Winning Wars of Cognition: Posturing the Air Force for the Tactical Information Fight

Major Jeremiah Deibler

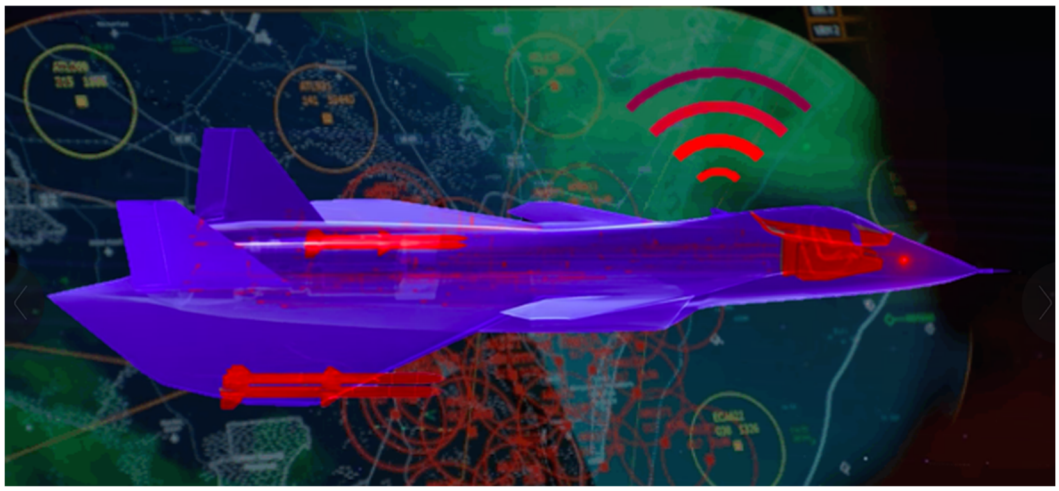

Image Source: CBS and DefenseOne

When the United States Air Force (USAF) announced its re-invigoration of Information Warfare (IW), it joined a global recognition that in Great Power Competition, prior to the outset of physical violence, wars are fought in the information environment. It also addressed a critical shortfall identified in the 2018 National Defense Strategy: "America's military has no preordained right to victory on the battlefield." This includes the information environment. Today, the USAF, seeks to organize around IW for the USAF. In doing so, the Air Force took a narrower approach to IW that emphasizes the integration of cyberspace operations, electronic warfare, information operations, and intelligence, surveillance, and reconnaissance (ISR). This narrower definition of IW addresses information's role at the tactical level of war and should not be misconstrued with the strategic or operational level, both of which possess an important informational component in modern Great Power Competition.

As the USAF organizes around tactical IW, it must consider the global implications of Electromagnetic Spectrum (EMS) and Cyberspace defense of the Airspace Control System and the unique nature of targets in the information environment. To address these arguments, this

paper will (1) delineate between IW at all levels of war, (2) describe the Offensive and Defensive considerations for IW, (3) describe the relationship between tactical level IW and support to the Joint Forces Air Component Commander (JFACC), and provide initial recommendations regarding the USAF's re-organization efforts.

On Information Warfare

IW exists at the strategic, operational, and tactical level. At the strategic level, Information combines with the other national instruments of power (Diplomacy, Military, Economic) to create a comprehensive design to achieve national policy objectives. IW at the strategic level may include the employment of social media and radio broadcast to deliver tailored messages to the population of a foreign nation. For example, Russia employed social media via the Internet Research Agency to influence the US elections. At the operational level, IW integrates physical and informational power to achieve the military objectives. China's dredging operations and employment of its Maritime Militia via its "Cabbage Strategy" signaling helps achieve its military objective to gain command of the South China Sea. At the tactical level, IW takes on the narrower definition employed by the Air Force. Here, Cyberspace, EMS, Information, and Intelligence, Surveillance, and Reconnaissance (ISR) operations are employed to affect the adversary's decision-making process while assuring the friendly process. While the strategic and operational applications of IW are critical to national policy goals, the focus of this paper remains on how, at the tactical level, IW can be employed in support of the JFACC.

