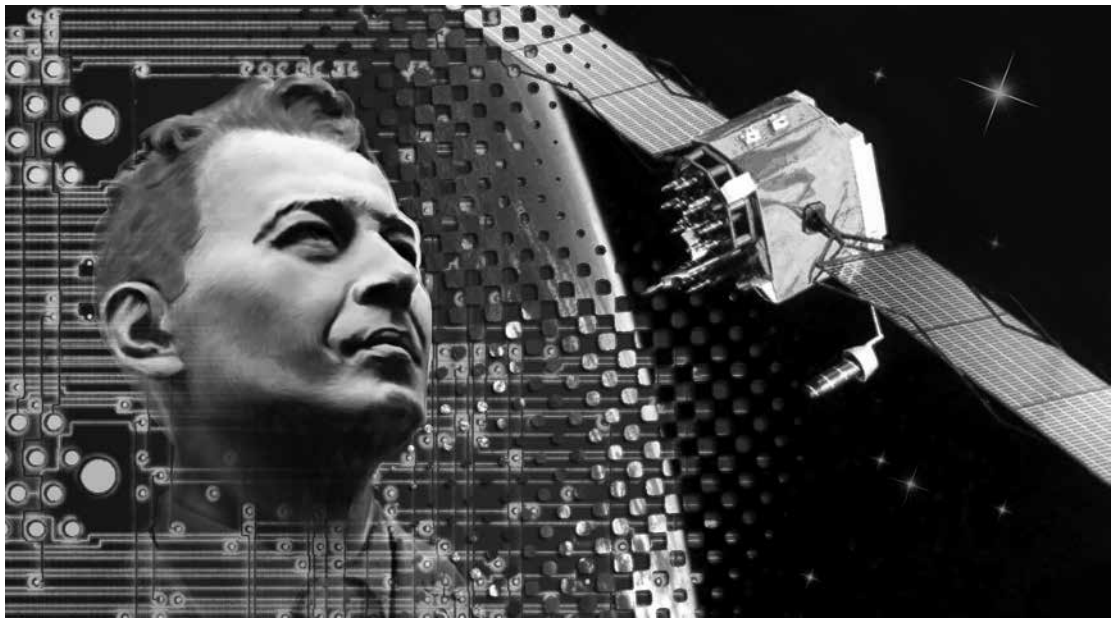


An Airman's Story

General John E. Hyten, USAF

Disclaimer: The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.



Every U.S. military operation across the planet, across the entire spectrum of conflict, depends on space and cyberspace to accomplish its mission. From humanitarian operations to full spectrum combat, our Joint force would not be as lethal or effective in the prosecution of our missions without space and cyberspace. They are perhaps the most joint of all the operational domains. All Services rely equally upon the capabilities delivered by, from and through these domains—but space, in particular, is an Airman's story. However, it is a story that Airmen, in general, don't tell particularly well. We should.

The Airman most associated with space is General Bernard Schriever. Most Airmen know him as the "Father of Air Force Space and Missiles." Schriever Air Force Base is named in his honor. He led the development of the ICBM as well as the CORONA satellite program in the late 1950s and early 1960s. Some know that then Major General Schriever was on the cover of *Time Magazine* in April of 1957 and in the



article discussed the future of space and missiles. Very few of us know that two months earlier, in February of 1957, he made the inaugural address to the Air Force Office of Scientific Research Astronautics Symposium in San Diego. In this address he stated:

In the long haul, our safety as a nation may depend upon our achieving “space superiority.” Several decades from now, the important battles may not be sea battles or air battles, but space battles, and we should be spending a certain fraction of our national resources to ensure that we do not lag in obtaining space supremacy. Besides the direct military importance of space, our prestige as world leaders might well dictate that we undertake lunar expeditions and even interplanetary flight when the appropriate technological advances have been made and the time is ripe.¹

It is most remarkable to realize that this great Airman was talking like this and leaning forward even before the launch of Sputnik in October of 1957—when the rest of the world thought the space race began. The race was already underway, and General Schriever was talking about it—leading our Air Force into the future—which leads to consider another visionary Airman and space leader: The 4th Air Force Chief of Staff, General Thomas D. White.

