Research Report

ELIZABETH BODINE-BARON, JONATHAN FUJIWARA

Challenges to Achieving Information Warfare Convergence in the U.S. Air Force

This publication has completed RAND's quality-assurance process but was not edited.

For more information on this publication, visit **www.rand.org/t/RRA771-2**.

Published by the RAND Corporation, Santa Monica, Calif.

About This Report

This report summarizes the major challenges facing the U.S. Air Force (USAF) as it attempts to mature information warfare (IW) forces and capabilities. The findings and recommendations documented here were developed as part of a larger project titled "Intelligence Support to the Air Force Information Warfare Enterprise" sponsored by the Assistant Deputy Chief of Staff for Cyber Effects Operations, Headquarters U.S. Air Force (HAF A2/6). The objective of this project was to make recommendations for the USAF to better meet operational needs in the information domain against a competitive adversary, with a particular focus on intelligence support to the USAF IW Enterprise. It was conducted between August 2020 and November 2021within the Force Modernization and Employment Program of RAND Project AIR FORCE. It should be of interest to information warfare professionals in the USAF, those involved in or supporting operations in the information environment across the Department of Defense, as well as senior leaders tasked with developing policy or prioritizing resources related to information warfare. An accompanying report, "Improving Intelligence Support to Air Force Information Warfare and Integrating Information into Air Force Operations," not available to the general public, summarizes findings and recommendations related to key intelligence questions and processes for IW.

Project AIR FORCE

RAND Project AIR FORCE (PAF), a division of the RAND Corporation, is the Department of the Air Force's (DAF's) federally funded research and development center for studies and analyses, supporting both the United States Air Force and the United States Space Force. PAF provides the DAF with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future air, space, and cyber forces. Research is conducted in four programs: Strategy and Doctrine; Force Modernization and Employment; Workforce, Development, and Health; and Resource Management. The research reported here was prepared under contract FA7014-16-D-1000.

Additional information about PAF is available on our website: http://www.rand.org/paf.

Acknowledgments

Many people within the Department of the Air Force and the U.S. intelligence community, as well as colleagues in academia and the private sector, contributed to this report. We would like to especially thank our sponsors in HAF A2/6, Brigadier General Robert K. Lyman and Mr. Kenneth Bray, as well as Mr. Dale Benedetti at NASIC, for spearheading this effort and offering

critical guidance along the way. Mr. Rob Mussen, Major Michael Stamat, and Major Raymond Sealey supported the project as the main point of contacts and project monitors.

We are also grateful for the collegial interactions and valuable inputs we received from the Department of Defense Strategic Multilayer Assessment program as part of the Integrating Information into Joint Operations project. We benefited enormously from the inputs of subject matter experts at HQAF, ACC, 16AF, AFOSI, and NASIC; while there are too many to list here, we note that this work could not have been conducted without their enthusiastic participation.

At RAND, we would like to thank our colleagues Quentin Hodgson, Tracy Krueger, Hilary Reininger, Christopher Ferris, Christopher Paul, Michael Schwille, and Paul Emslie for their contributions to our analysis. We would also like to thank Alyssa Demus and Jim Williams for their very thorough reviews and helpful suggestions to improve this report.

That we received help and insights from those acknowledged above should not be taken to imply that they concur with the views expressed in this report. We alone are responsible for the content, including any errors or oversights.

Summary

Issue

The United States is facing a rapidly growing and evolving threat in the information environment as peer and near-peer adversaries compete to gain military, political, and economic advantages. In order to compete efficiently and effectively, as well as to ensure success in any future military conflict, the U.S. Air Force (USAF) needs to be able to integrate non-kinetic capabilities and conduct information warfare (IW).

In 2019, the Air Force reorganized—through the establishment of 16th Air Force as the service's IW Wing and the merger of AF/A2 and AF/A6 at the Headquarters Air Force level—in order to better strategize, organize, train, and equip for IW. These organizational changes present an opportunity for the Air Force to configure and streamline its information warfare capabilities to fight and win in the information domain against a challenging adversary. However, gaps across the DOTMLPF-P spectrum need to be systematically identified and addressed for the Air Force to fully take advantage of opportunities enabled by these freshly configured organizations. In parallel with other efforts in the USAF and Joint community, this research aimed to provide recommendations to better meet operational needs in the information domain against a competitive adversary.

Approach

To understand the challenges facing the USAF regarding enabling IW, the RAND team reviewed existing documentation (including published and draft documents) such as Department of Defense (DoD) and USAF strategy and doctrine as well as prior and ongoing IW research in government and academia. The team also conducted interviews with USAF and DoD subject matter experts, surveyed private industry approaches relevant to IW, and analyzed trends in IW personnel within the USAF. Based on this input, the team developed an information framework and created use cases to illustrate potential future force structures to enable IW. This report summarizes the findings and recommendations from the interviews and literature review analysis, focusing on the major challenges facing the Air Force as it matures IW.