Understanding Information Superiority

The objective of tactical IW is to gain and maintain information superiority. Information Superiority is defined in a 2004 Research and Development Corporation (RAND) Study definition: "the ability to collect, process, and disseminate information as needed; anticipate the

changes in the enemy's information needs; and deny the enemy the ability to do the same." RAND focused on ISR's contribution to information superiority. Nonetheless, by understanding RAND's explanation of the C4ISR process, IW planners may identify vulnerabilities within the decision-making process to exploit or defend in order to achieve information superiority. RAND breaks the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) process down to six steps (see Figure 1).

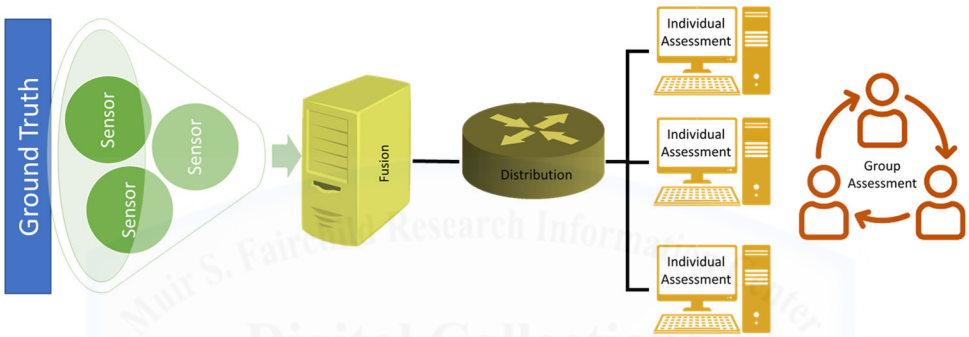

Figure 1. Author's Visual Depiction of RAND's C4ISR Process

The information environment is a subordinate component to the total operational environment. There exists a ground truth, "restricted [by RAND] to physical battlespace entities and their attributes." For RAND, this is Step 0. There is no direct correlation between information superiority and ground truth. It merely exists. Step 1 initiates observation and immediately begins affecting the perception of the observer. Once a sensor acquires the information, it "transmits their data to fusion facilities." During Step 2 (Fusion), individual intelligence disciplines are first processed before being fused at a central processing facility. Once fused, the information is distributed (Step 3) to several analysts who perform Individual Assessment (Step 4). Finally, the analysts collaborate on a Group Assessment (Step 5) to deliver to the decision-maker.

Through each subsequent step from Ground Truth to Group Assessment, there are several filters that *may* degrade the quality of information available at decision reducing the decision-makers effectiveness. By defending or exploiting vulnerabilities at each of these filters, a commander may gain or maintain information superiority. For example, the "quality of the sensor" affects the perception of the ground truth by limiting the end user's direct observation of the environment. Algorithms at both stages of fusion may be flawed. End users of the distributed information may face "loss of service, errors, and delays." Finally, biases and team dynamics may affect assessments by both individuals and groups. These degradation filters can be broken into four categories: confidentiality, availability, integrity, and trust. The first three are derived from the National Institute of Standards and Telecommunications (NIST): An Introduction to Information Security; the last is a broad characterization by the author of individual and group biases and exist on the cognitive, rather than logical plane.

Per NIST, confidentiality "[preserves] authorized restrictions on information access and disclosure" to prevent an unauthorized user from discovering critical information. Availability "[ensures] timely and reliable access" and is subject to Electronic Attack (EA) within the EMS or Offensive Cyberspace Operations (OCO). Building a mesh network with multiple means of connectivity (High Frequency, Satellite Communications, Fiber Optic Cable) may increase network reliability. Integrity "[guards] against improper information modification or destruction and ensuring information… authenticity" and covers both data and the system. Improving encryption algorithms for friendly communications may protect data's confidentiality while erorr detection protocols can ensure data's integrity. Conversely, modifying the processes on an adversary's information system to deceive or degrade its operation will reduce the effectiveness of the target's decision-making process.

Outside of NIST's definitions, Trust is encompassed by two sub-categories: individual trust and group trust. Individual trust constitutes the confidence an individual possesses regarding their perception of the information. Group trust constitutes the weight each individual's assessment carries within the group dynamic and the overarching cohesiveness of the organization (trust in one another). To gain and a maintain information superiority, a commander targets the confidentiality, integrity, availability, and trust of an adversary's information system (Figure 2) and information while securing his or her own.