In 1958, shortly after Sputnik, General White coined the term “aerospace.” In early 1959, as he sat in front of a skeptical House committee to testify on the importance of space, General White used this word twelve times. He explained “Air and space comprise a single continuous operational field . . . there can be no operational boundary between them.”² It is important to note the words he chose. He did not try to claim that aerospace was a single physical domain—it was a continuous operational field—with no operational boundaries. Even in 1958, he was trying to focus the world on the operational effects that would be enabled and generated from and through space and that the power of the Air Force would be found in integrating and applying them together to create advantages over our adversaries. General White clearly understood the advantages space could bring to military operations.

Which then brings us to General Jerome (Jerry) O’Malley. In the late 1970s and early 1980s, as the Vice Chief of Staff of the Air Force, based on a belief the space domain had the potential to fundamentally change warfare and improve the ability of our Air Force to conduct operations, he became convinced of the need for the Air Force to establish a separate space command. Almost all space capabilities were highly classified at the time, and most warfighters were not even aware of the existence of military satellites in a variety of mission areas (weather, communications, intelligence-surveillance-reconnaissance (ISR), missile warning, etc.). He began pushing the AF leadership to create an operational command focused on using space capabilities to support the warfighter. He had the support of many others, but he was the driving force. His efforts eventually resulted in the creation of Air Force Space Command in 1982—and the operational focus of space in the military really began to accelerate.

Schriever, White, and O’Malley—three of the most important pioneers and legends of the space business in our Air Force. Most remember the role of General Schriever, but few remember the roles of General White and General O’Malley—but these three pioneers are responsible for much of what we have today and for the transformation of warfare from the industrial age to the information age. And what did they all have in common? They were not Aerospace Engineers. That field of study did

not even exist when they were in college, nor was term even created. They were not “space professionals” or even “space officers.” They were all aviators and, more importantly, they were Airmen—and that is why space, although incredibly Joint today, is an Airman’s story and a story every Airman should be able to tell. Most of us do not remember this legacy, but we need to study it and learn from it because new challenges are looming. We must prepare to respond to new threats in space—and in cyberspace—and we must ultimately ask ourselves, is cyberspace an Airman’s story as well?

Our Dependence on Contested Domains

At the time General White gave his testimony, there were only two countries remotely capable of placing a satellite in orbit: The United States and the Soviet Union. There were only a handful of man-made objects in space, all of which reentered the atmosphere in relatively short order. The number of threats to our space assets were minimal. As more countries have become space-faring nations, several, including the United States (Operation Starfish Prime, ASM-135 (F-15) program, SM-3) have demonstrated anti-satellite capabilities. Our perspective of space has changed from “safe haven” to “contested” and from “sanctuary” to “theater.”

All remotely piloted aircraft (RPA) depend on space systems, just one example of which is the Global Positioning System (GPS). Without GPS, the RPA does not have the ability to enter a theater, nor does the pilot have the ability to know its position. Beyond basic flight, the RPA operator would not be able to use precision weapons or perform ISR missions with confidence.

Degradation or denial of GPS would have worldwide civil implications as well. Civil aviation, Wall Street and the agricultural community are just a sample of organizations poised to suffer serious impacts if position, navigation and timing were not available. Senator Jeff Sessions of Alabama recently said “[Our adversaries] stand to undermine the space-enabled advantages our country has benefited from for nearly sixty years.”³ He was not just speaking about military capability; his perspective included civilian applications as well.

