Preparing for Multidomain Warfare

Lessons from Space/Cyber Operations

Maj Albert "AC" Harris III, USAF

America is under attack. The enemy has jammed signals from the Global Positioning System (GPS), limiting unmanned aerial vehicle support and precision air strikes. Satellites are blinded by ground-based lasers, preventing actionable intelligence on enemy maneuvers within denied areas and degrading threat warning capabilities. At home, cyber intrusion threatens America's critical infrastructure that supports satellite command and control (C2) and cripples in-theater satellite communications, putting deployed naval strike groups at risk. To complicate matters further, news outlets report on the attacks with information that defense officials know not to be true. Yet this misinformation sparks outrage from the American public and encourages hasty decisions by lawmakers. America is under attack, and all this happens without a single kinetic strike.

These events describe a potential scenario in the next Great War. How could America get to this point? For years, we have achieved national objectives through military operations other than war. Such activities were focused on nonstate actors like Al-Qaeda, Islamic State in Iraq and Syria (ISIS), and Al-Shabaab. Yet as war fighters integrate joint capabilities to defeat extremists, nation-states are learning from the success and failures not only of our military activities, but also those actions performed by our enemies. This makes them more capable in challenging American interests, and curtailing our war-fighting advantage.

How do we prepare our military to meet the challenges of this evolved adversary? In a 2017 letter to Airmen, General Goldfein stated that to counter this adversary, we must enhance multidomain C2.[1] He tasked Brig Gen B. Chance Saltzman, a space weapons officer, to lead Air Force efforts toward multidomain solutions. Since then, much progress was made, yet even with progress it is going to take time before we see significant change across the Air Force. To help speed the enhancement of multidomain C2, tactical leaders, such as those at or below squadron levels, should cultivate multidomain thinking in their units. Leaders at the tactical level should consider employing the following steps in shaping their environment for multidomain C2:

1. Know your domain, and know it well.
2. Identify and collaborate with tactical mission partners in other domains.

3. Train and exercise multidomain approaches.
4. Document lessons learned.
5. Apply multidomain lessons in agreements, plans, and tactics.

These transferable steps have helped enhance multidomain C2 at the tactical level. But before this discussion dives right into the five steps, I want to add context to their usefulness and review why multidomain C2 is the solution for preparing our nation for the next Great War.

Courtesy of Wayne Clark

Gen David L. Goldfein, USAF chief of staff, speaks at the February 2018 Air Warfare Symposium.

A Smarter Adversary Requires an Improved War-fighting Approach

President Donald J. Trump's first *National Security Strategy* reminds us that America "faces an extraordinarily dangerous world, filled with a wide range of threats that have intensified in recent years."[2] Whether a nation-state, an extremist group, or even a lone wolf, the enemy of today is smarter than ever before. As American national power evolves, our adversaries continue to challenge us in each of the diplomatic, informational, military, and economic sources. For example, on the economic front, extremists have learned that sustained threats against a nation can deter investors and disrupt productivity.[3] On the diplomatic and information fronts, noticeably absent from accords on cybersecurity and intellectual property rights, are those countries that are active in cybercrime and cyber espionage against the US.[4] On the military front, years of budget cuts and fiscal uncertainty have compli-

cated and impeded military solutions to these evolved threats.[5] Russia is using false information to influence elections around the world, hacking into American information systems, and violent extremists are using social media to promote their causes.[6] If we want to be successful in keeping the peace and be ready for the next Great War, our operational art must confront this smarter adversary using multidomain approaches.

Courtesy: Scott Ash

Gen John W. Raymond, Air Force Space Command (AFSPC) commander, testifies with the Secretary of the Air Force and Chief of Staff before the Senate Armed Services Subcommittee on 17 May 2017.

Multidomain approaches at the tactical level involves the lowest warfighting echelon taking advantage of secondary domains—land, sea, air, space, or cyber—to deliver effects more effectively across their primary domain. At the operational level of warfare, they will help provide a greater level of synergy, bolstering solutions to complex matters such as antiaccess and area-denial problems presented by Russian and Chinese military capabilities.[7] The Army called warfare that uses this approach "multi-domain battle," and suggests it enables the projection of "combat power from land, and into other domains to enable joint force freedom of action."[8] The Marine Corps also highlights the necessity of exploiting all domains, as doing so increases maneuvering capabilities and combat effects.[9] In concert, the Navy is exploring inno-

vative ways for employing land forces from other military branches to secure access to shared domains—particularly those within the Pacific area of responsibility.[10]

For Airmen, multidomain operations are by no means new to Air Force culture. Our service was born from airpower's promise of combat effects that could enable more effective maneuvers on battlefields ashore and combat areas at sea. Over the years, Airmen have studied ways to employ airpower in ways that it drives desired effects in other domains. Before World War II, Airmen at the Air Corps Tactical School developed theories for employing airpower that were key to defeating Hitler.[11] A little more than 40 years after we became an independent combat force, the Air Force developed an evolved operational strategy drawn from years of airpower experience, and employed a new strategic attack strategy during the first Gulf War.[12] Much of that strategy was a result of the theories offered by Col John Warden, who advocated an approach that visualized the enemy as a system, where simultaneous offensive fires (by combined arms) on various components delivered synergistic effects across the entire social and military system.

