16th Air Force and Convergence for the Information War

Lieutenant General Timothy D. Haugh
Lieutenant Colonel Nicholas J. Hall
Major Eugene H. Fan

The world has changed, and our approach to warfare must change with it. As traditional organized power structures erode, disorder fills the void. We are moving from successive regional conflicts to a future characterized by continual global competition. This circumstance will reward those who can leverage information for strategic advantage. The 2018 National Defense Strategy (NDS) described this new paradigm by emphasizing the need to compete with adversaries now.[1] The Air Force recognizes that we are already in competition below the threshold of armed conflict. Within the Air Force, the standup of 16th Air Force as an Information Warfare (IW) Numbered Air Force (NAF) in October 2019 represents a direct response to this new reality. In the document directing the standup, the Air Force described IW as "The employment of military capabilities in and through the information environment to deliberately affect adversary human and system behavior."[2] Our task is to synchronize – Cyberspace; Intelligence, Surveillance, and Reconnaissance (ISR); Electromagnetic Warfare (EW); Information Operations (IO) – across the continuum of cooperation, competition, and conflict, and support the joint force's ability to compete, deter, and win wars across multiple domains.[3]

Within the 16th Air Force, IO describes a collection of activities to include Military Information Support Operations (MISO), Military Deception (MILDEC), Operations Security (OPSEC), and Audience Engagement. We intend to synchronize all 16th Air Force capabilities and activities through a unifying approach of convergence. We define convergence as *the integration of capabilities that leverage access to data across separate functions in a way that both improves the effectiveness of each functional capability and creates new information warfare outcomes*. This builds on the U.S. Army concept of convergence that focuses on enabling tactical multi-domain effects during combat, by emphasizing competition and synchronizing effects in the information environment. In this article, we describe

Lt Gen Timothy D. Haugh is the Commander, Sixteenth Air Force, Commander, Air Forces Cyber, and Commander, Joint Force Headquarters-Cyber, Joint Base San Antonio-Lackland, Texas. Lt Gen Haugh is responsible for more than 44,000 personnel conducting worldwide operations. The general leads the global information warfare activities spanning cyberspace operations, intelligence, targeting, and weather for nine wings, one technical center, and an operations center. Previously, he was Commander of the Cyber National Mission Force, where he coordinated the prevention and response to cyber incidents and campaigns perpetuated by threat actors in order to preserve U.S. critical infrastructure and key resources. Lt Gen Haugh is a graduate of Lehigh University in Bethlehem, Pennsylvania, and holds Master's degrees from Southern Methodist University, Naval Postgraduate School, and the Industrial College of the Armed Forces.

how competition in the 21st-century necessitates a change in our approach to warfighting. Next, we discuss why 16th Air Force was stood up in response to this change and our approach to IW. Finally, we introduce the concept of convergence as a framework for how to compete in the information environment on a flexible but global scale.

COMPETITION AND THE RESULTING IMPERATIVE

Our adversaries have brought strategic competition to the nation's front door by engaging the United States' (US) population in the information environment. Russia and China have sought to create distrust in the US and allied political, military, and economic institutions and processes. Our adversaries' goal is to degrade political will or to generate internal conflict, while creating the plausible deniability necessary to avoid international responsibility.[4] As state and non-state actors rapidly evolve IW capabilities to control the narrative surrounding their actions, they are redefining what "combined arms" means in 21st-century warfare.[5]

In 2016, Internet trolls working for the Russia-based Internet Research Agency (IRA) exploited social media to target the US electoral process in an IW campaign designed to spread disinformation, create distrust, and increase societal division.[6] However, Russia's malign influence stretches well beyond the US. The Kremlin's efforts to influence political outcomes span the globe, ranging from political financing, to private military corporations, to special operations activities on nearly every continent.[7]

More recently, China leveraged the COVID-19 pandemic to expand its influence through a full-spectrum of IW activities. To deflect perceptions that it was mishandling the initial stages of the COVID-19 outbreak, China initiated a "global coronavirus rescue campaign," focused on sending aid packages to European Union nations. China aggressively publicized this effort while

Lt Col Nicholas J. Hall is the Director of the Commander's Action Group, Sixteenth Air Force /Air Forces Cyber. A career intelligence officer, Lt Col Hall was previously the Director of Operations for the 15th Intelligence Squadron, Joint-Base Langley-Eustis, Virginia. He has served as an analyst in the U.S. Central Command and U.S. Pacific Command areas of responsibility, as an intelligence crew member in an Air Force Special Operations Command MQ-1B unit, and has held three targeting positions at the squadron, major command, and combatant command level. He has also deployed to the Combined Air Operations Center in Southwest Asia and to Afghanistan, where he was a U.S. Army cavalry squadron S2. Lt Col Hall is a graduate of Baylor University in Waco, Texas, holds a Master's degree from American Military University, and is a distinguished graduate of the U.S. Air Force Air Command and Staff College.