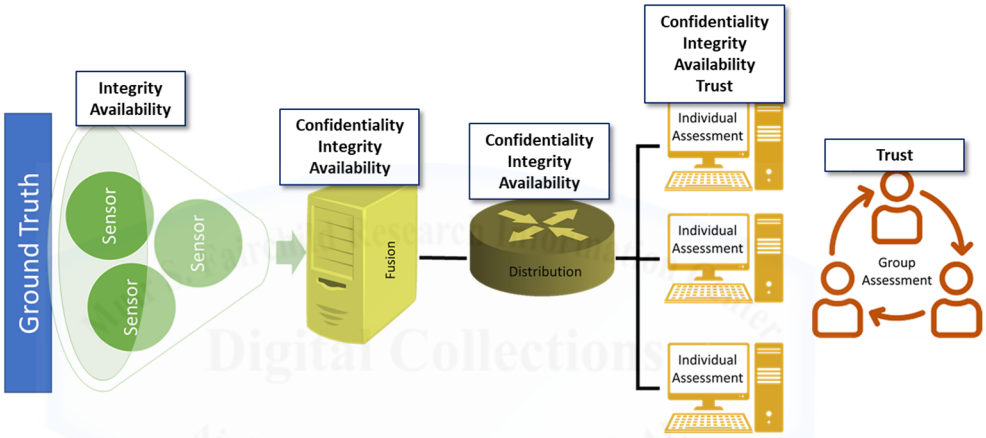

Figure 2. Author's Overlay of Degradation Filter Categories with RAND's C4ISR Model Integrated Information Warfare

At the tactical level, the commander employs the combination of Cyberspace, EMS, Information, and ISR Operations to gain and maintain information superiority. Cyberspace, EMS, and ISR operations are critical to defending and attacking the machine components of the information system. Information operations are critical to affecting how the sensors observe the ground truth (i.e., Camouflage, Concealment, and Deception (CC&D)) and how an individual's or group's biases cause them to perceive the information environment. When integrated, Cyberspace, EMS, Information, and ISR operations enable maneuver by "[placing] the enemy at a disadvantage through the flexible application of movement and fires." IW uses combined

information fires across the phases of the information system (Figure 2) to increase or reduce fog and friction for the decision-makers. Information fires weaponize data, modulated EMS particles or waves, network protocols, system processes, and cognitive biases to shape the information environment.

By affecting each phase, combined information fires produce a compounding effect. When the integrity of a sensor is affected in Phase 1, it cascades to the decision-maker. It can only be overcome via additional sensors. The system may maintain a perfect picture of the ground truth up through individual assessment. However, that individual's assessment may be undermined by a decision-maker subject to pre-conditioned biases. To increase the likelihood of misinterpretation, operations to affect the information system must not be individual in nature but be combined.

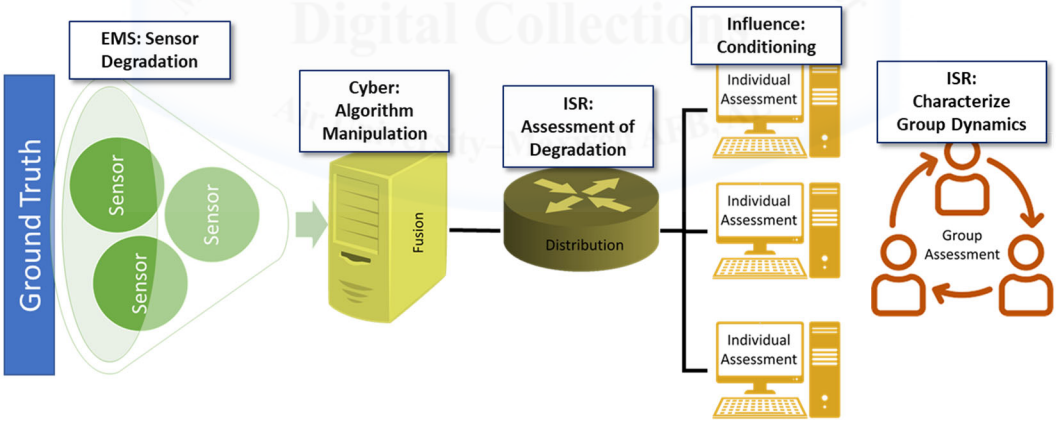

Figure 3. Author's Concept of Offensive Combined Information Fires

Offensive Combined Information Fires (Figure 3) seek to compound fog and friction while validating the effectiveness of their operations. Degrading sensors creates initial fog for the target. Simultaneously, cyberspace operations to deceive the fusion algorithms compounds information degradation. Multi-source surveillance and reconnaissance of data-in-transit (Distribution) enables the commander to validate the success of the prior operations and establish