Courtesy of USAF

Air Force fighter aircraft fly over oil fields during Operation Desert Storm.

With this new strategy, the Gulf War became a watershed moment for airpower advocates. Not only did the air campaign validate the efficacy of modernized strategic attack, it is considered the first major conflict in which space played a vital role.[13] Under the leadership of Lt Gen Thomas S. Moorman Jr., AFSPC commander

at the time, space war fighters around the world proved that they knew their domain and delivered effects from space that made the success of strategic attack possible. During a 1991 presentation at an Air Force Association chapter in Minnesota, General Moorman proudly acknowledged that in Desert Storm, "space owned the battlefield. We had a robust on-orbit constellation and the inherent spacecraft flexibility to alter our operations to support specific needs of the terrestrial warfighter."[14] Although we demonstrated how multidomain employment of airpower can achieve strategic objectives in the first Gulf War, the Air Force continued to improve its ability to operate using multidomain approaches, driving even more operational successes as seen later in Operation Inherent Resolve.[15]

As the conflicts in Iraq and Afghanistan evolved, America's grand strategy pivoted toward Asia. Russia, China, North Korea, and others were keen observers of US military engagement in the Middle East and did not want to suffer the same fate. Their efforts to counter American military effectiveness seemed deceptively simple: deny America's ability to project power to the battlefield. However, we did not sit idly by and allow the adversary to prevail with such antiaccess/area denial strategies. When the Air Force and Navy experimented with air-sea battle, it improved our ability to employ airpower using multidomain approaches. Yet its inherent weakness was in the fact that the concept focused primarily on combat operations across the air and sea domains, rather than across air, space, cyber, land, and sea domains.[16] Nevertheless, experimenting with air-sea battle helped the services relearn the value of joint force integration, resulting in a "Joint Concept for Access and Maneuvering in the Global Common."[17]

As a service with significant responsibilities in three war-fighting domains (air, space, and cyber), Airmen play a vital role in this joint concept. However, we should not consider such concepts at just the operational and strategic levels, we must also consider them at tactical levels. To evolve airpower thinking toward multidomain solutions more effectively, Airmen should observe the lessons from natural multidomain packages, like those found in the space and cyber mission areas. After all, America's increasingly integrated joint fighting force relies heavily on the decision advantages and deep reach provided by the multidomain effects delivered through space and cyber capabilities. Almost 20 years ago Colonel Warden predicted, "Information will become a prominent, if not predominant, part of war to the extent that whole wars may well revolve around seizing or manipulating the enemy's datasphere."[18] As a key architect for the airpower strategy in the Gulf War, he also predicted that although information was not a prominent part of warfare at that time, it would be. He was right.

Today, space and cyber capabilities support every US military operation, providing significant combat and combat support effects that secure American interests around the world. Space and cyberspace capabilities are so integrated that they function as a multidomain package unseen and unappreciated by many until something interrupts the advantages they provide. The next Great War will likely involve extensive cyber campaigns and will likely extend into, or even start, in space. To be prepared, we should learn from space and cyber operations and use those lessons to shape the environment for multidomain C2.

General Goldfein receives a GPS mission brief from the 2nd Space Operations Squadron.

Tactical space operators enable multidomain solutions and help to assure joint operations worldwide. Tactical space operators located around the world command and control their assets in a way that enables the free flow of effects from their space systems. During Operation Iraqi Freedom, effects from communication satellites, such as the Mobile User Objective System, the Wideband Global Satellite Communications System, and the Military Strategic and Tactical Relay, were essential for effective military maneuvers on land, at sea, in the air, and provided the secure communications needed to coordinate synchronized tactical multidomain fires. Missile warning satellites, such as the Defense Support Program and the Space-Based Infrared System, offered a unique awareness of key areas. This afforded more time and space for decisions by commanders at all levels, and helped to counter Iraqi dictator Saddam Hussein's ability to conduct surprise movements. Even today, GPS helps guide American ships, aircraft, and troops to their objectives, and put the "smart" in smart munitions, enabling them to hit targets requiring high levels of precision. Data from signals intelligence and imagery satellites have the reach to fill critical intelligence gaps in denied areas that other air, sea, and land assets cannot observe without significant risk of interdiction or destruction.