The cyberspace domain faces similar situations on a daily basis. Joint, worldwide military operations depend on information delivered by this domain—everything from F-35 helmets to loadmaster checklists and from special operations equipment to the software in the USS *Ford*, the Navy’s newest aircraft carrier. The information and data missions within cyberspace are vital to accomplishing Joint missions. Precision operations require the information not only be available and expedient but to be accurate as well. Anything from a simple power surge to a complex manipulation of data can render all decisions, from tactical to strategic, much less effective and questionable. Not coincidentally, civil aircraft, Wall Street and the agriculture community face the same dire impacts if civil cyberspace is unavailable as well. While these domains are very different, any disruption by an adversary has the same outcome on capability and mission effectiveness.

These dependencies create vulnerabilities, and thus create centers of gravity for potential adversaries to exploit. Joint Publication 5-0, *Joint Operation Planning*,



clearly states the Characteristics of Centers of Gravity (COG).⁴ Space and cyberspace fit every criteria, not only for our adversaries, but for the United States as well. Most telling is the characteristic “Can endanger one’s own COGs.”⁵ This has never been truer than with space and cyberspace. If the effectiveness of space and cyberspace operations were diminished, the effectiveness of the land, air and sea forces would all be diminished as well. For example, if an adversary ever denied us the ability to operate in space, the United States would be forced to use pre-space tactics to conduct land operations. Which begs the question: If we are not prepared to defend or oppose an adversary in the space or cyberspace domains, are we prepared to use a World War II mindset to win? World War II was fought using completely different doctrine and principles. If space and cyberspace were removed from today’s joint capabilities, the United States would need a mass of force to replace the precision, agile force the world has come to expect. The Department of Defense would require large global footprints to replace the agile expeditionary logistics we have come to rely on. Not all changes would occur at the tactical level. If space and cyberspace were removed from our Joint doctrine, commanders at all levels would be forced to regress to predictive assessments instead of using the conclusive analysis of intelligence we use today.

Whether you subscribe to Col John Warden’s “five-ring” model of strategic attack or the Clausewitz Center-Of-Gravity theory, the United States’ dependence on space and cyberspace is undeniable. The Department of Defense must protect these domains, not just for military superiority, but for the Nation’s diplomatic and economic Instruments of Power as well.

Air Force Space Command Is Changing to Meet Future Challenges

To each there comes in their lifetime a special moment when they are figuratively tapped on the shoulder and offered the chance to do a very special thing, unique to them and fitted to their talents. What a tragedy if that moment finds them unprepared or unqualified for that which could have been their finest hour.

—Sir Winston S. Churchill

As the Department of Defense realizes the dependencies and vulnerabilities of our space and cyberspace situations, there is a single indisputable fact: the Air Force and Air Force Space Command must adapt to meet and defeat these challenges.

Prior to space and cyberspace entering the battlefield, land commanders would require significant time prior to executing mass maneuver. It used to take hours or days for tactical warfighters to pass intelligence, relay damage assessments or request more forces. Now, space and cyberspace capabilities are used to facilitate the flow of information, empower faster decisions, and build knowledge of the theater for even the most tactical warfighter. A land commander can, within mere moments, coordinate precision maneuvers with concentrated firepower, and relay follow-up orders based on near-real-time feedback from the results. This can all happen while National decision-makers monitor the battle in near-real-time from the opposite

side of the globe. Space and cyberspace create accuracy, availability and speed for the warfighter, the likes of which the world has never seen before.

While the entire Joint force requires these capabilities, the Air Force needs to answer a single question: what does the Air Force need to do to ensure these capabilities are available if challenged by an adversary? The answer: the Air Force must build Airmen who are ready to respond effectively and in a timely manner in the space and cyberspace domains. The answer, while simple, requires deliberate planning and execution.

