Strategy Research Project

# POSSIBLE FUTURES: SPACE CAPABILITY RISKS AND THE JOINT FORCE

BY

LIEUTENANT COLONEL GEORGE B. LAVEZZI
United States Air Force



USAWC CLASS OF 2010



U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| **1. REPORT DATE** *(DD-MM-YYYY)* | **2. REPORT TYPE** | **3. DATES COVERED** *(From - To)* |
|---|---|---|
| 24-03-2010 | Strategy Research Project | |

**4. TITLE AND SUBTITLE**

Possible Futures: Space Capability Risks and the Joint Force

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**

Lieutenant Colonel George B. LaVezzi

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Colonel Murray R. Clark
Department of Command, Leadership, and Management

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

**10. SPONSOR/MONITOR'S ACRONYM(S)**

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION / AVAILABILITY STATEMENT**

Distribution A: Unlimited

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

By the mid 2020s, near peer competitors, regional powers and international non-state actors will be able to threaten the Joint Force's access to and application of space-based capabilities. These threats will cover the spectrum of space operations, from on-orbit satellites to ground control elements, and will include physical, electronic and cyber attacks. Analysis of the threat environment reveals recurring vulnerabilities in the satellite control network and in capabilities designed to disrupt or deny a competitor's use of space capabilities. Additionally, the United States must develop some redundancy in intelligence, surveillance, reconnaissance and communications capability in the event adversary activities interfere with access to these satellites. Services and Joint Force commanders can use this forecast of vulnerabilities to inform near term investment decisions impacting spacing capabilities in an effort to mitigate longer term risks.

**15. SUBJECT TERMS**

Space-based Capabilities, Vulnerabilities, Investment

| **16. SECURITY CLASSIFICATION OF:** | | | **17. LIMITATION OF ABSTRACT** | **18. NUMBER OF PAGES** | **19a. NAME OF RESPONSIBLE PERSON** |
|---|---|---|---|---|---|
| **a. REPORT** | **b. ABSTRACT** | **c. THIS PAGE** | | | **19b. TELEPHONE NUMBER** *(include area code)* |
| UNCLASSIFED | UNCLASSIFED | UNCLASSIFED | UNLIMITED | 28 | |

USAWC STRATEGY RESEARCH PROJECT

# POSSIBLE FUTURES: SPACE CAPABILITY RISKS AND THE JOINT FORCE

by

Lieutenant Colonel George B. LaVezzi
United States Air Force

Colonel Murray R. Clark
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.



U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

## ABSTRACT

AUTHOR: Lieutenant Colonel George B. LaVezzi

TITLE: Possible Futures: Space Capability Risks and the Joint Force

FORMAT: Strategy Research Project

DATE: 24 March 2010 WORD COUNT: 5,340 PAGES: 28

KEY TERMS: Space-based Capabilities, Vulnerabilities, Investment

CLASSIFICATION: Unclassified

By the mid 2020s, near peer competitors, regional powers and international non-state actors will be able to threaten the Joint Force's access to and application of space-based capabilities. These threats will cover the spectrum of space operations, from on-orbit satellites to ground control elements, and will include physical, electronic and cyber attacks. Analysis of the threat environment reveals recurring vulnerabilities in the satellite control network and in capabilities designed to disrupt or deny a competitor's use of space capabilities. Additionally, the United States must develop some redundancy in intelligence, surveillance, reconnaissance and communications capability in the event adversary activities interfere with access to these satellites. Services and Joint Force commanders can use this forecast of vulnerabilities to inform near term investment decisions impacting spacing capabilities in an effort to mitigate longer term risks.

# POSSIBLE FUTURES: SPACE CAPABILITY RISKS AND THE JOINT FORCE

Since the fall of the Soviet Union, United States Joint Force Commanders have enjoyed space supremacy and the unfettered access to information and capabilities this supremacy provides. Whether this happy condition will be true during the potential conflicts of the 2020s is a debatable question.[1] United States' dominance in space launch and satellite production is giving way to competition in both the developed and developing worlds. In the coming decades many nations may be able to acquire significant space capabilities.[2] Of particular importance is the question: where should the Department of Defense focus its investments and efforts to ensure space superiority and Joint Force access to space-based capabilities?

In fifteen years, threats to the Joint Force Commander's capabilities could include the possibility of adversary on-orbit counter-space operations as well as physical and cyber attacks against United States space control, information and communications networks. Additionally, potential adversaries may gain access to previously unavailable force-multiplying capabilities from the proliferation of space services provided by commercial companies.[3]

The United States must investigate threats to United States space superiority in the middle of the 2020s in order to mitigate their disruptive counter-space effects. What follows is a general discussion of the types of space-based capabilities the United States may possess and a brief description of the means or mechanisms from which those capabilities are vulnerable. Three scenarios for future conflicts are then considered, each presenting in more detail the vulnerabilities Joint Forces will face

against certain classes of adversaries. Finally, areas where additional investigation or capability may be warranted are suggested and prioritized.