simultaneously blaming the US for causing the pandemic.[8] Some observers have noted that China's information strategy surrounding the pandemic appears similar to the Russian playbook of spreading disinformation to create doubt about established facts.[9] Our adversaries employ integrated approaches, combining messaging in the media with economic pressure, military maneuvers, and diplomacy to impose a cost. The US must expand and broaden our own competition globally in the information environment while remaining consistent with our values built on a "foundation of mutual respect, responsibility, priorities, and accountability" with our allies as outlined in the NDS.[10]

As US adversaries increasingly pull the multidisciplinary levers of IW, the information environment gives them global access to compete at a low cost. In a globalized data-age, the outcomes of these actions are not constrained to segmented geographic regions. Department of Defense (DoD) leaders have recognized this threat. The Chairman of the Joint Chiefs of Staff has pushed the joint force toward globally integrated campaigns and exercises to operationalize cross-combatant command coordination on global problem sets.[11] However, this transformation will not happen overnight. Joint force commanders are demanding options below the level of armed conflict, and plans that integrate multi-domain capabilities and creatively leverage IO. As the DoD explores options to increase competition, we must look for new ways to partner across U.S. Government departments and agencies. If we want to gain the initiative in the information environment, we need a new approach to warfighting.

THE RESPONSE – WHY 16TH AIR FORCE WAS ESTABLISHED

Since 9/11, the joint force approach to warfighting has been shaped by the conflict against violent extremism. The Air Force ISR enterprise and the

Maj Eugene H. Fan is the Aide-de-Camp to the Commander, Sixteenth Air Force/Air Forces Cyber. A career logistician and aircraft maintenance officer, Maj Fan has held various positions to include Operations Officer, Executive Officer, and Officer-in-Charge at multiple echelons and maintenance organizations. Prior to his current position, Maj Fan was the Chief of the Maintenance Operations Branch, Headquarters Twenty-fifth Air Force, Joint Base San Antonio-Lackland, Texas. He has also deployed as an Operations Officer to Southwest Asia, where he led the generation of strike, intelligence and reconnaissance, aeromedical evacuation, and command and control missions in support of several operations in the theater. Maj Fan is a graduate of the University of Georgia in Athens, Georgia, holds a Master's degree from Oklahoma University in International Relations, and is a graduate of the Air Force's Advanced Maintenance and Munitions Operations School.

Intelligence Community more broadly optimized collection, analysis, and reporting strategies to enable find-fix-finish operations against single or small groups of combatants on the battlefield. The target development required to establish a pattern of life, distinguish between combatants and non-combatants, and achieve positive identification of the enemy was enabled by time-intensive and overlapping collection in a permissive environment. For example, the 2006 strike on Abu Musab al-Zarqawi took "600 hours of Predator time and thousands of hours of analyst time to facilitate a strike executed in a matter of minutes."[12] In this environment, the joint force developed a series of command and control processes that synchronized ISR and EW capabilities to efficiently find and fix a homogenous adversary. Those processes were not constrained by time, and they were geographically bounded. Additionally, cyberspace and IO capabilities were rarely used as either a primary effects mechanism or as a collection enabler. This model was sufficient for its time and place. However, to effectively respond to inter-state competition from Russia and China, the joint force must better integrate IW capabilities and employ a process that is relevant to the speed of the information environment. Within the Air Force, previous approaches to ISR strategies for great power competition; the integration of Cyber, IO, and EW; and command and control of these capabilities fell short.

Russia's annexation of Crimea in 2014 was achieved using a combination of armed force, deception, IO, criminal activity, and political and economic actions.[13] Russia's strategy – what some have termed the "Gerasimov doctrine," for Russia's Chief of the General Staff General Valery Gerasimov – blurs "the line between a state of war and peace" and employs "extensive use of political, economic, diplomatic, information, and other nonmilitary measures, all supported by the protest potential of a population."[14] At the time, the North Atlantic Treaty Organization

(NATO) Supreme Allied Commander Europe, General Philip Breedlove, admitted that "the actions of Russia and its leadership are extremely difficult to predict."[15] This difficulty resulted in part because military service and Intelligence Community capabilities were positioned to assess Russian actions as indications and warning predictors within a traditional "conception of conflict."[16] Orienting joint force capabilities in this way creates a "curtain of ambiguity," limiting insights into adversary intent and complicating the identification and discrimination of targets in the information environment. In 2014, the DoD was seemingly unprepared to offer any IW response.