Modern warfare has shown that a space capability, such as a satellite communications asset, can support tactical air control parties, provide links for armed unmanned aerial systems, facilitate in-flight retargeting of cruise missiles, enable rescue forces to talk to isolated personnel, and transmit sustainment instructions back to the US—all at the same time.[19] In short, a small crew of space operators on watch commanding and controlling a single space capability have simultaneously brought both combat and noncombat support effects to a range of military operations around the world. These war fighters have proven their operational prowess again and again. From delivering space effects against enemies during the first Gulf War to using space in the fight against the Islamic State, Airmen operating space assets continue to drive operational success in all war-fighting domains. As such, any enemy that wishes to defeat American's military might would likely target space capabilities.

Adversaries are aggressively seeking counterspace capabilities to limit US war-fighting advantage. America's adversaries see space as a key enabler of combat action and thus have invested in counterspace weapons to seize the initiative seemingly at an increasingly faster pace.[20] One does not have to look far for examples of this. China is expanding its intelligence, surveillance, and reconnaissance capabilities while concurrently developing systems that could be employed to curb such advantages.[21] In early 2017, a Chinese researcher was reportedly awarded a national prize for his work in high-power microwave technology, which could potentially be employed toward a wide range of enemy multidomain fires.[22] Russia's development of laser weapons and kinetic kill capabilities is also threatening, as such weapons may possibly be used to blind imagery satellites or destroy them altogether.[23] As long as space remains a key enabler for combat effects across multiple domains, our adversaries will continue to look for ways to counter our space capabilities. In the next Great War, one could assume that the enemy will attempt to disrupt America's war-fighting advantage through offensive cyberspace campaigns on systems that enable space operations.

Like tactical space operators, tactical cyberspace operators provide and enable vital effects that shape the nature of military activities in all domains. Tactical cyberspace operators deliver combat and combat support effects by leveraging physical or logical computer networks, or by leveraging cyber personas. In physical networks, cyber operators can target information technology (IT) components that make up the network. IT hardware stored on aircraft, ships, satellites and data processing centers, or in the palm of a Soldier's hand, can be key physical network targets that can be exploited through various technical means.[24] Within logical networks such as websites, SharePoint, or the "Cloud," cyber operators can maneuver across domains to deliver fires on selected targets. Offensive actions conducted in the logical network could render systems inaccessible, denying war planners and operators access to essential mission data and communications. Access points in the logical network can also be leveraged to target physical network systems, bringing down IT hardware and leaving a technology-dependent unit nonmission capable. Virtual identities, or cyber personas, can be targeted to gain access to the physical or logical IT layers. A stolen virtual identity can give an adversary access to

personal computer systems and personal information, or even to the target's physical work spaces.

With enemies poised to use cyberspace as the means to attack America, or challenge American interests, tactical cyber operators remain combat-ready. Although rarely discussed in the open, these war fighters have employed options to achieve national security objectives. They have monitored the cyber environment as Russia asserted aggression against Ukraine, and are working with other US government entities to defend the US homeland against cyber attacks from Russia, China, and other entities capable of malicious cyberspace behavior. [25]

Source: Defense Visual Information Distribution Service

Cyber Airmen in the 175th Cyberspace Operations Group

Adversaries see cyberspace as an effective means to challenge American interests. As cyber attacks on America become more frequent, one could wonder if the enemy is actually conducting live fire training events in preparation for attacks on more sensitive targets. For instance, when North Korea executed offensive cyber campaigns against Sony in 2014, it compromised more than 3,000 computers, 800 servers, and a huge amount of data, including the personal information of employees.[26] In another attack in May of 2017, the ransomware known as WannaCry infected hundreds of thousands of Microsoft Windows operating systems in more than 150 countries.[27] This particular attack targeted files, encrypted them, and held them hostage for money. In essence, this was a cyber equivalent of a worldwide

hostage crisis. Imagine if these attacks were on military capabilities or on the critical infrastructure of allied nations engaged as a coalition in armed conflict. Each offensive action reveals not just the civilian, but also the military threat, underscoring vulnerabilities of an IT-dependent interconnected society.

The nature in which cyber assures the space mission helps to highlight the efficacy of multidomain operations. In a February 2018 statement to the Senate Intelligence Committee, the director of national intelligence, Daniel Coats, confirmed that Russia and China are reforming military capabilities in a way to enable multidomain fires against US space systems.[28] With this, one could infer that Russia and China are considering offensive cyber tactics to disrupt space capabilities. This is a serious threat because although cyber attacks can threaten operations in all domains and in practically all aspects of society, the space domain is uniquely vulnerable to adverse effects on its cyber dependencies.[29] For instance, Soldiers, Sailors, Marines, and Airmen, once employed, have engaged in combat without the use of cyber capabilities. However, space operators have always leveraged cyber effects to deliver military success in, through, and from space. Satellites are useless without the cyberspace link that allows for the flow of data to and from them, or the processors that transform that data into meaningful information. Attacks on cyber systems could easily exploit the vulnerabilities of space activities, and could cause cascading events that limit the delivery of space effects, and reduce America's ability to meet its national security objectives.