First, Air Force Space Command is building a robust architecture to gain complete situational awareness. Air Force Space Command is the oldest non-regional Major Command in the Air Force with the least operational domain awareness. This concept is basic to all warfare. This easily equates to awareness of the airspace. Compared to the space domain, Joint Combatant Commanders have a clear understanding of their airspace at all times. There are several layers of redundant systems to identify, distinguish and track friendly, civilian, or hostile aircraft. However, Air Force Space Command's Area of Responsibility (AOR) is 73 trillion cubic miles. The difficulties and complexities required to identify and track satellites are enormous. In addition, "we have to develop new space tactics and doctrines, to account for a contested space environment."⁶

The same can be said for the cyberspace domain. The world's first man-made operational domain is already known for its dependencies, but its vulnerabilities are not completely understood. The cyber breach of the Office of Personnel Management became public in June 2015, and it became one in a series of high-profile penetrations targeting valuable information. This is also a highly-contested domain. To drive home the point, the U.S. Army Cyber Command, in its website recruiting video, blatantly asks: "Are you ready to step onto the cyberspace battlefield?"⁷ Understanding what is over the next "cyberspace hill" requires Air Force Space Command to explore and gain awareness of the cyberspace domain. As we build deliberate cyberspace situational awareness, it is important to keep in mind the newness of this domain. Air Force Space Command is still appreciating the possibilities of this domain. As we shift our understanding, we must not fool ourselves. Deputy Secretary of Defense Bob Work points out that the "sanctuary . . . and the margin of technological superiority upon which we have become so accustomed to [in space and cyberspace] is steadily eroding."⁸ Adversarial aggression in these contested domains is being deterred and defended against every day.

Second, Air Force Space Command must fundamentally change the presentation of Forces to Combatant Commanders. This also requires a shift in the command and control of these forces, and how we train our forces. Air Force Space Command is currently developing the Space Mission Force, and portions of the Cyber Mission Force, to meet this need. Space and cyberspace professionals will be receiving specialized training to fluently understand our domain capabilities to respond to adversarial threats. This is absolutely congruent with Joint Publication 3-0, which requires this understanding for Joint Operations.⁹

Third, joint commanders must be aware of the complexities of the space and cyberspace domains, and the operations required for safety of flight and mission assurance. There is an absolute uniqueness to both space and cyberspace. Space and



cyberspace provide mission support to the joint fight, but they are domains and AORs as well. Space and cyberspace cannot be thought of in the context of a traditional “Area of Responsibility.” In a geographical AOR, the air, land and sea domains can be separated from those of another AOR. For example, aircraft flying in one AOR are of little concern to an AOR on the other side of the world. This is not true with space or cyberspace. The space, or cyber, domain of one AOR cannot be separated from that of another AOR. These two domains are inherently global. A satellite in orbit, friend or foe, is of equal concern for AORs around the world and cyber operations transit global networks continuously and at the speed of light. It is equally important to keep in mind the capabilities these domains provide directly influence the flow of information. Because of this, defending information, and preventing it from getting in the wrong hands, is a vital concern.

To be clear: “Space” and “Cyberspace” are not missions; they are unique operational domains in which global military operations and missions are performed. It is important to understand that space and cyberspace are operational domains to engage and defeat adversarial aggression, not simply support functions to enhance joint air, land and sea operations.

Strategic leverage derived from space and cyberspace capabilities has created a fundamental shift in the nature of warfare. No longer does the advantage lie with the largest military or the force with the largest arsenal. Nor does it lie with the biggest weapon or most defensible position. These can all be countered with the integration of space and cyberspace capabilities by delivering warfighting decision superiority across all military missions.

As such, before any possible conflict, commanders must understand how space and cyberspace assets in these two domains must be protected. The organization of space and cyberspace domains under one command is a natural placement. While some may argue against this construct, there is a simple, logical reason: space and cyberspace create the same effects for every mission.

Space and cyberspace support every one of the five Air Force Core Mission areas: (1) air and space superiority; (2) ISR; (3) rapid global mobility; (4) global strike; and (5) command and control. It is worth pointing out: every Air Force Core Mission will fail unless we maintain the freedom to operate and conduct missions in the space and cyberspace domains.