To respond effectively to similar scenarios in the future, the Air Force must adopt an approach that enables a clear focus on these hard problems. This approach should take a global viewpoint and use access to data across each IW capability to generate insights into the adversary's whole-of-nation approach to strategic competition. It must not only effectively integrate capabilities to produce timely effects in the information environment, but it should also enable partners across the DoD, U.S. Government departments and agencies, and foreign partners to counter a present and growing threat. The Secretary of the Air Force established the 16th Air Force for this reason; to specifically converge these capabilities and activities in the information environment.

Convergence on priority problems positions the 16th Air Force to enable combatant commands and air components to create IW outcomes in globally integrated campaigns. Outcomes are results that directly achieve a commander's objective. Within the context of strategic competition, these can range from using cyber effects to deny or degrade an adversary's operations, precision messaging that leverages deception to affect individual or unit behavior, a public affairs release that exposes malign activity, Treasury Department (USDT) sanctions, State Department (DOS) demarches, and other means. While the Air Force has enabled some of these outcomes previously, our service was not postured to generate these IW outcomes in a timely, consistent, or synchronized manner. The order establishing the 16th Air Force succinctly describes the challenge highlighted in the preceding paragraphs: "The separation of Cyber, Intelligence Surveillance and Reconnaissance (ISR), Electronic Warfare (EW), and Military Information Support Operations (MISO)/Military Deception (MILDEC) among different organizations coupled with an inability to integrate multi-domain operational and tactical activities puts the Air Force at a disadvantage across the conflict continuum."[17],[18] The 16th Air Force is charged with integrating these capabilities, and will leverage a unique global vantage point to generate insights on adversary activity that lead to outcomes that make us competitive now.

Convergence in the information environment integrates capabilities by combining cross-functional data and tradecraft in creative ways, ultimately generating outcomes greater than each individual capability can create on its own. As the 16th Air Force builds towards convergence, we must articulate our approach to IW as a command, how we operationalize convergence, and examine how convergence applies to, and changes, warfighting.

INFORMATION WARFARE FOUNDATION

The 16th Air Force IW outcomes are built on three foundational lines of effort: Generate Insights, Compete Now, and Prepare for Escalation.

Generate Insights. All warfighting activities center on understanding the adversary. The 16th Air Force is uniquely positioned within the joint force to continuously generate insights across a spectrum of activities now integrated into an IW force. These include Signals Intelligence (SIGINT) missions as delegated by the National Security Agency (NSA), medium-and high-altitude ISR collection as tasked by air components, problem-centric analysis and exploitation through the Distributed Common Ground System (DCGS) enterprise, robust reach-back analysis and targeting enterprise, insights derived from operations in cyberspace, and insight into adversary mindset from behavioral science resources.

Two factors within this line of effort complicate a transition to converged IW. The first is that in the information environment, battlespace awareness often looks different from the traditional Intelligence Preparation of the Operational Environment (IPOE), which focuses on the order of battle of physical targets and decision support. While these activities must continue, we need to think differently. This will require new tradecraft to recognize and counter threats, and may involve new data sources, collection strategies, and methods of analysis to create outcomes in the information environment. Second, the need to improve data integration among intelligence capabilities increases as we shift to global challenges that affect traditional geographic and functional areas of responsibility. Units within our enterprise will require tight integration to rapidly incorporate insights generated across multiple disciplines. Convergence addresses the various functional Air Force data stovepipes that have formed over the last two decades.

Compete Now. The implementation of convergence will be marked by a cultural shift across the Air Force. We must begin to expose adversary activities that seek to undermine the US position and destabilize the international order. U.S. Africa Command (USAFRICOM) took this initiative on May 26, 2020, when it publicly released unclassified imagery of Russian MiG-29 and Su-24 aircraft deployed to Libya. In a statement amplified by CNN, USAFRICOM disclosed that "Moscow recently deployed military fighter aircraft to Libya in support of Russian state-sponsored private military contractors operating on the ground there."[19] The aircraft had also been painted to remove national markings. The USAFRICOM exposure of Russian malign action is an IW outcome the 16th Air Force should regularly enable by generating the initial insights into the adversary activity and shaping the information environment to counter adversary actions.

U.S. Cyber Command (USCYBERCOM) has also advanced joint force thinking on competition through General Paul Nakasone's concept of Persistent Engagement. This concept implements the 2018 DoD Cyber Strategy, which explains that contact with adversaries in cyberspace is continuous. Thus, it is appropriate to "defend forward" and engage militarily in this domain to

protect our national interests.[20] Indeed, the 2019 National Defense Authorization Act (NDAA), embraces this strategy by defining operations in cyberspace as a "traditional military activity."[21] A similar shift has started within the information environment but must accelerate more broadly. Leveraging not only cyberspace but all IW capabilities, 16th Air Force must converge on the nation's highest priority problems. This process will yield outcomes for the joint force or options for partners within the U.S. Government to execute multi-domain IW operations against our adversaries.