Joint Force Space Capability Review

Today's Unified Command Plan assigns the responsibility for the space domain to United States Strategic Command.[4] As such the Commander of United States Strategic Command conducts space force enhancement, space support, space control and space force applications missions for the nation. Space force enhancement operations are designed to increase joint force effectiveness.[5] The forces conducting these operations operate satellite constellations providing: intelligence, surveillance, reconnaissance; communications; and space-based positioning, navigation and timing. One can find intelligence, surveillance and reconnaissance constellations in high, medium and low earth orbits, depending on the requirements of the sensor payloads.[6] This mix of orbits will continue into the 2020s; sensors will still drive trade-offs between coverage, dwell time and resolution afforded by multiple orbit geometries. These constellations provide imagery, infra-red event detection and various electromagnetic spectrum surveillance options to Joint Force Commanders and other national customers.[7]

Satellites in high earth orbit provide most of the Department of Defense's organic satellite communications. The demand for broadcast bandwidth currently outpaces the capacity of Department of Defense satellite communications systems and this phenomenon is likely to persist over the next few decades.[8] As a result, the Department of Defense, and thus Joint Force Commanders, will depend on access to commercial vendors to fill a portion of their satellite communication needs.[9] Many commercial

communications companies place less costly and less capable systems in low earth orbit. The need for more satellites is offset by their lower production and launch costs.[10]

Space-based positioning, navigation and timing satellites, colloquially known as the Global Positioning System, are perhaps the most valuable and most difficult to replace force-enhancement system in the Department of Defense's arsenal. Highly accurate timing pulses, used for navigation, geo-location, world-wide network synchronization and encryption provide the Joint Force Commanders' advantages in accuracy, network capability, data sharing and collaborative solutions. A system in medium earth orbit provides the current position, navigation and timing signal. A Global Positioning System competitor, the European Union Galileo program, operates in the same orbital band and is scheduled to be operational by the 2020s.[11]

While space enhancement missions provide services to all Joint Force Commanders, space support operations are designed to emplace, maneuver and update satellite systems.[12] Additionally, space support operations may reconstitute or replace capabilities as required.

Elements of the United States Strategic Command conduct space control operations to support friendly freedom of action or deny the same to an adversary.[13] These offensive and defensive actions develop accurate space situational awareness and include terrestrial, on–orbit or cyberspace operations to produce the desired effects.

Finally, space force application involves the use of weapons transiting space. International conventions prohibit the "basing" of weapons in-orbit.[14] The United States and its adversaries will continue to comply with these conventions in the 2020s.

Areas of Potential Vulnerability in the mid 2020s

In the future, potential adversaries will be able to threaten United States superiority and Joint Force Commanders' assured access to space capabilities through four general types of operation. These include challenging United States space superiority by accessing their own or commercial space systems; interfering with the delivery of services at tactical ground-based terminals or receivers; attacking the ground-based elements of the satellite control network; and, finally, directly attacking orbiting satellites.[15]

First, a potential adversary may challenge the Commander of United States Strategic Command's ability to deny or disrupt adversarial use of space. The joint concept of space superiority will have to expand from its present scope. Current joint doctrine defining space superiority as "The degree of dominance in space of one force over another that permits the conduct of operations by the former...at a given time and place without prohibitive interference by the opposing force" will have to more explicitly include the concept of denying the enemy the use of space.[16] During recent and past conflicts, the United States has largely been able to restrict, exploit or deny adversarial access to operationally relevant space capabilities through diplomatic and economic means. Additionally, the United States has been willing and able to "buy up" international commercial satellite time, bandwidth, and services so none is available on the open market for its adversaries to procure. This ability to deny past adversaries use of space capabilities has been largely due to those adversaries' lack of organic space capability and poor diplomatic leverage. Future adversaries possessing organic capabilities, or sufficient diplomatic power, may be able to maintain access to space services.[17]

Next, potential adversaries may be able to interfere with the delivery of space services at the tactical level through a process known as down-link jamming. This would probably manifest as electromagnetic spectrum denial or offensive cyber-operations.[18] In past conflicts, adversaries have attempted to jam both communications and position-timing-navigation signals in an effort to locally disrupt the effectiveness of these systems.[19,20] Computer networks in Estonia and Georgia were effectively shut down during confrontations with Russia.[21,22] As these capabilities mature and proliferate, they pose a threat to the future Joint Force.

Third, potential adversaries may be able to attack critical ground-based elements of the United States' satellite control network through both kinetic and non-kinetic means.[23] Attacks against satellite up- and down-link facilities may provide disproportionate effects until those facilities can be repaired or replaced.