We have seen evidence of this already. Between 2007–08, government officials suspected Chinese actors in hacking and taking control of two imagery satellites (National Aeronautics and Space Administration's Landsat-7 and Terra AM-1). During a congressional testimony, Dean Cheng stated that this incident, among others, suggests that the Chinese "are actively exploring vulnerabilities in space information systems."[30] Chinese actors are also suspected in hacking the National Oceanic and Atmospheric Administration's weather satellite in September 2014.[31] These are just a few of many incidents, and space and cyber Airmen are working hard to mitigate the apparent threat to defense systems.

Together, space and cyber operators provide vital advantages toward national security objectives. They make up an advantageous multidomain package and the enemy knows it. Actions by our adversaries suggest attempts to curb this advantage by challenging not only our space superiority, but our cyberspace superiority as well. The *2018 National Defense Strategy* says it best: "today every domain is contested—air, land, sea, space, and cyberspace."[32] As the enemy vigorously develops new capabilities to challenge US interests, their perceived emphases on being able to deliver multidomain fires illustrate America's need for strengthening multidomain C2.

Shaping the Environment for Multidomain Command and Control

Enhancing multidomain C2 requires deliberate action at the tactical level. At this level, planners and operators of one domain must have not only the skills to perform their own missions, but they must also understand how planners and operators of other domains assure or even challenge their mission accomplishment.

Building this knowledge at the lower levels can help enhance multidomain C2 at operational and strategic levels. Leaders at the tactical level should consider the following steps when shaping their environment for multidomain C2:

1. Know your domain, and know it well. To shape tactical environments for multidomain C2, we have to first know our domain and know it well. In any case, before one can consider synchronized tactical actions from multiple domains, we must first be experts in our primary domain. But this knowledge goes far beyond just job acumen. We have to recognize how our piece of the mission fits into the bigger fight. At the tactical level, we must understand how our actions enable operational objectives, and leaders must effectively communicate this understanding to those they lead. This helps Airmen be mentally ready to support units that operate in other domains.

Maj Hanif Flood talks with Air University (AU) about his experience in integrating space and cyber at the Space Symposium in Colorado Springs, Colorado, 18 April 2018.

For tactical space and cyber operators, they master their domain not only through local opportunities, but also through advanced education and training opportunities offered by the DOD, intelligence community, and various commercial vendors. For instance, within both the Advanced Space Operations School and the National Security Space Institute at Peterson AFB, Colorado, space operators learn how to better operate in their domain.[33] They also explore challenges and approaches toward space integration into joint operations at not just the tactical, but also at the operational and strategic levels. Within the Center for Cyberspace Research, cyber Airmen enhance their ability to, among other things, "plan, direct, and execute offensive and defensive cyberspace operations."[34] At AU, an increased focus on space, cyber, and multidomain C2 provides valuable training that is available to all Airmen, bolstering cross domain learning, and inquiry.[35]

2. Identify and collaborate with tactical mission partners in other domains. Tactical leaders should identify units with missions in opposite domains, and then collaborate to ascertain possible cross-domain synergies that may contribute toward multidomain mission success. At times, this may be evident as the mission of some tactical units is to provide support to another. However when evaluating cross-domain synergies, leaders should meticulously understand how actions in one domain have the potential to impact the mission of a unit operating in another, positively or negatively. Then, those leaders should develop mission assurance tactics that improve the probability of operational success. With these tactics in place, leaders will help underpin the building blocks for multidomain C2, extending options available to the operational or strategic-level commander's battle management responsibilities.

Tactical space and cyber units continue to evolve, with many now presented to combatant commanders in a way that better enables collaborative partnerships with tactical mission partners from other domains. Some partnerships have been improved, in part, due to the establishment of the Space and Cyber Mission Force. The 2012 establishment of the Cyber Mission Force (CMF) by United States Cyber Command (USCYBERCOM) was designed to improve the organization of cyber forces, and better address cyber threats to US interests.[36] Air Force efforts, such as the Cyber Squadron Initiative, complements CMF concepts, building tactical cyber mission defense teams to better protect and defend the delivery of air and space power.[37] On the one hand, the Space Mission Force (SMF), introduced by AFSPC in 2016, focuses on advanced training that better prepares space operators to execute space war-fighting missions.[38] The SMF also adjusts the presentation of space forces to combatant commanders, enabling improved integration of tactical space capabilities into joint war-fighting campaigns.[39]

Efforts within Joint Task Force Ares, a USCYBERCOM operation against the ISIS, can serve as excellent examples for how tactical units within the CMF use multidomain partnerships to enhance solutions at operational and strategic levels.[40] Like fires from other domains, cyber fires must be coordinated with not just stakeholders at the strategic and operational levels but with tactical mission partners as well.[41] After all, we do not want to conduct offensive cyber operations on enemy networks if friendly forces are using those networks to achieve desired effects.