Producing an outcome in the information environment does not always require DoD action; other government departments and agencies often bring unique authorities and approaches. For example, some outcomes can result from a USDT sanction, a Department of Justice (DOJ) indictment, or enabling DOS to work through a partner nation. Such partnerships led to the March 2018 USDT sanctions against five entities and nineteen individuals for "interference in U.S. elections, destructive cyber-attacks, and intrusions targeting critical infrastructure."[22] This approach can enable the full power of the U.S. Government to achieve strategic outcomes.

Multi-domain and whole-of-government IW operations will impose a cost on US adversaries by exposing their malign activity and eliminating their plausible deniability.[23] This approach will force adversaries to respond, expend resources internally, or change their strategies. The Air Force has many of the resources required to compete persistently in the information environment, which is an NDS imperative. We now need an approach that accelerates action. As 16th Air Force aligns on priority targets for competition, the challenge will be to synchronize the activities required to produce effective outcomes inside our adversaries' OODA loop— Observe-Orient-Decide-Act.[24]

Prepare for Escalation. As 16th Air Force expands its options to compete, we must remain ready for conflict escalation. We must continue to perform each IW capability with excellence and be ready to support joint force commanders in the event of a conflict. The 16th Air Force approach to IW should also include strategies that impose cost and deter escalation without provoking it. Additionally, US adversaries should be mindful that IW outcomes can rapidly shift along the competition continuum.[25] The intelligence and targeting data used to generate outcomes that compete with our adversaries in the information environment can be applied to produce non-kinetic or kinetic outcomes if the conflict escalates.

Conflict with a peer adversary will be characterized by several complicating factors, including, the "geographic asymmetry" posed by our force posture relative to China and Russia, and an increased number of adversary targets on the battlefield.[26] Our adversaries will employ a range of offensive standoff weapons to deny access as well as "semi-autonomous unmanned aircraft, drone submersibles, small vessels, and smart mines" to complicate effective maneuver.[27] Additionally, China and Russia will target our most critical capabilities, including the network and communications infrastructure, which the joint force relies on for command and control.

To win in this environment, 16th Air Force must deliver a range of kinetic and non-kinetic outcomes. Effective IW operations in a peer conflict will require tight synchronization among ISR, Cyber, EW, and IO, as well as seamless integration into combatant command operational processes. Future battlespace conditions will expand the distance but limit the time required to find, fix, and finish targets. Accordingly, the data produced by each IW capability must be automatically accessible and integrated into all nodes in the kill chain both vertically and horizontally. The Joint All Domain Command and Control (JADC2) concept linking all sensors to all shooters describes this approach.[28] In addition to the material means required to achieve this level of integration, we must shift "our doctrinal dependence on large vulnerable centralized command and control nodes to more agile, networked solutions."[29] Our IW forces must integrate into joint command and control concepts that allow for the flexible employment of a distributed force. The speed of decision required to respond to a peer adversary in a dynamic tactical situation will require ISR, EW, IO, and offensive and defensive cyber Airmen to repeatedly make decisions and execute distributed operations under mission command with limited direction from higher headquarters. The possibility of such a scenario requires 16th Air Force to maintain excellence across its IW capabilities, and the convergence of our forces in the information environment will now prepare us to seamlessly integrate in a future conflict.

CONCEPTUALIZING CONVERGENCE

The 16th Air Force is building an approach to IW by tailoring the Army's concept of convergence to our enterprise. We will operationalize convergence by both commanding and controlling our assigned forces, and enabling the horizontal awareness among tactical units required to synchronize the broader enterprise at the operational level of war. To succeed, we must acknowledge and overcome several historical biases and thereby rapidly transition to a problem-centric approach that leverages 16th Air Force global operations, authorities, and access to data.

The U.S. Army's Multi-Domain Operations (MDO) doctrine defines convergence as "the rapid and continuous integration of capabilities in all domains, the electromagnetic spectrum, and the information environment that optimizes effects to overmatch the enemy through cross-domain synergy and multiple forms of attack all enabled by mission command and disciplined initiative."[30] The Army's concept prescribes the need for data from any sensor to flow through any command and control node to enable any shooter, which is critically important, especially at the tactical level. The Air Force IW enterprise is service-unique, so we have built upon the Army's foundational work. As 16th Air Force expands convergence to address strategic competition, we must address some long-standing biases that could impact how we compete effectively on a global scale.