a baseline of how the adversary is receiving the information for future assessment. ISR operations to characterize the group environment enables the identification of key individuals to facilitate conditioning. The ISR operations serve the secondary benefit to enable assessment of the total operation to determine whether the sensor degradation, algorithm manipulation, and conditioning achieved the desired effect.

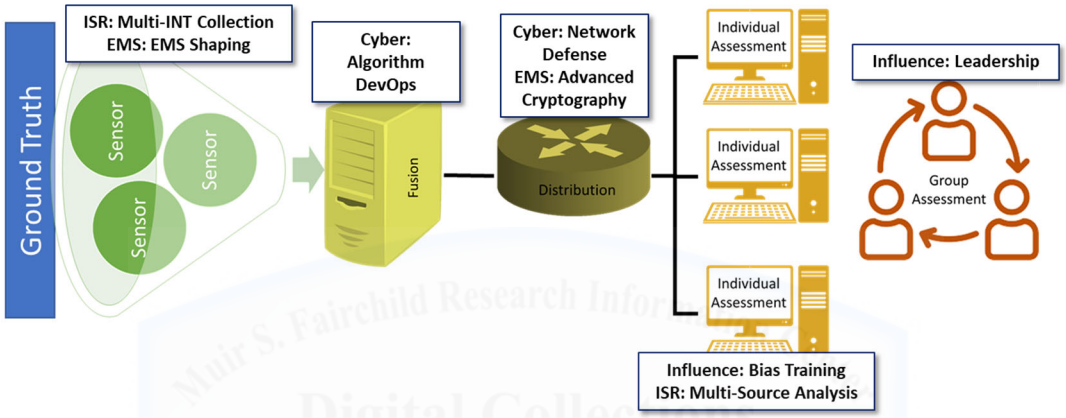

Figure 4. Author's Concept of Defensive Combined Information Fires

Defensive Combined Information Fires (Figure 4) increase information superiority by denying the adversary the ability to affect friendly decision-making. Multi-discipline ISR collection strategies increases information redundancy. Performing enabling-EMS operations to shape the environment enables the collection strategy. For fusion, implementing a Development Operations (DevOps) approach to the fusion algorithms complemented by data audits reduces the likelihood of adversary manipulation. Network defense and advanced cryptography are unsurprising additions to secure data-in-transit. Multi-source analysis increases an individual assessment's confidence. Finally, leadership and continuous, formal training are critical to reduce friction from biases in the information fight.

Both offensive and defensive approaches to IW employ ISR, EMS, Cyberspace, and Information operations to gain and maintain information superiority. Offensive IW's principal

purpose can be described as decreasing the confidentiality, integrity, availability, and/or trust in both information systems and information of the adversary. On the other hand, through unity of effort and unified action, defensive IW, assures the confidentiality, integrity, availability, and/or trust in friendly information systems and information.

IW and the Air Force

General Goldfein, Chief of Staff of the Air Force (CSAF), argued that the USAF must be able to observe more than our adversaries to "wars of cognition." The Air Force then built off CSAF's comments by laying out the foundational concept of AF IW. There are two pillars the USAF must be ready to support. First, it must be organized, trained, and equipped to present forces to support a Joint Forces Commander (JFC) prior to conflict. Second, if the US enters Major Combat Operations (MCO), the USAF must be organized, trained, and equipped to perform IW specifically in support of JFACC priorities. After a brief overview of airpower in support of a JFC prior to conflict, this section will focus on the latter requirement of USAF IW in support of the JFACC during MCO.