Multidomain partnerships leveraged by tactical space forces have also enhanced solutions at operational and strategic levels. At Schriever AFB, Colorado, unique partnerships between space, cyber, and ground support units have improved space mission assurance, directly contributing toward combat, and noncombat support effects in theater.[42] These partnerships ensure that when deployed war planners reach back to the SMF, they receive tactical support from space experts ready to deliver space capabilities. For example, while US Central Command was planning air strikes against Syria after Bashar al-Assad once again deployed chemical weapons against his own citizens, war planners leveraged data provided by the SMF to develop space effects specifically designed to support the 14 April 2018 air strikes.[43] This example, along with efforts within the CMF, highlight the value of tactical multidomain collaboration and their impact on contributing toward strategic and operational successes.

3. Train and exercise multidomain approaches. Tactical leaders should conduct joint training and exercises to strengthen multidomain options. When conducting such activities, leaders must be careful not to focus solely on refining tactics that work. Some of the best lessons can be learned when we stress our ability to operate when the probability of mission failure is high or even certain. Quality exercises evaluate the most likely and most dangerous enemy courses of action that can complicate efforts to achieve the objective. In other words, tactical leaders must exercise their ability to fight through the adversary's multidomain fires and win.

Training and exercising multidomain approaches can be challenging. A notional enemy during an exercise can declare victory early in the scenario if it successfully conducts offensive cyberspace operations or offensive space control against key blue force capabilities. Imagine an air campaign without the precision, navigation, or timing from GPS satellites, the vital intelligence delivered by space capabilities, or without capabilities we take for granted, like our desktop computers, phones, and yes, even the lights. Yet those are the type of scenarios we need in our exercises. Fortunately, we are making progress with exercising multidomain approaches. For instance, space and cyber incorporation into Red Flag, marking a significant milestone in 2016 when then Col DeAnna Burt was the first nonrated wing commander (50th Space Wing) to be deployed for the exercise.[44]

Courtesy: David Salanitri

An Airman attempts to troubleshoot space systems on his F-16 Fighting Falcon during an exercise.

4. Document lessons learned. Building multidomain solutions to national security challenges takes careful observation, analysis, and then documentation of lessons learned. Yet documenting lessons from training and exercises are not enough; planners and operators must also learn from anomalies that drive maintenance actions or even maintenance actions that unfortunately drive anomalies. Sometimes the effects from those anomalies can mirror effects derived from adversary fires. Anomalies like this during peacetime operations can produce significant lessons that planners and operators can leverage for multidomain approaches during war.

Space and cyber units today are collaborating to better conduct multidomain operations. During my six years assigned at the National Reconnaissance Office (NRO), I witnessed the evolution of tactical space/cyber integration and had the honor of helping our airmen become better multidomain warriors. In a speech at the 34th Space Symposium, NRO Director Ms. Betty Sapp highlighted how partnerships with the Air Force allow touch points and opportunities like never before.[45] She echoed comments by General Goldfein and General Raymond by mentioning that our adversary is evolving, and we have to move fast and learn fast.[46] The increased focus on partnerships between tactical space and cyber units at the NRO and across AFSPC have produced valuable lessons that allow better employment of air and space power.[47]

5. Apply multidomain lessons in agreements, plans, and tactics. Leaders at the tactical level should apply multidomain lessons by codifying them into their local agreements, plans, and tactics. This is probably the most challenging step, as current operational needs tend to out-prioritize administrative functions, and typically the momentum for change has a short lifespan. However if we do not apply these lessons, we may jeopardize progress toward better tactical multidomain operations. We have to overcome the tendency to underprioritize this step, as application of such lessons can drive immediate improvements in multidomain efforts while the unit drives toward their mission.

Due in part to the fruitful collaboration between tactical space and cyber units across the NRO and AFSPC, these two space organizations have codified a series of strategic-level concepts of operations to better deliver on their respective missions in the national security space enterprise.[48] Those concepts, born from multidomain partnerships, exercises, wargames, and experiments involving tactical units, help shape environments for multidomain C2. With the Air Force driving toward multidomain concepts, Airmen, like those in AFSPC and those assigned to the NRO, have stepped up to validate the efficacy of multidomain operations, contributing extensively toward the projection of multidomain airpower.

For years, effects from both space and cyber have been recognized as force multipliers; now they are considered war-fighting domains on their own. The enemy understands that America's military success depend on both space and cyber capabilities and have taken steps to curb the advantages those capabilities provide. With these five steps, tactical leaders closest to the fight can cultivate a multidomain mindset within their unit and help speed the enhancement of multidomain C2.