Bias 1 – Geographic Organization and Outlook

Geographic boundaries pose no constraints for data and information; our IW outcomes should also be unconstrained. China and Russia do not operate in accordance with joint force command boundaries—they are global malign actors whose exploitation of the information environment impacts every combatant command. A Strategic Multilayer Assessment (SMA) White Paper released by the Joint Staff in May 2019 assessed Russia would increase its "gray zone" tactics across Europe and Central Asia, Africa, the Middle East, the US, and Latin America in the near term.[31] 16th Air Force capabilities are distributed globally and have an array of vantage points into each of those regions. To leverage the unique capabilities of our global enterprise, we must capitalize on the agility such a distributed force offers. In many cases, the Airmen working to develop an outcome might not be "owned" by or even reside within, a given command with authority to execute IW operations—they must instead work seamlessly with a command that does. The more globally integrated the joint force becomes, the more natural this will seem. We envision scenarios wherein the same commander can alternate between supported and supporting during the same operation, or simultaneously exist in both states.

Bias 2 – Command and Control Blinders

Command and control are essential to the efficient and disciplined execution of combat operations. At all levels of war, the joint force requires clear lines of command responsibility. However, if we only shoot, move, and communicate with those elements directly in our chain of command, we are less agile, less informed, miss opportunities, and are vulnerable to exploitation. Convergence does not require a change in command and control doctrine. What we need is a new framework that organizes global synchronization at the speed of IW.

Bias 3 – Focus on Conflict

We must always be prepared for armed conflict, but our adversaries are out-competing us now. The Secretary of Defense, Dr. Mark Esper, put it this way in a December 2019 press briefing: "We must deal with the world we live in, not the one we want."[32] While US adversaries' actions are at times escalatory, they fall below the threshold of armed conflict. They cannot act with complete impunity, yet their manipulation of the information environment clouds the truth, redirects blame, or creates plausible deniability that inoculates them against international consequences. Through these incremental gains, they achieve strategic ends without the need for war. There is a growing demand from combatant commanders to shift military service weight of effort toward outcomes that regain the initiative in the information environment.

OPERATIONALIZING CONVERGENCE

Implementing convergence in the information environment requires new operational art. Our framework starts within the 16th Air Force to synchronize outcomes on common operational priorities that cross combatant command boundaries. These outcomes address

problems that, in many cases, are being simultaneously requested and prioritized across combatant commands. Russian malign influence impacts each geographic and functional combatant command in the DoD. However, legacy, stovepiped processes, and data access all limit awareness and collaboration both inside 16th Air Force, and among component and combatant command staffs that are divided by geographic boundaries.

Convergence is designed to leverage both existing command and control constructs that direct forces and activities while enabling synchronization among partners that leads to mutually beneficial outcomes for multiple commanders. Ultimately, we will realize convergence by leveraging the inherent strengths of the 16th Air Force outlined below.

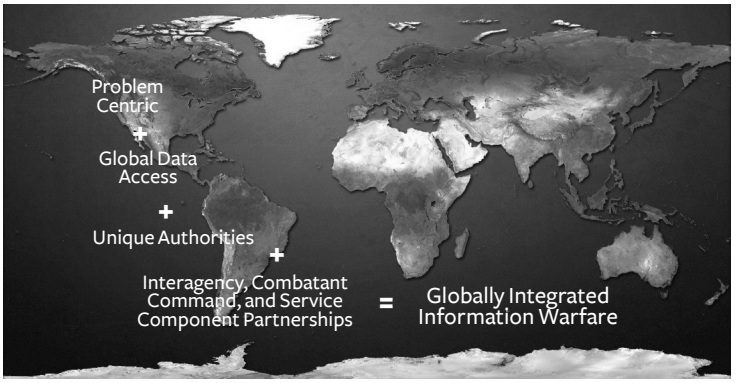

Figure 1. Convergence Formula

First, 16th Air Force is ***problem-centric*** and has moved away from a platform or sensor-based approach to one that leverages access to many data sources, regardless of origin. This approach allows our Airmen to gain insights that improve the understanding of the adversary and solve the most important operational problems for joint force commanders.

Second, 16th Air Force has ***access to data*** across each IW function. Integrating this data into a combined picture provides a global vantage point. As a result, the problem-centric approach becomes unconstrained by geographic boundaries and provides the opportunity to generate global outcomes.

Third, the 16th Air Force is assigned ***authorities*** unique within the Air Force, that include roles as the Service Cryptologic Component to the National Security Agency (NSA), a Component-Numbered Air Force (C-NAF) within Air Combat Command, a Service Cyber Component in Combatant Command relationship to USCYBERCOM and in general support to four other Combatant Commands, and as the operational commander of the Air Force Information Network (AFIN). The 16th Air Force will leverage these authorities to take full advantage of the elements we command and control in cyberspace operations, the enterprise data access inherent to each line of authority, and the broader capacity of our ISR, targeting, and EW capabilities.