Finally, some future adversaries may be able to disrupt or destroy orbiting satellites.[24] The United States, the former Soviet Union and the People's Republic of China have all demonstrated the ability to physically destroy satellites in low earth orbit. Additionally, there is some evidence that China may be pursuing the capability to dazzle or temporarily disrupt low earth orbiting satellites transiting over Chinese territory.[25]

Potential Adversary Scenarios

While these four broad areas of vulnerability will exist in the mid-2020s, not all future adversaries will have similar capability and capacity to threaten or exploit them. To simplify the future threat environment against which the Department of Defense will make investment decisions, it is useful to categorize future adversaries. Three categories of future adversaries pose potential threats to United States space capabilities in the mid 2020s: near peer competitors, Regional Powers, and international

non-state actors. Each adversary has particular characteristics and access to mechanisms by which they can disrupt and/or defeat future space-delivered capabilities and the impact the loss would have on the Joint Force Commander. Additionally, some of the adversaries will have access to capabilities which introduce a “wild card” element to future conflict. Considering such a wild card will provide additional insight on which space capabilities may be most vulnerable.

*Near Peer Competitor*. Near peer competitors will have both the power and motivation to confront the United States on a global scale.[26] Near peer competitors will have a variety of capabilities with which they could hold at risk space-based capabilities provided to the Joint Force Commander. Their more salient military characteristics would include the ability to conduct global kinetic and non-kinetic operations in pursuit of military and policy objectives. This does not imply near peer competitors would be able to sustain intercontinental invasions with large conventional forces, but rather they can plan and execute selected and effective military operations of significant duration at any point on Earth.[27] A second important characteristic will be the ability to unilaterally deter the United States from crossing the nuclear threshold. A near peer competitor must be able to underwrite its own survival without reliance on international pressure to restrain the actions of the United States. Finally, near peer competitors will have organic access to the space environment in terms of space operations and space support; they will not completely depend on foreign suppliers for space-derived capabilities.

On the diplomatic front, near peers will influence a meaningful sphere of nations to protect their interest as well as exert adequate international power to avoid catastrophically unfavorable actions by international organizations such as the United

Nations. Looking into the world of the mid-2020s, several nations or groups of nations have the potential to be Near Peers. These include the People's Republic of China, Russia, India and various nations in the European Union. Conflict with any of these polities is neither inevitable nor even likely; however, these countries have the demonstrated potential to compete with the United States at this level should events lead them in that direction.

Near peers offer the largest challenge to the United States. These nations or alliances can confront the United States across the full spectrum of capabilities including: space superiority through access to organic or leased space assets; the ability to disrupt terminals/receivers deployed with maneuver and support forces; the ability to interfere with globally dispersed ground control stations; and finally, the ability to disrupt or destroy on-orbit systems. To begin with, near peer competitors will challenge United States space superiority with access to their own space systems. In confrontations since the end of the Cold War, the United States has had the luxury of operating against adversaries with limited to no effective access to space-based capabilities. Near Peer Competitors will have and be able to exploit space-derived Intelligence, Surveillance and Reconnaissance, making operational security of maneuver forces more difficult, and potentially depriving the United States of the ability to gain operational surprise.[28,29] Communication satellite constellations can provide difficult-to-jam, spread spectrum or agile frequency hopping options used for command and control, intelligence and computer network operations. Past United States practices of using economic and diplomatic power to influence foreign companies and

governments to deny or limit adversaries' access to space may not be available against near peer competitors.[30]

In addition to being able to access and utilize space-based capabilities, near peer competitors may effectively disrupt the delivery of space-based capabilities at the receiver or terminal end. These threats exist today, such as Iraq's attempt to use Global Positioning System jamming to protect locations during Operation IRAQI FREEDOM, the proliferation of communications jamming technology, and the high level of computer network mapping (a pre-requisite for effective computer network attack).[31] Near peers may be able to produce localized outages of services. This is particularly worrisome for communications and positioning, timing and navigation capabilities. Disrupted communications could complicate the use of operational level unmanned aerial vehicles which depend on satellite communication for control and transmission of data.[32] The lack of assured and effective communications could hamper the ability of tactical and operational level headquarters to communicate and coordinate. Finally, the degradation of positioning signals could drastically reduce the effectiveness of precision munitions.[33] The United States has substituted accuracy for explosive weight in its munitions; the soon-to-be ubiquitous small diameter bomb contains only one-quarter of the explosives of its next larger cousin, the venerable Mk82 500lbs bomb.[34] These reductions in net explosive weight mean that missing by even a small distance can render the target immune from the blast's effects.

A near peer competitor will be able to jam these terminal/receiver at the time and place of their choosing to create favorable offensive or defensive conditions, thus forcing the Joint Force Commander to deal with additional ambiguity. The lack of

assured access to these space-based capabilities will factor into planning, creating the need for additional reserves and more conservative schemes of fire and maneuver.

