]

While the intent of an overpressure attack is to delay enrichment without hardware destruction, the possibility of lethal use led to the development of an alternate method. This new approach was simpler at the cost of being more easily detectable. Where the overpressure attacked the gas system, this new approach attacks the most sensitive component of the centrifuge the rotor. Each of the centrifuges has a motor capable of spinning at 100,000 revolutions per minute (rpm) with a constant torque during acceleration and deceleration. The Iranian centrifuges typically operated around 63,000 rpm, but the initial attack increased the speed by one third. It is unlikely that this modest speed increase had any impact to the rotors. An additional attack profile occurred by bringing all the centrifuges in the cascade to 120 rpm, and the spun them back up. An attack like this has a larger chance of damage since it is similar to a hard-braking maneuver. The control system likely would prevent an instant spin down, but this attack vector can allow the centrifuges to travel through zones were the harmonic dissonance could cause hardware damage. Both of these attacks show the capability to destroy equipment. Further modification of the cyber weapon could override the control system causing runaway failure. This shows the creator of the cyber weapon intended to delay the program, but not to overtly destroy or damage the hardware used by the Iranians. This strategy shows the varying shades of grey of weapon system employment to meet limited campaign objectives.[128]

---

[127] Ralph Langner, "To Kill a Centrifuge," *The Langner Group*, 5–7, last modified November 2013, accessed April 1, 2014, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.
[128] Ibid., 11–13.

The Stuxnet campaign highlighted the capabilities and impacts of a cyber-attack launched against a nation's interests. This is one of the only documented cyber-attacks to date, and shows an unprovoked attack based on the intent to pursue a nuclear weapons program. The attack itself was not reported in the media to result in any loss of life or any significant damage to national infrastructure, but did have a material impact on a national goal of enriching uranium. A further consideration on cyber-attacks is if a much more technologically developed country employs cyber weapons against a smaller country, under what circumstances would the smaller country attack. Although Iran's nuclear program suffered from a cyber-attack, there is no research to support an increase in terrorist operations against either the U.S. or Israel. Iran has a well-documented history of funding third-party terrorist organizations to attack both the U.S. and Israel. Moreover, based on their limited capabilities to attack the U.S., it is consistent that proxy violence sponsored by Iran would be the continued course of action. The result of cyber-attacks may be proxy violence, but war is not a foregone conclusion.

Russia's Cyber Attack Of Georgia

Georgia, a former republic of the United Soviet Socialist Republic (USSR), has experienced quite a bit of turmoil since the dissolution of the USSR. This turmoil is a result of history with the government changes frequently between the Russian czars, a short independence after the Bolshevik Revolution, and the Soviet Union. Georgia's post-Soviet borders included the province of South Ossetia, a province containing people

who were ethnically and linguistically different from Georgia.[129] North Ossetia happened to be within the borders of the Russian Federation, although its inhabitants are ethnically the same as the South Ossetians located in Georgia. There remained a state of protracted violence between the Russian backed province of South Ossetia seeking independence from Georgia. Several attempts had been made by the Russian-backed government to gain autonomy, but they were suppressed by the Georgian government. This situation continued to escalate until after the election of Georgian president Mikheil Saakashvili in 2003. During this period of escalation, President Saakashvili pursued an agenda that included building up military capabilities to quell the uprising in both South Ossetia and Abkhazia as well as applying to join the North Atlantic Treaty Organization (NATO).[130]

In what would become a similar pattern that would be observed in Russian operations to annex Crimea in 2014, the opposition to Saakashvili's action continued to increase tensions between the two states and would encourage anti-Georgian resistance in South Ossetia. On August 7, 2008, Georgia moved their military forces into the region in response for an alleged ceasefire violation. This ultimately led to a Russian military incursion into South Ossetia where they launched air strikes into limited targets in Georgia.[131] Just prior to Russia's military action, an alleged offensive cyber-attack against Georgian digital infrastructure was launched to confuse a coordinated military response. This attack undermined the effectiveness of the Georgian government in