Additionally, the partnerships we have built with air components, combatant commands, and within the interagency, enhance the effectiveness of 16th Air Force capabilities. This powerful combination will enable new global IW outcomes, either in the form of options for a supported joint force commander or as an outcome 16th Air Force creates as the supported component to compete in the information environment.

The 16th Air Force is tasked both with developing the partnerships that bring alignment and enable the horizontal awareness required to achieve problem-centric collaboration and data integration. This results in two byproducts. First, as we increase data sharing, each functional capability will gain additional insights that improve analysis, signal development, and follow-on collection. Second, as the operational staff synchronizes previously stovepiped capabilities on global problems, we will create new IW outcomes not previously realized within the Air Force. We expect many of these to be fact-based public disclosures. This is our comparative advantage, and it is an approach to convergence that has not yet been executed to the scale we envision.

SELECTED WARFIGHTING APPLICATIONS FOR CONVERGENCE IN THE INFORMATION ENVIRONMENT

Our approach to convergence will address several sets of problems within the information environment. The below examples are not all-inclusive but demonstrate a range of possible outcomes that allow us to compete against our adversaries now. A brief examination of these examples reveals opportunities to leverage our access to data, authorities, and partnerships. As 16th Air Force initiates operations, we begin to see the value of converged IW outcomes.

Countering Disinformation. We will quickly realize the potential for convergence in our mission to counter disinformation. Our adversaries aim to supplant logic and fact with fantasy and fear by saturating the information environment with lies.[33] We counter this by adhering to the inherent strengths and core values of our nation—we speak the truth. As the US military shifts its focus to this societal threat, our ability to generate insights postures the 16th Air Force well for this challenge.

Today, Joint Force Headquarters cyber teams are developing options to impose a cost on adversaries who inject disinformation into the environment. Additionally, our DCGS enterprise is employing a problem-centric approach to gain a deep understanding of adversary malign activity in support of air components. Our cyber defense Airmen are exposing malign cyber activity, while our global targeting wing has focused target systems analysis and non-kinetic intelligence analysis on malign adversary influence. Simultaneously, four wings across the 16th Air Force ISR enterprise are leveraging Publicly Available Information (PAI) to gain insight and develop tradecraft to expose a similar activity.

As we connect and share data among these functional capabilities, each unit will improve the quality of insights it can provide to the tasking command. Additionally, as the 16th Air Force IW Operational Staff organizes the converged approach, planners will identify new outcomes that can be generated by taking a global view of the data generated by each subordinate unit. Some outcomes might be precise and enabled by cyber. In other cases, our operationalized Public Affairs elements will be best suited to counter disinformation with the truth. Both options impose a cost on the adversary by either compelling a change in behavior or deterring a future action. Most importantly, we must recognize that what sets us apart from our adversaries is that rather than spreading disinformation, we deal in truth. The Air Force can be aggressive within the information environment because we will produce facts and fact-based evidence of malign activity. Convergence creates a framework that enables the 16th Air force to begin injecting that truth into the information environment at an unprecedented speed and scale.

Cyber-Enabled Information Operations. By integrating our Joint Force Headquarters cyber teams with our growing IO force, we can scale to create effects against targets where combatant commanders currently lack options. Alignment of our ISR collection and analysis units against these targets will also yield intelligence and cultural insights that our IO professionals can use to increase target fidelity and create behavioral change. For example, Joint Task Force (JTF) ARES achieved this against the Islamic State of Iraq and Syria (ISIS). JTF ARES integrated multiple disciplines to create confusion and distrust within ISIS and ultimately worked closely with partners to dismantle its web-based operations.[34]

Cyberspace access will be essential to creating precision effects in the information environment. Precision effects will also be somewhat of a cultural shift in military operations, which has often focused on messaging aimed at more generalized populations. Precision, cyber-enabled IO, provides an intermediate option between broad messaging and a kinetic strike. It may enable more predictable effects and, in some cases, lower cost, and pose a lower risk to escalation. Regardless of the use case, tight synchronization among units working across the information environment is required to converge effectively against global targets.

Convergence in Space. The 16th Air Force (Air Forces Cyber (AFCYBER)) was recently designated the cyber component in general support to U.S. Space Command (USSPACECOM). With the standup of the U.S. Space Force (USSF), we must consider what IW looks like in this domain. In the coming decades, space will become more accessible and consequential to the civil, military, and economic interests of all nations. As this happens, states will correspondingly increase competition in and through space.[35] No domain lends itself to the synergy of cyber, ISR, EW, and IO like space. A converged approach to IW in support of USSPACECOM should leverage these mutually supportive capabilities to rapidly generate outcomes.