More worrisome than the battlefield effects a near peer may create is the potential for an adversary to disrupt, usurp, or destroy the ground-based elements of our satellite control network. All United States satellite constellations require periodic communications with designated ground stations for maintenance, upkeep and control.[35] Loss of the ability to communicate and pass commands in this manner will lead to a loss of accuracy and effectiveness of our satellites, and can effectively produce a global outage of the services provided by entire satellite constellations.[36]

Satellite control network ground stations are vulnerable to physical destruction and cyber attack.[37] A near peer competitor may have the ability to physically destroy these locations through either conventional or special operations. Additionally, such an adversary may have the requisite capabilities to conduct a computer network attack, rendering the network incapable of proper operations. The loss of all secure satellite communications or inaccurate Global Positioning System signals will wreak havoc at all levels of United States strategy and operations.

Finally, near peer competitors will be able to directly challenge, disrupt and potentially destroy on-orbit satellites. This would materialize as either earth-based systems designed to disrupt or destroy satellites or space-based systems with the same goals. Several countries have already demonstrated the technology for such capabilities. The United States and People's Republic of China have systems which can intercept and destroy satellites in low earth orbit as evidenced respectively by their 2008 and 2007 tests of these systems; in 1985 the United States actually developed, tested,

then mothballed an anti-satellite missile designed to be launched from an F-15 aircraft.[38,39,40] Additionally, the People's Republic of China is suspected of using high-powered ground-based lasers or other electromagnetic systems to "dazzle," temporarily blind, or disrupt low earth orbit systems.[41] Thus many intelligence, surveillance, reconnaissance and communication satellite constellations in low earth orbit (less than 1000 miles in altitude) will be vulnerable to piece-wise disruption and destruction. Loss of individual satellites will create intelligence, surveillance, reconnaissance and communications gaps, directly impacting the Joint Force Commander's ability to plan and conduct operations.

In addition to ground-launched interceptors, primarily a threat to low earth orbit systems, near peer competitors may also field satellites to counter United States satellites at any orbit. In the 1970s, the Union of Soviet Socialist Republics orbited and tested "hunter-killer" satellites which intercepted the target satellite then destroyed it by detonating a payload of conventional explosives.[42] A near peer competitor may be able to orbit either "hunter killer," jamming or micro satellites near US communications, positioning, navigation and timing satellites.[43] Jamming satellites, vice destroying them, allows an adversary to discriminately deny service, to follow a *Jus in Bello* approach for satellite service disruption and to mitigate international ire caused by interfering with a world-wide service. For example, a Global Positioning System's satellite's "escort" may only disrupt the signal when that satellite is of use in the future areas of operations; it would function normally when not directly supporting a combat zone. However, the methodology of orbiting satellites to interfere with other satellites has several disadvantages. The satellite launches, and the maneuver of the hunter-killer/jamming

satellite once on orbit may be observable to the United States, affording time to take counter-measures. Additionally, there is considerable cost to develop, launch and operate such systems—thus the opportunity costs of such an investment may make it undesirable.

While Near peer competitors will have the capacity to interfere with the panoply of United States space capabilities, Regional Powers will face limits on both the breadth and depth of their potential counter-space operations.

*Regional Powers.* Regional powers will be capable of projecting their military power in their geographical area but not necessarily conducting effective sustained operations across the globe. A conspicuous difference between regional powers and near peers it the former's potential lack of organic access to space. Additionally, while they may possess limited weapons-of-mass-destruction capability, they will rely on the support of near peers or international norms to deter the United States from using nuclear weapons. More dangerous regional powers may be able to garner, if not open support, then at least non-interference of other great powers. This support will provide regional powers freedom of action in their desired sphere of influence. More powerful regional actors will be able to influence others to hamper or mitigate undesirable international and United Nations condemnations and sanctions.

In this manner, regional powers may be able to influence others in order to obtain access to non-organic space capabilities. Some regional powers may have limited organic access to space capabilities, but many may be able to access neutral or friendly government and commercial capabilities for intelligence, surveillance, reconnaissance

and communications. As in the case of near peers, future Joint Force commanders may have to contend with effectively networked, highly informed adversaries.

In addition to challenging the United States' ability to limit their access to space, regional powers will also be able to threaten the terminal/receiver end of the space-based capability. Regional powers, either through domestic production or military procurement, will have access to the same or similar disruptive systems. Using such systems, regional powers will challenge future Joint Forces' access to space-based capabilities guidance and communications, forcing future commanders to operate in a degraded environment.

Although regional powers will lack the ability to conduct sustained global (vice regional or local) operations of near peers, they may produce isolated effects at various points around the globe. Such attacks would more likely be in the form of special or irregular operations against specific point targets. Thus, portions of the United States' satellite-control infrastructure may be at risk from physical attack. More problematic may be the access of regional powers to cyber capabilities which disrupt the efficient operation of satellite maintenance and control systems. The effective disruption of these systems, either through kinetic or non-kinetic means, could introduce Department of Defense-wide disruptions in planning and operations.