Prior to conflict, the nature of airpower presents unique capabilities to the support national policy objectives. "By making effective use of the third dimension, the electromagnetic spectrum, and time, airpower can seize the initiative, set the terms of battle, establish a dominant tempo of operations, [and] better anticipate the enemy through superior observation." These factors enable the USAF to "express national will wherever and whenever necessary" via rapid power projection's global access and subsequent deterrent effect from forward-deployed tripwire forces or the threat of ballistic missile response. In contested areas, shows of force or presence in coordination with naval strait transits promote freedom of navigation in support national policy objectives. Specifically, the actions affect the physical ground truth to present a clear message to

strategic decision-makers by affecting their risk calculus. Commander's intent is achieved through non-violent physical power and requires no additional combined information fires to affect the sensors, fusion, or distribution of the information. ISR operations are likely required to validate whether the message was received as intended.

If national policy objectives called for shaping perceptions and attitudes of the population, the USAF's high ground for line-of-sight to the target audience provides optimal angles of access for EMS-based media transmission. In an air supremacy environment, the AF may deliver leaflets via airdrop. Today, these operations can be complemented by a social media presence that amplifies the messages delivered. While the air component is unlikely to be the lead for such operations, absent the development of an Information Corps or Information Force, Airmen will likely find themselves developing social media strategies both to discover (Publicly Available Information) or deliver, especially to counter foreign active measures. None of these types of operations come as a surprise given the many historical examples of these operations. However, as the USAF re-invigorates IW, it must evaluate its readiness to perform these tasks. An optimal organizational model, centralizes the assets used to perform these tasks under a single wing commander.

To prepare for MCO, the USAF must organize, train, and equip to conduct both Offensive and Defensive IW to achieve information superiority in support of key JFACC roles. Joint doctrine (JP 3-30) lists several to consider: airspace control authority (ACA), area air defense commander (AADC), and space coordinating authority (SCA).

Within the ACA role, the JFACC "assume[s] the overall responsibility for the operation of the airspace control system (ACS)" and uses that system "to reduce the risk of friendly fire incidents, enhance air defense operations, and permit greater flexibility of operations." Since the

ACS is an information system, it implicitly requires IW support. Within theater, Airmen must operate, secure, and defend the ACS across digital datalinks and other elements of the communication system (EMS and Cyberspace). Further, airmen must evaluate the information acquired by radars and other sensors to enable "comprehensive air defense identification procedures and rules of engagement." In accordance with NIST's Cybersecurity Framework, forces must detect and respond to threats to the ACS. While forces assigned to theater can and should perform the identification and protection functions, global detection and response must be centrally coordinated.

A global Network Security Operations Center (NSOC) is required to perform global detection and response to threats to the ACS in both the EMS and Cyberspace. The NSOC must be comprised of "security analysts organized to detect, analyze, respond to, report on, and prevent [EMS and/or cybersecurity] incidents." The NSOC should perform "real-time triage of alerts, as well as fielding phone calls from users and other routine tasks." If it becomes necessary, the NSOC can task a subordinate unit to perform incident analysis to remedy the problem. To organize effectively then, subordinate to the NSOC must be an Information Warfare Wing (IWW) focused on Defensive Cyberspace Operations, DOD Information Network (DODIN) Operations, and Electronic Protection (EP) of the EMS. The defensive IWW may then perform critical functions across the EMS and Cyberspace to build and extend the ACS and protect or respond to threats (malware analysis, red teaming, Electronic Warfare Integrated Reprogramming, etc). Finally, those airmen assigned to tactical units to perform local cyberspace and EMS defense should be under the operational control of the NSOC (the tactical commander retains tactical control) to report anomalous or suspicious activity to create a comprehensive global defense of the ACS architecture.

While IW support to the JFACC's ACS role is clearly more defensive in nature, the IW support to the AADC and SCA roles are decidedly more offensive. The AADC role seeks to protect the JFC's Defended Asset List (DAL). However, due to the Defensive Counterair (DCA) missions' dependency on air superiority, in a contested environment, within his or her AADC role, the JFACC must also "make [Offensive Counterair (OCA)]… recommendations to help counter the air and missile threat." SCA only explicitly authorizes the JFACC to coordinate "specific space functions and activities" by "request[ing] and integrat[ing] theater-specific space operations and capabilities." However, there is an implicit relationship between the AADC and SCA, specifically to counter threats to space. Therefore, based on the responsibilities of the AADC and SCA, the JFACC is concerned with three aspects of the adversary: Air and Air Defense, Space and Counterspace, and Ballistic Missile Launch and Defense. Each of these systems inherently have their own information system in accordance with RAND's information system breakdown. (Figure 5)