---

[129] Patrick Hemmer, "Deterrence and Cyber-Weapons" (Naval Post Graduate School, March 2013), 40, accessed August 23, 2015, https://calhoun.nps.edu/bitstream/handle/10945/32836/13Mar_Hemmer_Patrick.pdf?sequence=1.
[130] Armed Forces Communications and Electronics Association, "The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict," May 24, 2012, 3–4, accessed September 9, 2015, http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf.
[131] Hemmer, "Deterrence and Cyber-Weapons," 41.

dealing with the Russian attack. Essentially, this led to a one-sided information dominance that limited the Georgian's from managing the information of the attacks and leading to further confusion for the citizens of Georgia. Further cyber operations were initiated by hackers against the BBC and CNN to shape the opinions and portrayal of the Russian invasion. Specifically, these cyber-attacks were carried out to minimize the possibility of the Russians being observed as the aggressor in this operation. Additionally, there was a conscious effort to demoralize the Georgian people by defacing websites and comparing President Saakashvili to Adolf Hitler.[132]

The initial cyber-attacks targeted government and media services to prevent communication about the Russian invasion into Georgia. As the Russians moved further into South Ossetia, the cyber-attacks were expanded to include further government sites as well as those of financial institutions, business, educational institutions, and to known Georgian hacking forums to limit any counter cyber operations.[133] This cyber-attack was not limited to Georgian infrastructure. Cyber-attacks were launched into servers located in both Turkey and Ukraine that provided communication services into Georgia to further disrupt their network infrastructures.[134] The cyber weapons employed by the Russians were not terribly sophisticated and they primarily used distributed denial of service (DDoS) attacks and/or web-defacement. The techniques used by the Russian hackers were not intended to cause physical damage to the infrastructure even though the targeted services were vulnerable to such an attack.[135] While the cyber-attacks continued for

[132] Armed Forces Communications and Electronics Association, "The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict," 9–10.
[133] Hemmer, "Deterrence and Cyber-Weapons," 41.
[134] Armed Forces Communications and Electronics Association, "The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict," 8–9.
[135] Hemmer, "Deterrence and Cyber-Weapons," 42.

weeks after the invasion, the largest and most effective attacks took place during the initial five-day window of Russian military action from August 8 to August 12, 2008. After this period, all parties signed a ceasefire. However, attribution of the cyber-attacks was never established to a particular entity. Evidence supported that a wide variety of hacking elements within Russia were likely involved to include the Russian military, powered business networks, organized crime, intelligence agencies, and patriotic Russian hackers.[136]

Unfortunately, the lack of preparation and investment in network defense by the Georgian government led to a poor response to cyber-attacks and was inadequate to forestall the impacts. Since just a few years prior Estonia had been on the receiving end of a similar attack, the Estonian government was able to provide technical assistance to mitigate the damage done as well as address other vulnerabilities seen by Georgia. Georgia's initial response to block Russian IP addresses worked only for a short amount of time before the hackers rerouted their attacks from new IP addresses. Showing the benefits of corporate engagement, web services companies such as Google and Tulip allowed critical Georgian government functions to be re-hosted to servers located in the U.S. for further mitigation. While this did alleviate some of the direct attacks on Georgian systems, it led to a significant volume of the Russian attack being directed against those U.S.-based servers. This led to academic debates about private companies' roles in future cyber conflicts. All the while, Georgian hackers were able to rally in support of their nation and attempt to implement DDoS counter-attacks against Russian

[136] Armed Forces Communications and Electronics Association, "The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict," 13.

news media, but these efforts were too disorganized and small in scale compared to the Russian-based attacks.[137]