By the middle of the next decade, regional powers may have acquired limited ability to directly interfere with in-orbit systems. Regional powers may acquire the means to temporarily disrupt, jam or dazzle satellites in low earth orbit using ground-based emitters; they are able to procure more threatening and tightly controlled nuclear and ballistic missile technologies today.[44] They are unlikely to be able to directly attack

on-orbit systems or substantially impact the operations of satellites in medium or high earth orbits. Depending on the capacity and capability of these dazzling systems, future Joint Force Commanders may find themselves with limited access to space derived intelligence, surveillance and reconnaissance products.

*International Non-State Actors.* International non-state actors, be they criminal or extremist in nature, will have the fewest capabilities to interfere with a future Joint Force Commander's access to space-based capabilities. By their very nature, non-state actors will have limited access to either commercial or friendly government space-based capabilities. This does not imply that non-state actors will be unable to access space, but rather that their use of space will be heavily channelized into commercially available products and capabilities.

Additionally, non-state actors will be unable to directly attack on-orbit satellites and their use of dazzling systems or terminal/receiver jamming will be judicious and a-periodic. By their nature, dazzlers and jammers emit distinctive, electro-magnetic signals which are subject to identification and tracking. Routine use of such systems would hamper the ability of criminal and extremist groups to effectively blend into their surroundings, denying them the sanctuary they require to plan and conduct operations.

These groups may develop the ability to conduct isolated kinetic attacks against our satellite control systems. A coordinated irregular or suicide attack may be able to reach, damage or destroy isolated portions of the control network. The opportunity cost of this type of "counter-force" operation by criminals or extremists would be contextually sensitive—the value of attacking more visible security apparatus or of generally

terrorizing the target population would likely provide a better “bang for the buck” than the destruction of an isolated military target.[45]

However, non-kinetic cyber attacks, even if they are harassing in nature, may be sufficient to reduce the Department of Defense’s and Joint Force Commanders’ confidence in the availability and accuracy of these systems for time-sensitive data transmission. If non-state actors use these attacks to deny the Joint Force the requisite confidence in and speed of data transmission required by time-sensitive targeting, they can effectively mask high value targets. This provides non-state actors an importance force-protection function. Additionally, to the extent these cyber attacks also reduce the Joint Force’s confidence in their data systems, these attacks sow fog and friction and may be seen as a force-enhancement operation by criminal and extremist groups. A Joint Force which lacks confidence in network and communications systems is less agile, providing time sanctuaries and surveillance gaps for non-state networks to exploit.

*High Altitude Nuclear Detonation.* As described above, near peer competitors, regional rowers and non-state actors may all have some ability to threaten or interfere with the Joint Force Commander’s access to space-based capabilities. However, up to this point the means by which potential adversaries might challenge or interfere with space-based capabilities have been in the traditional force-on-force (or cyber-on-cyber) role. There are other methods available to some actors which can have far reaching impacts. One of these wildcard scenarios would be the low-earth-orbit detonation of a nuclear weapon.[46]

Such a use of nuclear weapons is possible today by acknowledged nuclear powers. Technically, all near peer competitors and many regional powers will have the

requisite ability to launch a low yield nuclear weapon into low earth orbit.[47] Today's SCUD missiles have the reach and payload to elevate a nuclear weapon to the necessary altitude (roughly 100 miles) and relatively low throw-weights, such as the estimated 12 kilotons of India's nuclear tests, are required of the weapons themselves.[48]

Politically, this course of action may be thought to be feasible if the interests at stake are vital. International law and opinion are ambiguous with regard to the use of nuclear weapons in an exo-atmospheric explosion. The 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, better known as the Outer Space Treaty, bans signatories from orbiting nuclear weapons, not from allowing them to have weapons transit space, as in the case of a ballistic missile's payload, or from detonating weapons in this global commons.[49] The Comprehensive Test Ban Treaty, which prohibits all nuclear explosions, everywhere, for any reason, has not been ratified by the necessary states to come into force; the United States is such a hold out, having signed but not ratified the agreement.[50]

The political decision to use a nuclear weapon in such a manner, as an act of self-defense to ensure state survival, may not necessarily result in unacceptable international repercussions; it may be viewed as a "David versus Goliath" or "Poor versus Rich" gambit to enhance state security. It may not be desirable for the United States to respond to the destruction of military and civilian hardware in space with the use of nuclear weapons on Earth.[51]

The high altitude detonation of a low yield nuclear weapon would have immediate and sustained impacts for the Joint Force Commander. Satellites near the detonation

would be destroyed, but given the large volume encompassed by low altitude orbit, the number of satellites directly destroyed would be small, estimated at less than 5-percent of a given satellite constellation.[52] Such a detonation, however, would flood the low radiation belts with high levels of persistent radioactivity. Satellites in low earth orbit would likely fail within months of the explosion.[53] Additionally; replenishment or replacement of the satellites would not be possible until the radiation levels decrease, a process that could take over 6-months.[54]

Under such a scenario, the United States could lose significant organic intelligence, surveillance, reconnaissance and communications capacity. This loss of capacity would be particularly acute if a future opponent conducts such an activity "pre-hostilities," as a signal of resolve and intent. Early detonation of a nuclear weapon in low-earth-orbit would provide the necessary time to degrade larger numbers of satellites before major combat operations began, severely curtailing the United States' asymmetric space capability advantage.[55]

Many commercial systems the United States accesses to provide additive communications bandwidth, such as the COMSAT and Iridium constellations would also be destroyed. Thus not only would the Joint Force Commander go in partially blind, but his ability to move information--to include operating a large number of Unmanned Aerial Vehicles--would be severely curtailed.