USSPACECOM has recently demonstrated clear initiative in responding to adversary space activity. Russia's direct ascent anti-satellite missile test on April 15, 2020, represents a clear threat to the global community and undermines Russia's advocacy for a treaty banning weapons

in space. In response, the Commander of USSPACECOM, General Jay Raymond, publicly stated, "This test is further proof of Russia's hypocritical advocacy of outer space arms control proposals designed to restrict the capabilities of the United States while clearly having no intention of halting their counter-space weapons programs."[36] He later responded to Iran's failed attempt to employ an imaging satellite by tweeting information regarding the failure derived from USSPACECOM space-tracking capabilities.[37] As adversaries increase competition in and through space, an IW posture such as the one demonstrated by the USSF will enable rapid outcomes that position the nation for continued ascendency over strategic rivals in space.

CHANGING THE WAY WE FIGHT

To effectively compete at scale, we need an approach to IW that builds on US strengths and values. IW requires tight partnerships among all elements of the DoD, the interagency, and our coalition partners, driving a shift in the weight of effort from preparing for conflict to competing now. As military leaders, this is an opportunity to re-evaluate historical biases that constrain us from competing in the information environment. We do not need a new approach to command and control, but a new framework that both materially creates the awareness *among*, and organizes the horizontal coordination *of*, organizations across the continuum of cooperation, competition, and conflict. The NDS is driving the DoD to examine competition through a new lens. We believe the creation of 16th Air Force and our approach to convergence in the information environment offers new opportunities to compete now. As the 16th Air Force enters full operational capability in 2020, we are taking a problem-centric approach to competition. Our global vantage point, enabled by access to data and authorities, will improve each of our capabilities while producing new IW outcomes through operations that will be simultaneously supported and supporting. We are confident this approach will change the way the Air Force fights.

NOTES

1. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America*, Washington, DC: Department of Defense, 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
2. Headquarters United States Air Force, Program Guidance Letter (PGL) 19-05, *Establishment of the Information Warfare (IW) Component Numbered Air Force (C-NAF) under Air Combatant Command*, September 6, 2019, 5.
3. Department of Defense, *Joint Doctrine Note 1-19: Competition Continuum*, Washington DC: Department of Defense, 2019, https://www.jcs.mil/Portals/36/Documents/Doctrine/ jdn_jg/jdn1_19.pdf.
4. Sean McFate, *The New Rules of War: Victory in the Age of Durable Disorder*, William Morrow, 2019.
5. Department of Defense, *Strategy for Operations in the Information Environment*, Washington DC: Department of Defense, 2016, https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.
6. Department of Justice, *Report on the Investigation Into Russian Interference In the 2016 Presidential Election*, Washington DC: Department of Justice, 2019, https://www.justice.gov/storage/report.pdf.
7. Tim Lister, Sebastian Shukla, and Clarissa Ward, "Putin's Private Army." CNN. Cable News Network, 2019, https://www.cnn.com/interactive/2019/08/africa/putins-private-army-car-intl/.
8. "Is China Winning the Coronavirus Response Narrative in the EU?" Atlantic Council, March 26, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/is-china-winning-the-coronavirus-response-narrative-in-the-eu/.
9. Jessica Brandt and Bret Schafer, "Five Things to Know About Beijing's Disinformation Approach." Alliance For Securing Democracy, April 1, 2020, https://securingdemocracy.gmfus.org/five-things-to-know-about-beijings-disinformation-approach.
10. Department of Defense, Summary of the 2018 National Defense Strategy of the United States of America, Washington, DC: Department of Defense, 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
11. Jim Garamone, "Global Integration Deserves More Attention, Selva Says." U.S. DEPARTMENT OF DEFENSE, June 19, 2019, www.defense.gov/Explore/News/Article/Article/1881159/global-integration-deserves-more-attention-selva-says/.
12. Robert Haffa and Anand Datla, "Joint Intelligence, Surveillance, and Reconnaissance in Contested Airspace," Air And Space Power Journal, May-Jun (2014): 31, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-28_Issue-3/F-Haffa_Datla.pdf.
13. John Davis Jr., "Continued Evolution of Hybrid Threats: The Russian Hybrid Threat Construct and the Need for Innovation," The Three Swords Magazine 28 (2015): 23, http://www.jwc.nato.int/images/stories/threeswords/CONTINUED_EVOLUTION_ OF_HYBRID_THREATS.pdf.
14. Timothy Thomas, "Russian Military Thought: Concepts and Elements," *Report sponsored by U.S. European Command*, (McLean, VA: MITRE Corporation, 2019), 11-13, https://www.mitre.org/sites/default/files/publications/pr-19-1004-russian-military-thought-concepts-elements.pdf.
15. Lysgard Asbjorn and Boye Lillerud, "How is Russian Hybrid Warfare a Challenge to the Intelligence Function at the Operational Level and to What Extent Should it Adapt," Arts and Social Sciences Journal 10, no. 3 (2019), 2, https://astonjournals.com/manuscripts/Vol_10_2019/ASSJ_Vol10_3_how-is-russian-hybrid-warfare-a-challenge-to-the-intelligence-function-at-the-operational-level-and-to-what-extent-shoul.pdf.
16. Frank Hoffman, "On Not-So-New Warfare: Political Warfare Vs. Hybrid Threats," War on The Rocks, July 2014, https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/.
17. Headquarters Air Combat Command Planning Order (PLANORD) 19-001, *Optimization of ACC Information Warfare (IW) Force Generation and Presentation*, April 3, 2019, 1.
18. Department of Defense, *Joint Publication 3-13: Information Operations* (Washington DC: Department of Defense, 2014), 34-35, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.
19. Ryan Browne and Gul Tuysuz, "US military accused Russia of deploying fighter aircraft to Libya." CNN.com. https://www.cnn.com/2020/05/26/politics/russia-fighter-aircraft-libya/index.html, accessed May 27, 2020.
20. Department of Defense, S*ummary of the Department of Defense Cyber Strategy*, Washington DC: Department of Defense, 2016, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF 2018.