Chinese Hack Of OPM

In June 2015, the U.S. government publicly acknowledged that that U.S. Office of Personnel Management (OPM) had been penetrated by cyber-attack. This acknowledgement purportedly would put the U.S. in an awkward position for a few reasons. First, just a few months prior to this cyber-attack, U.S. Secretary of Defense Ashton Carter had announced that the United States would retaliate against major cyber-attacks. This retaliation would use either cyber tools or other means at the government's disposal. The OPM cyber-attack is the first large scale test of this new strategy, and to what level the government will respond without clear evidence of who is behind this attack. More importantly, if these attacks are attributed to the government of China, a fellow nuclear state, what sort of retaliation would be acceptable and proportional? Additionally, will this action lead to deterrence against future attacks?[138]

The cyber-attacks against OPM resulted in the theft of personal information of more than twenty million Americans. By itself, that is unfortunate, but when coupled with the knowledge that the stolen information was mostly from current and former employees of the U.S. Federal government who in some cases serve in sensitive roles, sheds a different light on the hack. The stolen data are surmised as being from mostly

[137] Ibid., 12.
[138] Sico van der Meer and Frans Paul van der Putten, "Deterrence against Chinese Cyber Espionage: The Danger of Proliferating Covert Cyber Operations" (Netherlands Institute of International Relations, September 2015), 1, accessed February 1, 2016, http://www.clingendael.nl/sites/default/files/Deterrence%20against%20Chinese%20Cyber%20Espionage%20policy%20brief%20-%20Clingendael%20September%202015.pdf.

employees who served a non-sensitive, public trust or national security positon since 2000 as a government employee or Federal contractor. In the case of 1.1 million records, the stolen data included fingerprints of the employees. After the preliminary investigation, the U.S. Government believes the government of China is behind this instance of cyber-espionage. The deterrence question associated with this intrusion deals with the nature of the penetration and how important is the information?[139] From a basic level, the information garnered from this attack is a counter intelligence windfall of epic proportions. The Chinese Government could derive from this information agents operating in country as well as use this information to target individuals with access to sensitive material. At a basic level, this is not an attack with the sole intent of crippling U.S. cyber infrastructure, but it does have potential longer-term effects for national security.

I believe this will challenge the U.S. cyber policy, and likely requires some sort of retaliation. However, it is difficult to measure what level of retaliation is appropriate for this attack. Without clear ramifications for this level of attack, potential cyber deterrence is diminished going forward. There is discussion on the OPM hack differing from the traditional cyber-attack. This is based on the fact that the intent was not to steal commercial or military data, nor to inflict any physical damage. This is further compounded by the fact the U.S. makes a clear distinction between intelligence operations for national security and cyber-espionage for commercial gain. The U.S. has acknowledged its role in intelligence gathering in the cyberspace domain, which is a legitimate function of a nation. However, the U.S. argues that the cyber-espionage with

[139] Ibid., 2.

the intent of stealing commercial information is not. One could argue the OPM hack falls under legitimate intelligence collection, and former CIA/NSA director Michael Hayden is quoted as saying, "If I, as director of the CIA or NSA, would have had the opportunity to grab the equivalent in the Chinese system, I would not have though twice, I would not have asked permission."[140]

As noted earlier, it is very difficult to attribute a cyber-attack to a particular nation or actor. This is especially true with this OPM hack, and the availability of public information precludes that level of analysis in this case. If the Chinese Government was involved in acquiring personal data on U.S. Government employees or contractors, this enables them to plan further operations with those data. This could allow China to build comprehensive cyber-personas to spoof existing systems further penetrating U.S. cyber networks. On the other hand, the cyber-attack on OPM could be retaliation for earlier U.S. cyber-operations. This illustrates the fundamental issue in play, without attribution – deterrence is not possible. Without compelling evidence of who the attacker is, it is not possible to bring the evidence into the open without compromising potential U.S. operations. It comes down to a trade between protecting capabilities while maintaining deterrence to protect not only the information systems but personal information. Moreover, if the U.S. were to openly retaliate against China for a cyber-intrusion without definitive proof, they risk the condemnation of the international community.[141]