Concluding Thoughts and Recommendations

Multidomain operations are the solution to maintaining America's war-fighting advantage, and enhancing the multidomain approach at the tactical level will help prepare military forces for the next Great War. The space/cyber package is a natural multidomain option, but to offset the enemy's attempts to curb America's military advantage, Airmen at the tactical level must cultivate multidomain C2 in their own environment. Yet effective multidomain C2 goes far beyond just delivering effects across the military domains. It includes exploiting the capabilities of all government, commercial, and foreign entities willing to support America's national security objectives.

Although enhancing multidomain C2 starts at the tactical level, we still need to innovate and look for ways to improve multidomain thinking and application at the operational and strategic levels. If we want our Airmen to be successful in conducting multidomain operations, then we also need to develop multidomain capability areas that better organize, train, and equip tactical leaders for a multidomain conflict. For example, within AFSPC, space warriors are advancing toward a Space Enterprise Vision, which seeks to exploit such capabilities to succeed in multidomain warfare. As key enablers, cyber warriors are contributing to that vision. AFSPC is certainly contributing toward developing multidomain Airmen, and according to their vision, we can only expect that contribution to increase. However, we can always benefit from additional efforts that contribute toward the multidomain vision of future air and space power. Tactical leaders at or below the squadron level are key to making that happen.

Lastly, although there is an increased focus by senior leaders on space and cyberspace superiority, including breaking off space into a separate service and the evolution of cyber squadrons, we cannot lose focus on challenges that may threaten progress toward enhancing multidomain C2. Shortages in the pilot, space, cyber, and other key communities are concerning, as this doesn't just mean there are less Airmen to sustain their career field, but it also limits opportunities to evolve into a multidomain war-fighting force. After all, Airmen will continue to play a vital role in the CMF, and if directed, could also help shape a new military service for the space mission.[49] Secretary of the Air Force Heather Wilson and General Goldfein are certainly the Airman's champions for these difficult issues, as evident in their many presentations to Congress.[50] However, we need our national leaders to act on their call and provide the vital resources air, space, and cyber forces will need to be a dominant multidomain war-fighting package.

While the adversary explores ways to conduct multidomain fires to undercut our war-fighting advantage, we must explore ways to enhance multidomain capabilities. Without this, America will be at risk of strategic paralysis when confronted with widespread conflict. The five steps indicated above can help tactical leaders build a multidomain mindset to bolster multidomain C2, and help ensure America is prepared for the next Great War. ✪

Notes

1. Gen Dave L. Goldfein, "CSAF Focus Area: Enhancing Multi-Domain Command and Control. . . Tying it All Together," March 2017, http://www.af.mil/Portals/1/documents/csaf/letter3/CSAF_Focus_Area
_CoverPage.pdf.

2. White House, *National Security Strategy of the United States of America*, 18 December 2017, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

3. Subhayu Bandyopadhyay, Todd Sandler, and Javed Younas, "The Toll of Terrorism," *Finance & Development* 52, no. 2 (June 2015): 26–28, http://www.imf.org/external/pubs/ft/fandd/2015/06/bandyopa.htm.

4. G7 2017 Italia, "G7 Declaration on Responsible States Behavior in Cyberspace," accessed 29 April 2018, http://www.esteri.it/mae/resource/doc/2017/04/declaration_on_cyberspace.pdf.

5. Frederico Bartels, "Continuing Resolutions Invariably Harm National Defense," The Heritage Foundation, 21 February 2018, https://www.heritage.org/defense/report/continuing-resolutions-invariably-harm-national-defense.

6. Department of Homeland Security and Federal Bureau of Investigation, "GRIZZLY STEPPE—Russian Malicious Cyber Activity," 29 December 2016, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY STEPPE-2016-1229.pdf; and Jarred Prier, "Commanding the Trend: Social Media as Information Warfare," *Strategic Studies Quarterly* 11, no. 4 (2017).

7. Jeffrey M. Reilly, "Multidomain Operations," *Air & Space Power Journal* (*ASPJ*) 30, no. 1 (Spring 2016), 61–73, http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-30_Issue-1/V-Reilly.pdf.

8. Gen David G. Perkins, USA, *Multi-domain Battle: Joint Combined Arms Concept for the 21st Century*, Department of the Army, 14 November 2016, https://www.ausa.org/articles/multi-domain-battle-joint-combined-arms.

9. Department of the Navy, *The Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century* (Washington, DC: Headquarters US Marine Corps, September 2016), http://www.mcwl.marines.mil/Portals/34/Images/MarineCorpsOperatingConceptSept2016.pdf?ver=2016-12-02-073359-207.

10. Adm Harry Harris, "Role of Land Forces in Ensuring Access to Shared Domains" (speech, Association of the US Army Land Forces of the Pacific Symposium, Sheraton Waikiki, Honolulu, HI, 25 May 2016), http://www.pacom.mil/Media/Speeches-Testimony/Article/781889/lanpac-symposium-2016-role-of-land-forces-in-ensuring-access-to-shared-domains.