Future Space Vulnerability Prioritization and Implications for the Department of Defense

By the mid 2020s, potential adversaries will have a host of means available to exploit the space environment and attempt to disrupt or deny United States' access to its space-based capabilities. The Department of Defense should consider these future adversarial lines of action as it moves forward with near-term capability and investment

decisions. Although considering the full range of activities designed to change Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities can produced more resilient capabilities, this discussion will focus on those capabilities requiring the most long-term investment, namely Materiel and Facilities.

The first set of vulnerabilities the Department of Defense should address belongs to the space-control network, which has been built as if it would never come under attack.[56,57] This system has potential physical and cyber vulnerabilities. Often, the number of physical facilities and locations from which the network can communicate with on-orbit spacecraft is limited, creating key bottlenecks that adversaries can attack or exploit. While most of these facilities are on sovereign United States soil, they can be subject to conventional, special operations, irregular or computer network attacks.[58] Successful attacks against the satellite control network offer potential adversaries their biggest chance to eliminate United States space capabilities.[59] Other points of vulnerability in the space-capability array can only produce localized, not systematic, effects.

The Department of Defense should consider adding resiliency to this system through the addition of redundant and potentially mobile control elements.[60] By increasing the number of locations that must be attacked, the Department would complicate future adversaries' ability to effect the entire network. Additionally, the Department may wish to consider additional security for existing facilities to improve their survivability against improvised explosive devices, guided artillery or (where appropriate) conventional ballistic missile attack. Finally the Department of Defense must continue ongoing efforts to inoculate this system from cyber attack.

The Department of Defense should next consider the ability to deny future adversaries access to space systems. In the past, the United States has maintained space superiority by using diplomacy to persuade other governments not to provide space capabilities and services to our opponents. In addition, it has been able to “buy up” commercially available imagery and communications bandwidth that may have been exploited by its enemies. This will not be possible against near peer competitors and may not be feasible against regional powers that cannot be internationally isolated.

Among these capabilities, the Department of Defense should consider kinetic and non-kinetic means to disrupt a future adversary’s satellite control system, or the communications systems through which they access neutral commercial services. As indicated above, this approach would enable the Joint Force Commander to completely excise space capabilities from the adversary’s order of battle. In addition, the Department of Defense should investigate fielding a spectrum of both satellite dazzlers/jammers and terminal/receiver jammers to disrupt the adversary’s use of space-based capabilities. These approaches in concert can effectively deny an adversary the use of space.

The development of satellite-killers (anti-satellite missiles, hunter killer satellites or high-powered directed-energy weapons) should be a low priority; most space-based capabilities will continue to derive from constellations of orbital systems, which would continue to function, albeit in a degraded state, if a handful of satellites were destroyed. Additionally, destroying satellites may not be feasible if they belong to a neutral party.

Finally, the Department of Defense should invest in satellite capability redundancy, which would improve the resilience of space-based capabilities with an eye

towards underwriting their availability to future Joint Force Commanders. The Department of Defense should consider over provisioning some intelligence, surveillance, reconnaissance and communications capabilities with the intent of being able to rapidly restore the desired effects in the event satellite systems are unavailable, disrupted or destroyed. This could include the procurement and launching of spare satellite systems, as has been done with the Global Positioning System. It could also return to the practice of procuring and storing (terrestrially) spare satellites and launch capacity against a future need. Recently, the commander of United States Strategic command, General Kevin P. Chilton, bemoaned the fact that current acquisition practice does not provision additional satellites against their potential need.[61] The Department of Defense must balance the high cost of procuring spare satellites against the risk that they may be necessary.

Another way the Department of Defense can offset the loss of assured access to satellite systems would be to develop and deploy aircraft or airship systems designed to "gap fill" for a shortfall in intelligence gathering and communications. For example, the political repercussions of a near-peer confrontation could give pause to nominally neutral satellite communications companies. The United States and its adversaries could find themselves unable to buy the additional bandwidth high-tempo operations require. The wild card scenario could wipe out entire constellations and effectively block the launching of spare satellites. However, series of high altitude aircraft or airships could provide some of the capabilities a Joint Force Commander requires.

A "daisy chain" of line-of sight communications linkages may enable the Joint Force Commander to continue the high bandwidth operations (such as using

intelligence gathering Unmanned Aerial Vehicles) to which he has become accustomed. Formations of these systems, together with surface terminals could mitigate the loss of key space capability and enable high priority functions to continue. The Department of Defense must carefully consider if some portion of these redundant capabilities can and should be provided by autonomous manned systems.