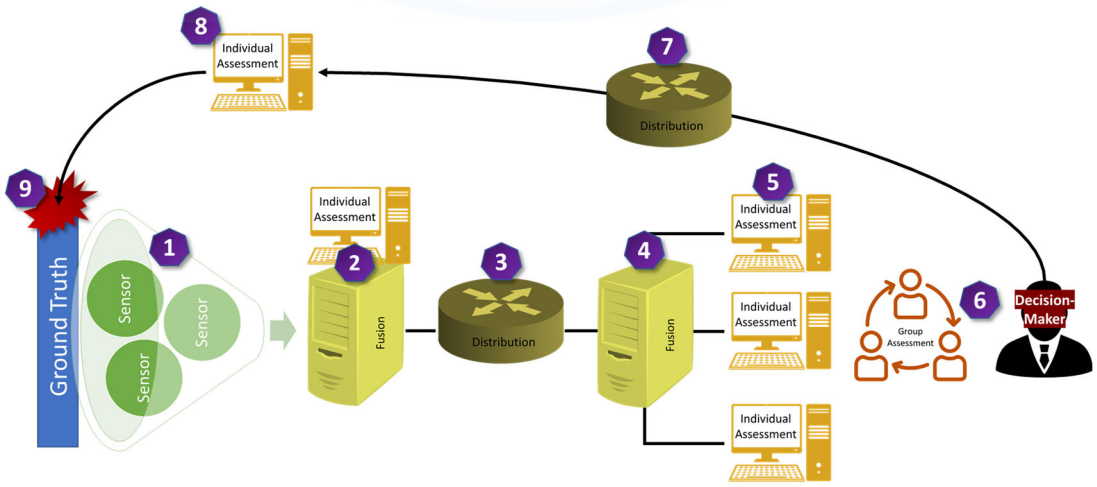

Figure 5. Author's Overview of a JFACC Target Information System

Bednar, Davitch, and Treadwell conduct an excellent breakdown of Integrated Defense Systems to consider in our analysis. “At its heart, an integrated air defense system (IADS) is a command and control organization, not a loose assembly of radars, control centers, and weapons.” Figure 5 applies the RAND C4ISR Model to a JFACC’s Target Information System. The sensors [1] and fusion & individual assessment [2] portion of the IADS constitute Air Surveillance. “Air Surveillance can employ a variety of sensors from visual observers wielding binoculars and a radio, to sophisticated radars capable of determining the precise location of a target in three dimensions.” In the case of space, Air Surveillance is replaced by Space Object Surveillance and Identification (SOSI). Air and space include battle management “comprised of the information fusion centers [4] that ingest, process, and analyze [5] surveillance data in order to recommend engagement courses of action to decision makers [6].” Once a course of action is selected, the decision is distributed [7] to another individual [8] charged with weapons control. In accordance with the decision-maker’s direction, “he or she may respond with fighter aircraft, surface-to-air missiles, air defense artillery and/or electromagnetic effects [9].”

At the heart of the effectiveness of these systems (air/air defense, space/counterspace, and ballistic missile launch/defense) is their integration. “Integration is made possible today by redundant, reliable command and control networks.” IW in support of the AADC and SCA roles of the JFACC should target the command and control networks through combined information fires. Bednar, Davitch, and Treadwell say it best:

> *“Any action taken to drive air defense components to an independent state is beneficial because it limits their integration. Therefore, one may see the benefits of viewing adversary defenses as part of a system and finding vulnerabilities within it. Using synchronized non-kinetic and kinetic effects to divide and isolate… system components represents the future of… operations.”*

To present forces capable of planning and executing these operations in support of the JFACC, the USAF must task-organize to develop airmen capable of understanding all IW

capabilities while retaining target expertise. This requires a fundamental reshaping of the AF approach to Information, Cyberspace, ISR, and EMS organization. Historically, the USAF developed functional expertise over the course of a career. EMS professionals were developed out of aircrew to become a specialized expert for their platform. Cyberspace professionals were predominately intended to build networks across which Command and Control (C2) and ISR data could flow out to the tactical edge. Since United States Cyberspace Command (USCYBERCOM) activated, emphasis on developing Offensive Cyberspace Operations (OCO) specialists increased. Information Operations was nearly a dead career field until it re-emerged in the last half decade.

