TalKing SHOP

THE FUTURE OF WARFARE & IMPACT OF SPACE OPERATIONS

BY LTC ROBERT E. BERG

Tomorrow's War – Detection and Attribution

War has changed and continues to change over time. This is not to say that we throw out the old and forget the lessons of the past. Many principles remain the same and can be applied to new forms of warfare. What each warrior and leader tries to anticipate is what the next war will be like. With such knowledge, or anticipation of what is next, leaders can shape and plan for success in the next conflict.

Some of the "next" war is already taking place. As nations enter the world stage through expanded economic and diplomatic ties abroad, they inexorably link their success with the world community. The leading nations of the world are tied in globally. Major economies succeed, in large part, due to global ties. How do these nations come into conflict with each other?

Outright conventional warfare has a greater effect today in the damage caused to the economies of warring parties. Cost of supporting war is high. Cost of rebuilding our modern infrastructure, or theirs, is high. Losses are also due to the obvious and the more subtle economic interlinking between the warring parties. Adverse international opinion and diplomacy effects are additional impacts to consider.

What is actually happening? The leading nations of the world have been avoiding direct conventional conflict with each other. This follows the old mutually assured destruction concept from the Cold War. Large nations are adverse to the negative impact of conventional warfare with a peer nation. The global economy has put larger chips on the table. Additionally, the incentive for a nation to gain territory through warfare no longer exists as the global community maintains a static view of national territories.

I mentioned that we do not forget the lessons from the past. The Cold War had elements that are being seen today. When outright nation-on-nation conflict has potential for escalating to the unthinkable, other less-powerful means are sought to prosecute the desired effects. Aiding another nation in conflict with your enemy is one means. Espionage is another. Whenever a method is available where the actor can remain hidden, an advantage is achieved in being able to act with impunity. A favorite statement of mine is the old Soviet Union "categorically denying" involvement in some event or crisis. Today we see something similar with a fight being waged in the cyber domain.

We, the United States, have been under daily attack. These attacks may be security breaches in order to test defenses. They may be for purposes of gathering restricted information. They may at times seek to cause disruption, damage, and degradation of systems. The attacks are occurring in the cyber domain. Cyber domain aggressors have a great advantage; they can be difficult to identify. Even when cyber aggressors can be identified, their association with a nation, group, or industry can be difficult to attribute.

There is simple attribution and there is a higher level of attribution. Simple attribution is basic knowledge of connections

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE
2011

2. REPORT TYPE

3. DATES COVERED
00-00-2011 to 00-00-2011

4. TITLE AND SUBTITLE
The Future of Warfare & Impact of Space Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Space and Missile Defense Command/Army Strategic Forces Command,Future Warfare Center,1330 Inverness Drive, Suite 440, Colorado Springs,CO,80910

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

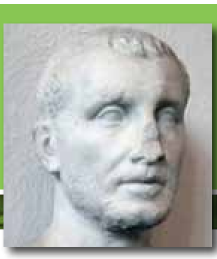
13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**4**	

Woodcut of Warfare Concepts



" We ought to live with things in advance, explained as a prefiguring of what is to happen."

- Posidenius, 135 – 51 B.C.

and likelihood that certain governing parties are responsible. Is the actor linked to commercial industry, a government, or an independent group? Simple attribution possibly can be used in efforts to counterattack and counterstrike via similar means. Higher level attribution is where the connection can be used on the world diplomatic stage. Is there evidence that the suspected group, to whom the actor is linked, is the responsible party? Higher level attribution is needed in order to take effective diplomatic action. For this reason, difficulty of attribution, cyber warfare is occurring as a preferred method of conflict between large players on the global stage.

Smaller players also are using the cyber domain to have impact on the battlefield. Sometimes the existing global network is used as a means of difficult-to-detect communication and coordination. Smaller players also have reasons to avoid conventional warfare and remain hidden. The American military is too strong to stand up to on a conventional basis. Like cyber warfare, small actors use other methods that are difficult to attribute.

"Actors too weak or too cautious to threaten NATO with overt conventional attack may employ jagged methods of assertion. This category of deterrable risk involves an unpredictable variety of pressures, constraints and challenges, sometimes anonymous, unattributable, uncertain or disputed… ."

–Paul Schulte, Strategic Insights, Volume VIII, Issue 4

In Iraq and Afghanistan, we have seen a common theme in the conflicts. Those who fight against us attempt to remain hidden. The individual who places an improvised explosive device attempts to engage us without exposure or identification. Those who aid the individual emplacing an IED do so with hidden networks of support. The IED is an anonymous weapon. Our difficulty in prosecuting such a fight is identification and attribution of those we are fighting against.

Large nations also have become more ethical in prosecuting a war. Collateral damage and civilian casualties have become of greater consequence. Even individual incidents not resulting in physical harm, such as took place in Abu Ghraib, have international impact. We can no longer bomb an entire city to take care of a problem. We cannot employ negative means against a populace. We must seek to target the individuals directly responsible. We must locate an enemy who is difficult to find. We must be able to attribute actions against us to those individuals we target.