Many other materiel and facilities solutions may emerge to protect the Joint Force Commander's unfettered access to space-based capabilities. However, the three highlighted above address both areas of significant vulnerability and capabilities which will require time, study and a significant commitment of resources to enact. These are the lines of inquiry and development which offer significant protection of our asymmetric space advantage.

## Conclusion

This essay began with the proposition that potential threats could emerge in the mid 2020s which might threaten both United States' ability to maintain space superiority and a Joint Force Commander's uninterrupted access to space-based capabilities. It examined the potential capabilities of three hypothetical future adversaries, a Near Peer, a Regional Power and a non-state actor, to utilize space capabilities for their own advantage while disrupting or denying a future Joint Force Commander's access to the same.

When considering these adversaries, including their potential use of nuclear weapons to destroy satellite constellations in low earth orbit, it identified three critical areas of vulnerability the Department of Defense should consider. These are vulnerabilities of the satellite control network, capabilities designed to disrupt or deny a competitor's use of space capabilities, and the need to provide some redundancy in

intelligence, surveillance, reconnaissance and communications capability in the event access to satellites is interrupted. These three vulnerabilities and actions the Department of Defense may undertake to mitigate them represent a useful starting point when considering capability strategies designed to assure United States space superiority in future decades.

Endnotes

[1] "US Using Space Supremacy To Wage Combat In Iraq And Afghanistan," Defense Talk, http://www.defencetalk.com/us-using-space-supremacy-to-wage-combat-in-iraq-and-afghanistan-6965/ (Accessed 5 Feb 2010).

[2] Michael D. Griffin, "Seeking the Right Stuff," National Aeronautics and Space Administration, 14 Sep 2008, http://www.nasa.gov/pdf/275133main_Seeking-the-Right-Stuff-14-Sep-08.pdf , (Accessed 5 Feb 2010).

[3] Commission to Address United States National Space Management and Organization, *Report Pursuant to Public law 106-65* (Washington DC, 11 January 2001), viii.

[4] Unified Command Plan

[5] JP 3-14, p II-1

[6] Tamar A. Mehuron ed, "2009 Space Almanac," Air Force Magazine vol 92, no 8, (August 2009), 61-65.

[7] Ibid.

[8] Andrea Maléter and Chad Frappier, "BRIEFING: DoD SatCom: Supply And Demand," MILSATMAGAZINE, (Satnews Publishers, Sonoma: CA, September 2008), 24.

[9] United States General Accounting Office, *Satellite Communications: Strategic Approach Needed for DOD's Procurement of Commercial Satellite Bandwidth* (Washington, DC: U.S. General Accounting Office, December 2003), 2.

[10] *Iridium Everywhere*, http://www.iridium.com/about/globalnetwork.php (accessed Feb 9, 2010).

[11] *The Future: Galileo*, http://www.esa.int/esaNA/GGGMX650NDC_galileo_0.html (accessed February 8, 2010).

[12]JP 3-14, p II-1

[13] Ibid.

[14] Ibid.

[15] The Commission to Address United States National Space Management and Organization adresses three of these vulnerabilities, 17.

[16] United States Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: Joint Staff, 12 April 2001 as ammended 31 October 2009), 502

[17] Ibid.

[18] Brian Garino and Jane Gibson, "Space System Threats," in *AU-18 Space Primer* (Maxwell AFB AL: Air University Press, September 2009) 275.

[19] Stephen Trimble, "In Iraq, GPS Is Surviving Jamming Threat, Pentagon Says," *Aerospace Daily and Defense Report* (25 March 2003), http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=aerospacedaily&id=news/gps.xml , (Accessed 11 Feb 2009).

[20] Tom Wilson, "Threats to United States Space Capabilities," prepared for the Commission to Assess US National Security Space Management and Organization, http://www.fas.org/spp/eprint/article05.html#10 (accessed 11 May 2009).

[21] John Markov, "Before the Gunfire, CyberAttacks," *The New York Times*, 12 August 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html, (Accessed 11 Feb 2010).

[22] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian,* 17 May 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia, (Accessed 10 February 2010).

[23] Garino and Gibson, "Space System Threats," 273-274.

[24] Bob Preston and John Baker, "Space Challenges," in *United States Air and Space Power in the 21st Century,* (Santa Monica CA: RAND, 2002), 169.

[25] Noah Shachtman, "Is this China's Anti-Satellite Laser Weapon Site," *Wired*, 3 November 2009, http://www.wired.com/dangerroom/2009/11/is-this-chinas-anti-satellite-laser-weapon-site/, (Accessed 10 Feb 2010).

[26] Thomas S. Szayna et al., *The Emergence of Peer Competitors,*(Sana Monica,CA: RAND, 2001), 7.

[27] Ibid, 11.