These events show that employment of these weapons systems is something that can be observed when the attacking country is using them overtly. However, there has not been any research presented to show the timeline of the OPM hack. At the time this

[140] Ibid., 2–3.
[141] Ibid.

thesis was written, there were only limited sources alleging the OPM hack occurring as early as November 2013.[142] The OPM event likely utilized an APT over the course of some time to exploit the security present on those servers. This shows what is possible with cyber-attacks when an adversary is patient enough to covertly engage another nation with the intent of gathering large amounts of information. Each of these cases highlights the difficulties of attributing the source of an attack to the point of origin. In addition, without that knowledge, it will be near impossible to justify retaliatory operations for reasons that will be explored in the next chapter.

[142] Aliya Sternstein and Jack Moore, "Timeline: What We Know About the OPM Breach (UPDATED)," *Nextgov*, last modified June 17, 2015, accessed April 5, 2016, http://www.nextgov.com/cybersecurity/2015/06/timeline-what-we-know-about-opm-breach/115603/.

CHAPTER FIVE – CONCLUSION

This paper has covered numerous topics relevant to space and cyber deterrence. To cover this topic effectively, it was necessary to explore what makes space and cyberspace unique when compared with the more traditional domains, as well as cover the technology being employed in current and future weapon systems. This paper also focused on several real-world examples of systems employment in recent history. These scenarios ranged from the 2007 Chinese ASAT test to various levels of cyber-attacks in Iran, Georgia, and the United States. Each of these chapters answered questions and led to the various conclusions that will be outlined in this chapter.

As more nations and organizations acquire either space or cyber capabilities, it becomes more difficult to protect vital infrastructure from attack. It is clear that with the immense resources being invested into space weapons by countries like China to offset the United States' military advantage that stability in space is not a foregone conclusion. The attractiveness of attacking vulnerable satellites does show some level of capacity for norms in space with regard to space weapons, but that is only if the U.S. works to build a credible deterrent to the employment of space weapons. It becomes essential to determine an effective cost to benefit analysis where the U.S. could punish enemies for attacks in space.

Earlier in the paper, Dr. Morgan asked, "Can future enemies be deterred from attacking U.S. space systems? To what degree is deterrence reliable, and under what circumstances might it fail?"[143] Furthermore, space systems are reliant on robust cyber

[143] Morgan, "Deterrence and First-Strike Stability in Space: A Preliminary Assessment," iii.

infrastructure and the same question applies equally to the cyber domain. Although the question cannot be answered equivocally, the U.S. can work toward satisfying the major components required to establish a successful strategy for deterrence. That strategy will require investment in attribution, signaling, and establishing credibility through demonstrated actions.

The very nature of space and cyberspace complicate attribution. The U.S. will require a robust capability that can observe not only space but also cyberspace. That is a nearly insurmountable challenge for any government to face. However, without the ability to attribute an attack, the deterrence is not possible. The U.S. has invested heavily into space situational awareness since the Cold War, and that continues today with upgrades to existing space monitoring capabilities. This should continue until the U.S. can maintain a seemingly complete chain of custody for any new object launched into space. The need to detect a space launch, track the newly launched object into orbit, and characterize whether or not the object is a threat is only the beginning. There will continue to be a need for ongoing monitoring of the various orbit regime to ensure that new objects and threats do not appear and threaten existing missions. Air Force Space Command has begun down that path with the launch of the Geosynchronous (GEO) Space Situational Awareness (SSA) Program (GSSAP). This capability will maneuver near an object of interest, and enable that characterization for anomaly resolution and enhanced surveillance, to aid in maintaining flight safety.[144] This program should be

[144] Air Force Space Command Public Affairs Office, "Factsheets : Geosynchronous Space Situational Awareness Program (GSSAP)," *Air Force Space Command*, last modified April 2015, accessed April 12, 2016, http://www.afspc.af.mil/library/factsheets/factsheet.asp?id=21389.

seen as an initial investment, and continue to be developed further to enable attribution in space.