The small player has something in common with the larger players in conflicts we are engaged in around the world. In both cases, they have reasons to use means that are anonymous and difficult to attribute. The IED is one such means. Other means include cyber warfare and disruption of Space-based intelligence, surveillance, reconnaissance and communications.

Other means of the future are likely to follow this theme of being difficult to detect and attribute. If we apply this thought to direct kinetic engagement, it is likely to be based on robotics. Already many nations have embraced unmanned aerial vehicles and are working toward ground-and water-based unmanned vehicles as well. As such technology becomes prevalent, it will become easier to use and more affordable for smaller players to use on a large scale. More importantly, as technology used in unmanned vehicles gains greater commercial availability, it will become more difficult to attribute. Physical stealth of unmanned systems and stealth in attribution have the potential to transform physical warfare methods and can be linked to nontraditional methods such as cyber warfare.

Both cyber warfare and insurgent use of IEDs depend upon difficulty in locating the actor and attributing those actions to a controlling cell or entity. Unattributable robotics is a natural progression for both. The prevalence of unmanned vehicles is likely to enable future warfare using unattributable robotics. Unmanned vehicles are leading in development of the technology necessary for this next step in progressive use of robotics. The large actor gains "plausible deniability," and the small actor remains difficult to locate. Some of these systems are being seen in development around the world such as power-line creeping robots, snake robots, and others in addition to the now common UAV. Robotics, like cyber warfare, is another way that the fight of the future can be waged in a difficult-to-attribute method.

What does all this mean for the military? For one thing, there are many players other than the military. Corporate organizations, state-run intelligence offices, political groups and others are in the cyber fight and will be able to step into other methods of fighting their battles while remaining hidden. Traditionally, militaries fight militaries or guerilla forces or insurgents. Now warfare is taking place on new battlefields with new objectives (yet linked to traditional goals). If a cyber attack targets a commercial corporation, does the corporation fight back or does a military force? There is likely a need for greater cooperation between the military, the commercial world, and the political and economic arms of the government as warfare progresses to operating primarily in new territories.

"A U.S. military response to espionage or crime would be a strange departure from international norms regarding the use of force. A retaliatory cyber attack (where the intention is to damage or to destroy, rather than exploit) or retaliation using a kinetic weapon for a cyber attack against countries that have not used force against us or against individuals with criminal rather than political aims, could easily be interpreted as an aggressive and unwarranted act by the international community. The result is to cast doubt on the credibility of a retaliatory threat, weakening any deterrent effect."

– James A. Lewis, Cross-Domain Deterrence and Credible Threats, July 2010

What are the primary keys in this fight of the future that we have begun to engage? Detection, location, and attribution are fundamental requirements that enable the fight to take place through targeting and effects. We are good at targeting, and we can create many useful effects. Effects on new battlegrounds such as in cyberspace are being pursued aggressively around the world. The great difficulty remains in detection, location, and attribution of the enemy. Primary keys in detecting, locating, and attributing can be found in cyber warfare methods and in Space-based assets. The military has stepped up to the plate in creating a U.S. Cyber Command and standing up service components to that command. Space-based capabilities also continue to be a growth field that is needed as a primary key for tomorrow's war.

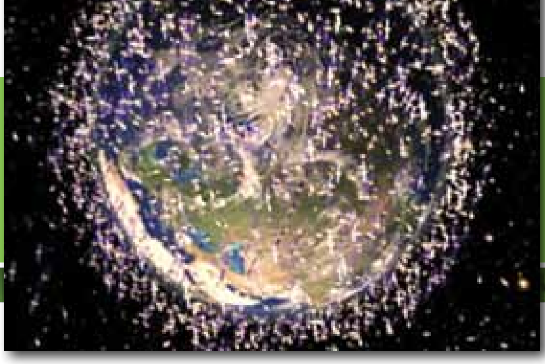
Space in Tomorrow's War

Military dependence on Space has grown tremendously. The peaceful nations and peoples of the world are also gaining greater dependence on Space. Soldiers rely on satellite-based navigation (as does the civilian populace of the modern world). Communications in remote regions are enabled through Space-based assets. Military timing is enabled through Space as are financial transactions around the world. Warning of missile threats, with such quickness to allow reaction in the scant time available, is possible through Space-based assets. We have many dependencies that have developed on Space and for good cause. Space-based assets provide keys in prosecuting the fight of the future.

Military planners are now adverse to any type of collateral damage; precision munitions are a key player in limiting collateral damage. These precision munitions are enabled through Space-based assets. The nature of ethical warfare has led in part to a dependence on Space for this precision. With a world integrated on a political and economic level, further refinement of what is ethical in warfare is likely to continue. Precision capabilities of weapon systems will likely remain a primary need in future conflicts.