11. *ASPJ* staff, "Air War Plans Division 1: The Air Plan That Defeated Hitler," *ASPJ* 17, no. 1 (Spring 2003), http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-17_Issue-1-4/spr03.pdf.

12. Department of the Air Force, *Air Force Doctrine 3 Annex 3-70: Strategic Attack*, 25 May 2017, http://www.doctrine.af.mil/Doctrine-Annexes/Annex-3-70-Strategic-Attack/.

13. Peter Anson and Dennis Cummings, "The First Space War: The Contribution of Satellites to the Gulf War," *The RUSI Journal* 136, no. 4 (December 1991), doi:10.1080/03071849108445553.

14. As cited by David Spires, *Beyond Horizons: a Half Century of Air Force Space Leadership* (Maxwell AFB, AL: Air University Press, 2002), 260.

15. Joe Pappalardo, "How a Syrian Airstrike Got Help from Space," *Popular Mechanics*, 24 April 2018, https://www.popularmechanics.com/military/weapons/a19980968/syrian-airstrike-from-space/.

16. Department of Defense (DOD), *Air-Sea Battle Office. Air Sea Battle: Service Collaboration to Address Anti-Access and Area Denial Challenges* (Washington, DC: DOD, May 2013), http://navylive.dodlive.mil/files/2013/06/ASB-26-June-2013.pdf.

17. Michael E. Hutchens, William D. Dries, Jason C. Perdew, Vincent D. Bryant, and Kerry E. Moores, "Joint Concept for Access and Maneuver in the Global Commons: A New Joint Operational Concept," *Joint Force Quarterly* 84 (January 2017): 134–39, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-84/jfq-84_134-139_Hutchens-et-al.pdf?ver=2017-01-27-091816-550.

18. Barry R. Schneider and Lawrence E. Grinter, *Battlefield of the Future: 21st Century Warfare Issues* (Honolulu, HI: University Press of the Pacific, 2002), 104.

19. "Raytheon: Tomahawk Cruise Missile," Raytheon: Customer Success Is Our Mission," accessed 14 March 2018, https://www.raytheon.com/capabilities/products/tomahawk.

20. Daniel Coats, *Worldwide Threat Assessment of the US Intelligence Community* (testimony, US Senate Select Committee on Intelligence, 115th Congr., Washington, DC, 11 May 2017), https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf.

21. Kevin Pollpeter, "The US-China Reconnaissance-Strike Competition: Anti-Ship Missiles, Space, and Counterspace," Institute on Global Conflict and Cooperation, University of California–San Diego, 28 February 2017, http://escholarship.org/uc/item/4s99s9rs.

22. Elsa Kania, "The PLA's Potential Breakthrough in High-Power Microwave Weapons," *The Diplomat*, 11 March 2017, http://thediplomat.com/2017/03/the-plas-potential-breakthrough-in-high-power-microwave-weapons/.

23. Cheryl Pellerin, "Hyten: Deterrence in Space Means No War Will be Fought There," DOD, 26 January 2017, https://www.defense.gov/News/Article/Article/1061833/hyten-deterrence-in-space-means-no-war-will-be-fought-there.

24. Joint Publication 3-12(R), *Cyberspace Operations*, 5 February 2013, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf.

25. Adm Michael S. Rogers, *Hearings before the Committee on Armed Services*, (statement, 115th Cong., Washington, DC, 27 February 2018), https://www.armed-services.senate.gov/imo/media/doc/Rogers_02-27-18.pdf.

26. Steve Kroft, "The Attack on Sony," *CBS News*, 12 April 2015, http://www.cbsnews.com/amp/news/north-korean-cyberattack-on-sony-60-minutes/.

27. "Alert (TA17–132A) Indicators Associated with WannaCry Ransomware," US Computer Emergency Readiness Team, 19 May 2017, https://www.us-cert.gov/ncas/alerts/TA17-132A.

28. Daniel Coats, *Worldwide Threat Assessment of the US Intelligence Community* (testimony, US Senate Select Committee on Intelligence, 115th Cong., Washington, DC, 13 February 2018), https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

29. Chris Babcock, "Preparing for the Cyber Battleground of the Future," *ASPJ* 29, no. 6 (Winter 2015): 61–74, http://www.airuniversity.af.mil/ASPJ/Display/Article/1152264/volume-29-issue-6-nov-dec-2015/.

30. *Information Dominance: The Importance of Information and Outer Space in Chinese Thinking*, testimony to the House Foreign Affairs Committee, 115th Cong., 3 January 2017 (statement of Dean Cheng), http://docs.house.gov/meetings/FA/FA05/20170426/105885/HHRG-115-FA05-Wstate-ChengD-20170426.pdf.

31. Mary Flaherty, Jason Samenow, and Lisa Rein, "Chinese Hack U.S. Weather Systems, Satellite Network," *Washington Post*, 12 November 2014, https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html?utm_term=.16f8a19c9b62.