Additionally, the U.S. should focus on effective signaling with regard to space and cyberspace mission. This begins with the National Space Policy of the United States of America that states, "The United States will employ a variety of measures to help assure the use of space for all responsible parties, and, consistent with the inherent right of self-defense, deter others from interference and attack, defend our space systems and contribute to the defense of allied space systems, and, if deterrence fails, defeat efforts to attack them."[145] This statement shows that U.S. as making a public declaration on the intent to deter hostile actors from attacking satellites of the United States. However, statements alone will not ensure deterrence. The U.S. needs to be a credible actor in this arena. If the U.S. government fails to act in accordance with this guidance if an American or allied satellite is attacked, that undermines the overall credibility towards deterrence. The U.S. cannot be trapped establishing redlines or rigid guidelines in this area. It is important to leave some level of ambiguity to prevent hostile nations from taking action just outside of those guidelines. Mr. Marquez noted that if the U.S. policy was that, "foreign satellites should not be closer than 1 kilometer of our national technical means, our response options would be limited and it would invite an adversary to stand 1.1 kilometers away from our NTM."[146] This would allow an adversary to follow the spirit of the U.S. guidance but not the intent.

[145] The White House, "National Space Policy of the United States of America," 3.
[146] Butterworth et al., "Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century," 22.

These three items will never guarantee deterrence and there is no certainty on the degree of reliability for any deterrence strategy. However, failure to meet these three criteria undermines any chance of success. This is further complicated by the fact that the U.S. may not understand what motivates an adversary and how to construct a strategy that will lead to credible deterrence. This leads to the final point of what to do in the case of deterrence failure.

Although not one of the three components of a deterrence strategy, the U.S. should develop a plan in the event that a U.S. satellite is attacked. The U.S. should go on record with limited details on what the U.S. response would be in the event of an attack. There should be no question in another governments mind that the U.S. will act in the event of attack. Deterrence is not a defensive strategy, and every effort should be made to establish a robust space architecture to operate in a contested space environment. The U.S. already has a declaratory policy on assured access to space.[147] Further investment in this area is one way to disincentive an adversary from attacking U.S. satellites. If the U.S. can replace satellites that have been attacked quickly that limits the utility of attacking the space asset. Satellites are already hardened to exist in the space environment, but further requirements should be levied during the design phase to ensure robust satellites are developed for operational use. Continued disaggregation of space systems should be pursued to complicate an adversary's targeting, and lead to a defense in depth of space systems. Although deterrence is never guaranteed – chance favors the prepared.

[147] The White House, "National Space Policy of the United States of America," 5.

REFERENCES

Air Force Space Command Public Affairs Office. "Factsheets : Geosynchronous Space Situational Awareness Program (GSSAP)." *Air Force Space Command*. Last modified April 2015. Accessed April 12, 2016. http://www.afspc.af.mil/library/factsheets/factsheet.asp?id=21389.

Armed Forces Communications and Electronics Association. "The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict," May 24, 2012. Accessed September 9, 2015. http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf.

Broad, William J., and David E. Sanger. "China Tests Anti-Satellite Weapon, Unnerving U.S." *The New York Times*, January 18, 2007. Accessed January 5, 2016. http://www.nytimes.com/2007/01/18/world/asia/18cnd-china.html.

Butterworth, Robert, Peter Marquez, John B. Sheldon, and Eric Sterner. "Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century." George C. Marshall Institute, November 16, 2011. Accessed April 2, 2016. http://marshall.org/wp-content/uploads/2013/08/Butterworth-et-al-Returning-to-Fundamentals-Deterrence-and-U.S.-National-Security-in-the-21st-Century-Roundtable.pdf.

Chase, Michael. "Defense and Deterrence in China's Military Space Strategy." *The Jamestown Foundation*. Last modified March 25, 2011. Accessed March 16, 2015. http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews[tt_news]=37699.