[28] For a description of how Iraq might have exploited access to space capabilities in Operation DESERT STORM, see Lambakis, Steven, "Space Control in Desert Storm and Beyond," *ORBIS*, 22 June 1995, http://www.accessmylibrary.com/article-1G1-17311154/space-control-desert-storm.html, (Accessed 10 Feb 2010).

[29] Theresa Hitchens, "Commercial Imagery: Benefits and Risks."

[30] Ibid.

[31] Doug Richardson, "GPS Proves Jam Resistant," *Armada International, Issue* 3, June/July 2003, http://www.armadainternational.com/03-3/article-full.cfm, (Accessed 10 Feb 2010).

[32] Andrea Maléter and Chad Frappier, "BRIEFING: DoD SatCom: Supply And Demand"

[33] Frank Vizard, "Safeguarding GPS," *Scientific American,* April 14, 2003 http://www.scientificamerican.com/article.cfm?id=safeguarding-gps, (Accessed 11 Feb 2010).

[34] Wikipedia, "Mark 82 Bomb," http://en.wikipedia.org/wiki/Mark_82_bomb and "Small Diameter Bomb," http://en.wikipedia.org/wiki/Small_Diameter_Bomb.

[35] JP3-14, II-4.

[36] Tom Wilson, "Threats to United States Space Capabilities."

[37] Garino and Gibson, "Space System Threats," 273-274.

[38] Marc Kaufman and Dafna Linzer, "China Shoots Down Satellite, Drawing Protests Worldwide," *Boston Globe*, 19 January 2007, http://www.boston.com/news/world/asia/articles/2007/01/19/china_shoots_down_satellite_drawing_protests_worldwide/ , (Accessed February 11, 2010).

[39] MSNBC.COM News Service, "Navy says missile smashed wayward satellite," http://www.msnbc.msn.com/id/23265613/, (Accessed 11 Feb 2010).

[40] Wikipedia, "ASM-135 ASAT," http://en.wikipedia.org/wiki/ASM-135_ASAT, (Accessed 12 Feb 2010).

[41] Noah Shachtman, "Is this China's Anti-Satellite Laser Weapon Site."

[42] Thomas O'Toole, "Soviets Test Hunter killer Satellite in Orbit," *Anchorage Daily News*,*vol XXXV*, No 95 April 18, 1980, http://news.google.com/newspapers?nid=1828&dat=9800419&id=R0EdAAAAIBAJ&sjid=ZacEAAAAIBAJ&pg=1158,3582911, (Accessed February 11, 2010).

[43] Tom Wilson, "Threats to United States Space Capabilities."

[44] Gertz, Bill, "N. Korea Sells Iran Missile Engines," The Washington Times, February 9, 2000, http://www.mail-archive.com/ctrl@listserv.aol.com/msg35458.html, (Accessed 18 Mar 2010).

[45] As discussed in Robert A. Pape, *Dying to Win*, (New York, NY: Random House Trade Publications, 2006), the purpose of terrorist actions is to inflict pain on societies, not necessarily to disrupt governments. Selecting isolated military targets, with low potential for collateral damage, is less effective than other targets with high collateral damage potential (or even the intentional selection of civilian targets.) See particularly Part I: The Strategic Logic of Suicide Terrorism.

[46] Garino and Gibson, “Space System Threats,” 279-280.

[47] Ibid.

[48] Carey Sublette, “What are the Real Yields of India’s Test,” 8 November 2001, http://nuclearweaponarchive.org/India/IndiaRealYields.html, (Accessed February 11, 2010).

[49] United Nations Office for Outer Space Affairs, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies,* January 1967, http://www.oosa.unvienna.org/oosa/SpaceLaw/outerspt.html , (Accessed 10 Feb 2010), 4.

[50] United Nations, *The Comprehensive Nuclear Test Ban Treaty,* September 10, 1996, http://www.state.gov/www/global/arms/treaties/ctb.html, (Accessed February 10, 2010).

[51] Defense Threat Reduction Agency, *High Altitude Nuclear Detonation Against Low Earth Orbit Satellites*, April 2001, http://www.fas.org/spp/military/program/asat/haleos.pdf (Accessed February 11, 2010), 27-28

[52] Ibid, 10.

[53] Garino and Gibson, “Space System Threats,” 280.

[54] Defense Threat Reduction Agency, *High Altitude Nuclear Detonation Against Low Earth Orbit Satellites*, 16.

[55] Ibid, 18.

[56] Adam J. Hebert, “Global Force Worries,” *Air Force Magazine, vol 93,* no. 1 (January 2010) 22.

[57] Tom Wilson, “Threats to United States Space Capabilities.”

[58] Garino and Gibson, “Space System Threats,” 273-274.

[59] Ibid.

[60] Tom Wilson, “Threats to United States Space Capabilities.”

[61] Kevin P. Chilton, quoted in Global Force Worries,” *Air Force Magazine, vol 93,* no. 1 (January 2010) 24.