32. DOD, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: DOD, 2018), https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf; and "Report to the Commission to Assess United States National Security Space Management and Organization," Defense Technical Information Center, 11 January 2001, http://www.dtic.mil/docs/citations/ADA404328.

33. National Security Space Institute, "Educating and Inspiring Visionary Space Leaders of Today and Tomorrow," accessed 27 April 2018, https://www2.peterson.af.mil/nssi/public/.

34. Air Force Institute of Technology School of Strategic Force Studies, "Cyberspace 200 Fact Sheet," 19 July 2016, http://www.afit.edu/images/pics/file/Cyberspace%20200%20Fact%20Sheet%20new.doc.

35. Gen David L. Goldfein (speech, 34th Space Symposium, The Broadmoor, Colorado Springs, CO, 17 April 2018).

36. DOD, *The DOD Cyber Strategy* (Washington, DC: DOD, April 2015), https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

37. DOD, "Cyber Squadron Enabling Concept," 15 March 2018.

38. "Details of Space Mission Force Now Available from AF Space Command," Air Force Space Command, 15 July 2016, http://www.afspc.af.mil/News/Article-Display/Article/841797/details-of-space-mission-force-now-available-from-af-space-command/.

39. Ibid.

40. "FOIA 17-023, 17-033, 17-064—USCYBERCOM Joint Task Force," US Strategic Command, 19 April 2017, http://www.stratcom.mil/Portals/8/Documents/FOIA/FOIA%2017-023,%2017-033,%2017-064%20-%20USCYBERCOM%20Joint%20Task%20Force%20Areas.pdf?ver=2017-04-19-111941-797.

41. Mark Pomerleau, "How Can Cyber Contribute to Multi-Domain Battle?" *Fifth Domain*, 22 August 2017, https://www.fifthdomain.com/home/2016/12/15/how-can-cyber-contribute-to-multi-domain-battle/.

42. 2nd Lt Scarlett Rodriguez, "Wing CC Praises Execution of First-Ever Ops," Schriever AFB, CO, 5 March 2018, http://www.schriever.af.mil/News/Article-Display/Article/1458091/wing-cc-praises-execution-of-first-ever-ops/.

43. Pappalardo, "How a Syrian Airstrike," *Popular Mechanics*.

44. Brick Eisel, "Space & Cyber at Red Flag," *Air Force Magazine,* September 2017, http://www.airforcemag.com/MagazineArchive/Pages/2017/September 2017/Space--Cyber-at-Red-Flag.aspx.

45. Betty Sapp (speech, 34th Space Symposium, The Broadmoor, Colorado Springs, CO, 17 April 2018).

46. Ibid.

47. Gen Dave L. Goldfein, Gen John Raymond, and Betty Sapp (speeches, 34th Space Symposium, The Broadmoor, Colorado Springs, CO, 17 April 2018).

48. Gen John Raymond and Betty Sapp (speeches, 34th Space Symposium, The Broadmoor, Colorado Springs, CO, 17 April 2018); and Gen Raymond (speech, Air Force Association Multi-Domain Command and Control Conference, Colorado Springs, CO, 14 August, 2017).

49. President Donald J. Trump, "Remarks by President Trump at a Meeting with the National Space Council and Signing of Space Policy Directive-3," (statement, White House, 18 June 2018), https://www.whitehouse.gov/briefings-statements/remarks-president-trump-meeting-national-space-council-signing-space-policy directive-3/.

50. Dr. Heather Wilson and Gen David L. Goldfein, "USAF Posture Statement Fiscal Year 2019," (presentation, Committees and Subcommittees of the US Senate and the House of Representatives, Washington, DC, 14 March 2018), http://www.af.mil/Portals/1/documents/1/FY19_AF_POSTURE_STATEMENT_HIGH_RES.PDF; Dr. Wilson, Gen Goldfein, Gen John Raymond, and Lt Gen Samuel Greaves, "Military Space Policy" (presentation, Subcommittee on Strategic Forces US Senate, Washington, DC, 17 May 2017) https://www.armed-services.senate.gov/imo/media/doc/Wilson-Goldfein-Raymond-Greaves_05-17-17.pdf.

Maj Albert "AC" Harris III, USAF

Major Harris (BA, University of Kentucky; MSIR, Troy University; DPA, Capella University) is an action officer at Headquarters Air Force Space Command, Peterson AFB, Colorado. Before his current assignment, he was the operations officer for the Communications Operations Squadron—East, delivering cyber mission assurance in support of satellite intelligence missions. Commissioned in 2004, Major Harris is a multidomain leader who focuses his efforts on integrating space, cyber, and intelligence capabilities to meet national security objectives. His previous assignments include intercontinental ballistic missiles, joint space operations, and joint planning and exercises.