Cheng, Dean. "China's Space Program: A Growing Factor in U.S. Security Planning." *The Heritage Foundation*. Last modified August 16, 2011. Accessed April 30, 2015. http://www.heritage.org/research/reports/2011/08/chinas-space-program-a-growing-factor-in-us-security-planning.

Clapper, James R. *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee*. U.S. Senate: Office of the Director of National Intelligence, 2016. Accessed April 3, 2016. http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.

Clark, Colin. "Two Scenarios Tested: STRATCOM's Haney On JICSPOC Lessons." *Breaking Defense*. Last modified January 22, 2016. Accessed April 2, 2016. http://breakingdefense.com/2016/01/two-scenarios-tested-stratcoms-haney-on-jicpsoc-lessons/.

Davis, Paul. “Deterrence, Influence, Cyber Attack, and Cyberwar.” *New York University Journal of International Law and Politics* 47, no. 2 (November 13, 2015): 30.

Dr. S. Sanz Fernández de Córdoba. “100km Altitude Boundary for Astronautics.” *Fédération Aéronautique Internationale (FAI).* Accessed December 10, 2015. http://www.fai.org/icare-records/100km-altitude-boundary-for-astronautics.

Fenwick, Jack, and Oli Smith. “Anonymous Destroy ISIS Twitter Accounts in Campaign US Officials Take ‘Secret Pleasure’ in.” *Express.co.uk*. Last modified November 19, 2015. Accessed March 12, 2016. http://www.express.co.uk/news/world/620184/ISIS-anonymous-paris-attacks-ISIL-IS-islamic-state-Abdelhamid-Abaaoud-scott-terban.

Garino, Brian, and Jane Gibson. “AU-18 Space Primer: Space Systems Threats.” United States Air Force, September 2009. Accessed January 15, 2016. http://www.au.af.mil/au/awc/space/au-18-2009/au-18_chap21.pdf.

Global Security. “SC-19 ASAT Test.” *GlobalSecurity.org*. Last modified January 2007. Accessed January 5, 2016. http://www.globalsecurity.org/space/world/china/sc-19-asat.htm.

Hemmer, Patrick. “Deterrence and Cyber-Weapons.” Naval Post Graduate School, March 2013. Accessed August 23, 2015. https://calhoun.nps.edu/bitstream/handle/10945/32836/13Mar_Hemmer_Patrick.pdf?sequence=1.

Hyten, General John. *National Security Space Budget for FY17: Presentation to the Subcommittee on Strategic Forces of the House Armed Services Committee*. U.S. House of Representatives: U.S. Government Printing Office, 2016. Accessed March 16, 2016. http://docs.house.gov/meetings/AS/AS29/20160315/104620/HHRG-114-AS29-Bio-HytenJ-20160315.pdf.

John, Tara. “Anonymous Launches ‘Biggest Operation’ Against ISIS in Response to Paris Attacks.” *Time*. Last modified November 16, 2015. Accessed March 12, 2016. http://time.com/4114182/anonymous-paris-attacks/.

Kelley, Michael B. “The Stuxnet Attack On Iran’s Nuclear Plant Was ‘Far More Dangerous’ Than Previously Thought.” *Business Insider*. Accessed April 1, 2014. http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

Kelso, T.S. “AGI USER Exchange 2007: Chinese ASAT Test Analysis.” *Analytical Graphics, Inc. (AGI).* Accessed January 5, 2016. https://www.agi.com/downloads/events/2007-agi-user-exchange/Chinese_ASAT_Analysis_CSSI.pdf.

———. “CelesTrak: Chinese ASAT Test.” *CelesTrak:* Last modified June 19, 2007. Accessed January 5, 2016. https://celestrak.com/events/asat.asp.

Kent, Glenn A., and David E. Thaler. “First-Strike Stability: A Methodology for Evaluating Strategic Forces.” The RAND Corporation, August 1989. Accessed February 22, 2016. https://www.rand.org/content/dam/rand/pubs/reports/2008/R3765.pdf.