Today, the AF stands significantly under-skilled in the behavioral sciences. The critical skillset is necessary for defending or exploiting the human component of the decision-making process. Additionally, ISR professionals have developed within their own stovepipes; today emphasizing development within intelligence disciplines or in support of specific functions: Cyberspace, Space, Air, or Special Operations Forces (SOF). These development strategies were complemented by functionally-aligned organizations to enable experiential career paths that were supported by training and education focused on the functions discussed above. To be clear, this is not an indictment of that approach. Rather, the USAF must evolve its approach. At the service level, the USAF embraced IW re-organization and career development via the new organization and an IW career field category. It should consider evolving its associated Wing structure.

To develop the required expertise in JFACC target information systems, the USAF should take a target-centric approach to its Wing and below organization. For example, it could establish a United States European Command (USEUCOM)-aligned IWW. The USEUCOM-aligned IWW would possess (1) the OCO forces presented to USCYBERCOM allocated to

support USEUCOM; (2) EMS, Cyberspace, and Information forces responsible for developing waveforms, tailored messages, or cyber tools in support of USEUCOM priorities; and (3) ISR professionals responsible for conducting Intelligence Preparation of the Environment (IPOE) and Target Systems Analysis (TSA). The Wing Commander would coordinate with the AOC for reachback support, the Intelligence Community to develop organizational relationships with key offices, and USCYBERCOM to present ready OCO forces within his or her command. Prior to the outbreak of conflict, the Wing Commander may focus on developing the IPOE, TSA, and requisite tools and capabilities required to be effective on a potential D-Day. To complement the active duty wing, the AF should then align Air National Guard and Air Force Reserve units to the Wing. Through Total Force Integration (TFI), the Wing would possess the requisite forces for activation and, if necessary, deployment to the AOC or the JOC, if competition transitioned to conflict.

By creating a functionally diverse, target-centric organization, the USAF can deliberately develop Airmen to understand a target information system. While traditional air operations employ a common capability against diverse targets, IW requires tailored capabilities for employment against unique targets. Training and education can be employed to bring someone to a familiar or proficient level in an IW functional competency (Behavioral Science, EMS, Intelligence, Cyberspace) but only experience over an extended period-of-time can provide the requisite target expertise required to lead an IW campaign. Target-centric task organization thus satisfies CSAF Focus Areas #2 and #3 by strengthening joint leaders and teams through combined information arms and enhancing multi-domain operations by tying all of IW together.

Conclusion

In conclusion, the world order is once again in the midst of a Great Power Competition. The USAF is taking important steps towards the re-invigoration of Information Warfare to take on the challenge. The activation of the new Information Warfare organization provides an opportunity for it to do so. The integration of Cyberspace, EMS, ISR, and Information operations through combined information fires to attack adversary information systems or defend our own constitutes Information Warfare. Information Warfare's objective is to gain and maintain information superiority. To do so, the USAF must understand information systems as targets made up of data, systems, and people. The vulnerable points of those systems can be organized into four broad categories: confidentiality, integrity, availability, and trust. Whether prior to conflict or in support of the JFC during MCO, the USAF must be ready to present forces to conduct offensive and defensive Information Warfare in support of key JFACC roles: Airspace Coordinating Authority, Area Air Defense Commander, and Space Coordinating Authority.

First, the USAF should organize the assets that employ airpower to deliver or detect waveforms under the leadership of a Wing Commander(s) charged with training and equipping the associated Airmen. Second, it should organize around Defensive Information Warfare by establishing a global NSOC to task a subordinate defensive Information Warfare Wing to train and equip Airmen to conduct Defensive Cyberspace Operations, Electronic Protection, and Department of Defense Information Network operations to build, extend, protect, and respond to threats to the global ACS architecture. Finally, in support of the JFACC's role as the Area Air Defense Commander and Space Coordinating Authority, the USAF should design target-centric Information Warfare Wing's comprised of Offensive Cyberspace Operations, Information, EMS, and ISR forces. Taking these actions enable will increase USAF readiness "to win wars of cognition."

"Opinions, conclusions, and recommendations expressed or implied within are solely those of the author(s) and do not necessarily represent the views of the Air University, the United States Air Force, the Department of Defense, or any other US government agency. Cleared for public release: distribution unlimited."