NOTES

21. National Defense Authorization Act for fiscal year 2019: conference report, Washington, D.C.: U.S. G.P.O.
22. Department of the Treasury. *Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks:* Press Release on March 18, 2018, https://home.treasury.gov/news/press-releases/sm0312.
23. Sean McFate, *The New Rules of War: Victory in the Age of Durable Disorder.*
24. David S. Fadok, *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis,* Air University Press, (Maxwell AFB, AL, February 1995), 16, http://dtlweb.au.af.mil/webclient/treamGate?folder_id=0&dvs=1590791287782~577.
25. Department of Defense, *Joint Doctrine Note 1-19: Competition Continuum* (Washington DC: Department of Defense, 2019), https://www.jcs.mil/Portals/36/Documents/Doctrine jdn_jg/jdnl_19.pdf.
26. Michael Mazarr, "Toward a New Theory of Power Projection," War on The Rocks, April 2020, https://warontherocks.com/2020/04/toward-a-new-theory-of-power-projection/.
27. Ibid.
28. Morgan Dwyer, "Making the Most of the Air Force's Investment in Joint All Domain Command and Control," Center for Strategic International Studies, March 2020, https://www.csis.org/analysis/making-most-air-forces-investment-joint-all-domain-command-and-control.
29. Dan DeCook, "Innovation, National Defense Strategy, the future: CSAF at Air Force Association Air Warfare Symposium," Secretary of the Air Force Public Affairs, February, 2018, https://www.af.mil/News/Article-Display/Article/1449095/innovation-national-defense-strategy-the-future-csaf-at-air-force-association-a/.
30. Department of the Army, *The US Army in Multi-Domain Operations: 2028.* TRADOC Pamphlet 525-3-1. Fort Eustis, Virginia, December 2018.
31. John Arquilla, et. al., *Russian Strategic Intentions,* Department of Defense, Joint Chief of Staff, May, 2019, https://nsiteam.com/social/wp-content/uploads/2019/05/SMA-TRADOC-Russian-Strategic-Intentions-White-Paper-PDF-1.pdf.
32. "Department of Defense Press Briefing by Secretary Esper and General Milley." U.S. DEPARTMENT OF DEFENSE, December 20, 2019, www.defense.gov/Newsroom/Transcripts/-Transcript/Article/2045725/department-of-defense-press-briefing-by-secretary-esper-and-general-milley-in-t/.
33. Herbert Lin, "The Existential Threat from Cyber-Enabled Information Warfare," Bulletin of the Atomic Scientists 75, no. 4 (2019): 187–96, https://doi.org/10.1080/00963402.2019.1629574.
34. Dina Temple-Raston, "How The U.S. Hacked ISIS." NPR. National Public Radio, September 26, 2019, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.
35. Air Force Space Command, "The Future of Space 2060 and Implications for U.S. Strategy: Report on the Space Futures Workshop," 2019.
36. Nathan Strout and Aaron Mehta, "Russia Conducted Anti-Satellite Missile Test, Says US Space Command." C4ISRNET. C4ISRNET, April 15, 2020, https://www.c4isrnet.com/battlefield-tech/space/2020/04/15/russia-conducted-anti-satellite-missile-test-says-us-space-command.
37. Travis Fedschun and Lucas Tomlinson, "Iran's Military Satellite a 'Tumbling Webcam in Space,' Space Force Commander Says." Fox News. FOX News Network, April 26, 2020, https://www.foxnews.com/world/iran-military-satellite-us-space-force-commander-tumbling-webcam.