Langner, Ralph. “Cyber Weapons: Stuxnet’s Secret Twin.” *The Brookings Institution*. Accessed April 1, 2014. http://www.brookings.edu/research/opinions/2013/11/19-stuxnet-secret-twin-langner.

———. “To Kill a Centrifuge.” *The Langner Group*. Last modified November 2013. Accessed April 1, 2014. http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

Loverro, Douglas. *Statement of Douglas Loverro Deputy Assistant Secretary of Defense (Space Policy) Before the House Committee on Armed Services Subcommittee on Strategic Forces on Fiscal Year 2016 National Defense Authorization Budget Request For National Security Space Activities*. U.S. House of Representatives: U.S. Government Printing Office, 2015. Accessed April 6, 2016. http://docs.house.gov/meetings/AS/AS29/20150325/103106/HHRG-114-AS29-Wstate-LoverroD-20150325.pdf.

MacDonald, Bruce W. *Space and U.S. Security: Hearing before the Strategic Forces Subcommittee of the Committee on Armed Services, House of Representatives*. U.S. House of Representatives: U.S. Government Printing Office, 2009. Accessed March 18, 2015. https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg51760/html/CHRG-111hhrg51760.htm.

Martin, David. “The Battle Above.” *60 Minutes*. Last modified April 26, 2015. Accessed April 27, 2015. http://www.cbsnews.com/news/rare-look-at-space-command-satellite-defense-60-minutes/.

McAfee, An Intel Corporation. “Combating Advanced Persistent Threats - How to Prevent, Detect, and Remediate APTs.” McAfee, An Intel Corporation, 2011. Accessed February 1, 2016. http://www.mcafee.com/us/resources/white-papers/wp-combat-advanced-persist-threats.pdf.

McKinnon, Mika. “A History of Garbage in Space.” *Earth & Space*. Accessed January 17, 2016. http://space.gizmodo.com/a-history-of-garbage-in-space-1572783046.

van der Meer, Sico, and Frans Paul van der Putten. “Deterrence against Chinese Cyber Espionage: The Danger of Proliferating Covert Cyber Operations.” Netherlands Institute of International Relations, September 2015. Accessed February 1, 2016. http://www.clingendael.nl/sites/default/files/Deterrence%20against%20Chinese%20Cyber%20Espionage%20policy%20brief%20-%20Clingendael%20September%202015.pdf.

Mirkovic, Jelena, and Peter Reiher. “A Taxonomy of DDoS Attack and DDoS Defense Mechanisms.” University of Delaware - Computer and Information Sciences Department, 2003. Accessed February 1, 2016. https://www.eecis.udel.edu/~sunshine/publications/ccr.pdf.

Moore, Heidi, and Dan Roberts. “AP Twitter Hack Causes Panic on Wall Street and Sends Dow Plunging.” *The Guardian*, April 23, 2013, sec. Business. Accessed February 5, 2016. http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall.

Morgan, Forrest. “Deterrence and First-Strike Stability in Space: A Preliminary Assessment.” RAND Corporation, 2010. Accessed March 18, 2015. http://www.rand.org/content/dam/rand/pubs/monographs/2010/RAND_MG916.pdf.

Murray, Craig. “China Missile Launch May Have Tested Part of a New Anti-Satellite Capability_05.22.13.pdf.” *U.S. - China Economic and Security Review Commission*. Last modified May 22, 2013. Accessed April 17, 2015. http://www.uscc.gov/sites/default/files/Research/China%20Missile%20Launch%20May%20Have%20Tested%20Part%20of%20a%20New%20Anti-Satellite%20Capability_05.22.13.pdf.

Olsen, Parmy. “Interview With PBS Hackers: We Did It For ‘Lulz And Justice.’” *Forbes*. Accessed February 5, 2016. http://www.forbes.com/sites/parmyolson/2011/05/31/interview-with-pbs-hackers-we-did-it-for-lulz-and-justice/.