Air Force Space Command continues to build a defensible space and cyberspace enterprise as we restructure to build capabilities for United States Strategic Command and United States Cyber Command. While Joint Forces Air Component Commanders have been using this model for years, this construct requires a fundamental shift in thinking for the space and cyberspace domains. These two contested domains are facing threats, and in some cases attacks, every day.

No person, military or civilian, should ever want a war in space or cyberspace. However, if there is, our nation has the right to defend itself, and we must be ready. The United States has the inherent right to self-defense, and we need to be prepared to exercise that right at any time, if required.

Conclusion

It is no use saying, "We are doing our best." You have got to succeed in doing what is necessary.

—Sir Winston S. Churchill

To be prepared for War is one of the most effectual means of preserving peace.

—George Washington

Adversarial challenges within the space and cyberspace domains are not imminent; they are already here. The future of our space and cyberspace superiority depends on our actions today.

Our requirement to prepare for conflict is unavoidable. The Department of Defense's dependencies on space and cyberspace capabilities require our operators to win against adversaries in these contested domains.

The Department of Defense is reliant on the 24/7 availability of space and cyberspace. Space and cyberspace systems have given us a near-real-time capability to correlate information and data across all National Instruments of Power. Global space and cyberspace information provides the "nervous system" for our Air Force and the Joint Force. This gives our commanders and National leaders the decision superiority needed to preserve peace, which we must be prepared to defend. Air Force Space Command is committed to improving our situational awareness and operational mindsight in order to effectively control our AOR when needed so that we can continue to support joint missions worldwide. This is an Airman's responsibility—and an Airman's story. ✪

Notes

1. Maj Gen Bernard Schriever, "ICBM—A Step toward Space Conquest" (address to the Air Force Office of Scientific Research Astronautics Symposium, San Diego, 19 February 1957).
2. House, Gen Thomas D. White, Chief of Staff, USAF, *Testimony before the House Committee on Science and Astronautics, Missile Development, and Space Sciences*, 86th Cong., 1st sess., 3 February 1959.
3. Senator Jeff Sessions (R-AL) (opening statement in transcription of the Senate Armed Services Subcommittee on Strategic Forces hearing on military space programs, 29 April 2015, page 3), <http://www.armed-services.senate.gov/hearings/15-04-29-military-space-programs->
4. Joint Publication 5-0, *Joint Operation Planning*, 11 August 2011, III-23, fig. III-11, http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.
5. *Ibid.*
6. Deputy Secretary of Defense Bob Work (speech to the GEOINT Symposium 2015, Washington Convention Center, Washington, DC, 23 June 2015), <http://www.defense.gov/News/Speeches/Article/606685>.
7. "Army Cyber Protection Team," video, 4:11, US Army Cyber Command, accessed 27 August 2015, <http://www.arcyber.army.mil/index.html>.



8. Deputy Secretary of Defense Bob Work (speech to the China Aerospace Studies Institute, RAND Corporation, Arlington, VA, 22 June 2015), <http://www.defense.gov/News/Speeches/Article/606683>.

9. Joint Publication 3-0, *Joint Operations*, 11 August 2011, IV-5, fig. IV-2, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf.



General John E. Hyten, USAF

General Hyten (Bachelor's degree in engineering and applied sciences, Harvard University; Master of Business Administration degree, Auburn University) is Commander of Air Force Space Command, Peterson Air Force Base, Colorado. He is responsible for organizing, equipping, training and maintaining mission-ready space and cyberspace forces and capabilities for North American Aerospace Defense Command, U.S. Strategic Command and other combatant commands around the world. General Hyten oversees Air Force network operations; manages a global network of satellite command and control, communications, missile warning and space launch facilities; and is responsible for space system development and acquisition. He leads approximately 38,000 space and cyberspace professionals assigned to 134 locations worldwide.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

<http://www.airpower.au.af.mil>