Space enables our military in a way that greatly reduces the requirements for ground-and air-based systems and manpower. We hunt individuals and cells that do not show themselves as a regular, recognizable military. Space-based platforms can cover large areas in identifying, locating, and attributing. Space-based intelligence across the spectrum (such as signal, infrared, visible, radar, and multi-and hyper-spectral imaging) is a critical enabler in hunting the enemy. We see Space providing tipping and cueing in multiple areas. Without the tipping and cueing provided, the search would be intensive and likely often fail to produce timely results. Missile warning, geo-location, Joint Friendly Force Tracking, interference identification, Space situational awareness, and more are linked to intelligence requirements and situational awareness needs.

Moves are being made toward more automated analysis of Space platform data. Analysis by individuals only targets a focused area that has been identified as being of interest. Data fusion and correlation across multiple areas is time and manpower intensive unless it can be automated. Being without these Space and automated capabilities would require massive amounts of ground forces, a larger quantity of airborne platforms, and large numbers of analysts to meet the need. If we wish to continue to be capable in handling large landarea missions with small amounts of forces, the intelligence aspects provided by Space and automated analysis will continue to be critical.



Crowded Low Earth Orbit

What is the future conflict? We are partly in it. Our conventional forces cannot be matched by our typical opponents. There is a continuing integration of nations economically and politically on a global level. Those who are our peers avoid conventional conflict with the United States as do we do with them. Our enemies, and friendly competitors, resort to nonconventional means. Identifying and locating our targets (individuals, cells, sources, etc.) has become more difficult. Space has become a key player in target identification that cannot be supplemented without large increases in ground and air-based assets and associated manpower. Precision engagement is ethically critical and enabled by Space. We will likely continue to see the same difficulties and need for capabilities of Space-based assets in the future.

Across the full spectrum of operations such as major combat operations, humanitarian assistance, countering weapons of mass destruction proliferation, and homeland defense, the same Space-based capabilities provide needed intelligence or critical information about the situation. These operations are often likely to involve even fewer forces on the ground or limited ability to use airborne assets, leading to Space once again meeting the need.

With the great capability that Space provides, enemies will see our Space assets as key targets. The dependency on Space-based assets also creates a need to provide for the defense of these assets and their capabilities. There are antisatellite missiles, laser systems, and electromagnetic jamming threats to satellites on orbit. There are capabilities such as GPS jamming that deny a Space-based capability in a local terrestrial area. The possible threats are highly varied. So, what areas should be concentrated upon?

Looking back at the global integration of nations on an economic and political level, nations that have the capability to physically destroy an object in Space are likely to avoid such action. Space provides them capabilities at multiple levels that would harm their economic well-being if lost. For major nations, low earth orbiting satellites are easy targets. Attacking these targets is similar to the concept of mutually assured nuclear destruction in that we each hold the entire LEO belt hostage. The region is highly crowded with satellites and debris. A few destructive strikes could set off what is known as the Kessler Syndrome, a domino effect of destruction in Space caused by a chain reaction of millions of pieces of debris colliding with satellites at velocities faster than the fastest bullets. International repercussions are also likely as the world on a whole depends more and more upon satellite systems. For these reasons, nations are likely to endeavor to use effects that do not cause debris.

Such nondestructive effects are being seen today. International news sources last year reported Iranian jamming of BBC and Voice of America satellite broadcasts. The cost to conduct such jamming is minor compared to the high cost of a direct ascent antisatellite missile or an orbital platform that could cause disruption. Not only are individual unit costs low for ground-based systems that provide temporary and reversible effects, but those systems are also based on known technology with little to no development needed. An example of how low cost and simple satellite interference from the ground can be is exemplified in an individual case, John R. MacDougall, a.k.a. Captain Midnight, who jammed HBO broadcasts in 1986. These jamming effects are typically nondestructive and reversible, making them less likely to be of concern to the international community. The effects also can be difficult to identify, locate and attribute, creating opportunity for actors to operate with greater impunity. In future conflicts, of both limited and larger scale, we are likely to need strong capabilities to identify, locate and attribute temporary and reversible interference and disruption of our satellite systems.

Our dependence on Space has increased greatly as a military, as a nation and as a global community. The capabilities to identify, locate and attribute provided by Space are critical in prosecuting future wars. For ethical reasons, we rely on Space for precision engagements. Space provides navigation, tracking, communications and warning to the global community and the military. Conflict in Space is likely to follow the methods being used in cyber warfare in that the actors seek to remain hidden or difficult to positively attribute. Warfare in general is apparently moving in this direction of anonymity. Our nation must assess how these future global conflicts, economically and politically integrated with the world, will be fought. We as Space professionals do our part in attempting to foresee how Space will play a role.

LTC Berg works in the Directorate of Training and Doctrine with the U.S. Army Space and Missile Defense Command/Army Forces Strategic Command. His last assignment was at the Johns Hopkins University Applied Physics Laboratory where he worked on multiple projects, including a disruptive innovation team where he wrote a white paper on stealth robotics initially exploring some of the concepts in this article.