Payne, Keith B. *The Fallacies of Cold War Deterrence and a New Direction*. First Edition. Lexington, Kentucky: The University Press of Kentucky, 2001.

Payne, Keith B., Thomas K. Scheber, Kurt R. Guthe, and Cynthia L. Storer. “Deterrence and Al-Qa’ida.” National Institute for Public Policy, 2012. Accessed March 8, 2016. http://www.nipp.org/wp-content/uploads/2014/12/Deterrence-web.pdf.

Pollpeter, Kevin, Eric Anderson, Jordan Wilson, and Fan Yang. “China Dream Space Dream_Report.pdf.” *U.S. - China Economic and Security Review Commission*. Last modified March 2, 2015. Accessed March 17, 2015. http://www.uscc.gov/sites/default/files/Research/China%20Dream%20Space%20Dream_Report.pdf.

Riebeek, Holli. “Catalog of Earth Satellite Orbits: Three Classes of Orbit.” *NASA Earth Observatory*. Last modified September 4, 2009. Accessed April 10, 2016. http://earthobservatory.nasa.gov/Features/OrbitsCatalog/page2.php.

Sellers, Jerry. *Understanding Space, An Introduction to Astronautics*. Third Edition. McGraw-Hill Companies, Inc., 2007.

Shixiu, Bao. “Deterrence Revisited: Outer Space*.” *China Security Journal*, no. Winter 2007 (January 1, 2007): 119.

Sternstein, Aliya, and Jack Moore. “Timeline: What We Know About the OPM Breach (UPDATED).” *Nextgov*. Last modified June 17, 2015. Accessed April 5, 2016. http://www.nextgov.com/cybersecurity/2015/06/timeline-what-we-know-about-opm-breach/115603/.

The White House. “International Strategy For Cyberspace - Prosperity, Security, and Openness in a Networked World,” May 2011. Accessed March 30, 2014. https://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf.

———. “National Security Strategy,” February 2015. Accessed March 18, 2015. https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

———. “National Space Policy of the United States of America,” June 28, 2010. Accessed August 10, 2015. https://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf.

U.S. Air Force. “Air Force Doctrine Document 3-14 Space Operations,” June 19, 2012. Accessed December 15, 2015. http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-14/afdd3-14.pdf.

U.S. Department of Defense. “Aegis Ballistic Missile Defense, One-Time Mission: Operation Burnt Frost.” *Missile Defense Agency*. Accessed April 9, 2016. http://www.mda.mil/system/aegis_one_time_mission.html.

———. *Annual Report to Congress - Military and Security Developments Involving the People’s Republic of China 2015*. Washington D.C.: Office of the Secretary of Defense, May 2015. Accessed January 10, 2016. http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf.

———. “Department of Defense Strategy for Operating in Cyberspace,” July 2011. Accessed March 27, 2014. http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

———. “Deterrence Operations Joint Operating Concept,” December 2006. Accessed February 20, 2016. http://www.dtic.mil/doctrine/concepts/joint_concepts/joc_deterrence.pdf.

———. “Joint Publication 3-12(R) Cyberspace Operations,” n.d. Accessed December 16, 2015. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

———. “Joint Publication 3-14 Space Operations,” May 2013. Accessed December 15, 2015. http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf.

———. “New Joint Interagency Combined Space Operations Center to Be Establish.” *U.S. Department of Defense*. Last modified September 11, 2015. Accessed April 2, 2016. http://www.defense.gov/News/News-Releases/News-Release-View/Article/616969/new-joint-interagency-combined-space-operations-center-to-be-established.

Weeden, Brian. “China’s BX-1 Microsatellite: A Litmus Test for Space Weaponization.” *The Space Review*. Accessed January 31, 2016. http://www.thespacereview.com/article/1235/1.

“UCS Satellite Database.” *Union of Concerned Scientists*. Last modified February 25, 2016. Accessed April 10, 2016. http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database.