Key Findings

- While changes are occurring in all levels of policy and doctrine, information related efforts are not synchronized, and vary across the Services. Even within the USAF there remains much confusion about the role of information in operations.

- The definition of information warfare poses a challenge, as multiple terms and overlapping concepts result in confusion and hinder implementation. Two separate and somewhat competing concepts, “information warfare” and “operations in the information environment” (OIE), have led to substantial divergence about interpretation. As a result, the debate becomes about the definition rather than how to move forward with integration.
- IW is not resourced adequately, either in terms of capabilities or personnel. IW capabilities do not usually survive the planning, programming, budgeting, and execution process as they are often split between multiple panels and do not have a single strong advocate.
- There are also simply not enough personnel trained and experienced in IW to meet the USAF’s needs. The main officer Air Force Specialty Code (AFSC) for IW, 14F, is relatively recent and still very small workforce.

Recommendations

- Standardize the USAF lexicon and approach to information, leveraging the proposed RAND Information Framework
- Designate a single person or office as the lead for championing IW and integrating information into operations, allowing airmen to look to one place for guidance
- Continue to grow and expand the 14F career field
- Provide cross-functional training to make every Airman “information aware”
- Leverage table-top exercises and wargames to explicitly explore organizational constructs for presenting IW capabilities and demonstrate the value of IW to USAF missions
- Establish a program element or specific panel for resourcing IW capabilities

Contents

Figures and Tables

Figures

Tables

Chapter 1. Information in Operations

Though the terms used to describe the concept have changed, information has always been an integral part of war. During World War II, *Operation Fortitude* was a pivotal information campaign that shaped the Axis Powers' perceptions and thereby actions in a way that enabled the Allies to successfully land on the beaches of Normandy[1]. The Allies were successful in conducting an offensive against a formidable and entrenched adversary because they dedicated the resources and priority to creating a deceptive information environment (IE) that enabled combat maneuver.

As the U.S. military matured post World War II, it primarily viewed IE as the methods and modes of transporting data[2]. Investments in this part of the U.S.' military arsenal resulted in capabilities that enabled the transport of Blue force data and capabilities that affected the transport of Red force data. An information transport advantage coupled with superior technology and military have been key to U.S. military success in conflicts against nations with less adequately trained and equipped militaries. In the most recent US conflicts in the Middle East, treating operations in the information environment not as an integral part of combat operations but rather ancillary activities have resulted in a less than desirable outcome.

As the U.S. postures to ensure the Department of Defense (DoD) remains a formidable force in the face of rapidly advancing adversaries, there has been a realization that the kinetic combat military capabilities that have been heavily relied on thus far may not be sufficient in the face of potential conflict with a diverse set of global threats. The increasing recognition and employment of activities in all domains below the level of conflict has also emphasized the need for the U.S. to maintain its information advantage to remain a dominant power on the global stage. Near peer nation states have taken note of the U.S. reliance on superior military might and a significant information transport advantage and have developed strategies and new capabilities to close those gaps and reduce the U.S. advantage. This has resulted in the DoD turning to a re-emergence of information warfare to offset near peer gains in military capability and compete more effectively and efficiently.

---

[1] Bickell, Craig, "Operation FORITUDE SOUTH: An Analysis of its Influences upon German Dispositions and Conduct of Operations in 1944," *War & Society*, Vol. 18, No. 1, May 2000, pp. 91-121. As of September 26, 2022: https://doi.org/10.1179/war.2000.18.1.91.

[2] Chairman of the Joint Chiefs of Staff, "Joint Publication 3-13: Joint Operations", 27 November 2012 Incorporating Change 1 20 November 2014.

Information in a Joint Context

As part of the DoD maintaining a strategic advantage over near peer competitors, information was added as a joint function in 2017 to the original functions of command and control, intelligence, fires, movement and maneuver, protection, and sustainment.[3] This comes with the realization that the information environment is more than a data transport concept and that all military activities produce information. The intent of adding information as a joint function is to provide the joint force the ability to understand and leverage the pervasive nature of information, its military uses, and its application during all military operations.[4]

As a joint function and part of the operational environment, information in conjunction with intelligence includes determining relevant actor perceptions, attitudes, and decision-making processes. This requires an understanding of cultures, history, and narratives with knowledge of the means, context, and established patterns of adversary communications. As a joint function, there are efforts to have information move from simply being a supporting activity in the form of the traditional information related capabilities but an inherent and crucial part of all military activities.

Because all military actions affect the information environment, commander's decision processes need to be informed by the status of the current information environment and consider how actions affect the information environment. Joint Publication 3-04[5] builds from Joint Publication 3-0's doctrinal concepts for how information plays a role in joint operations. Ultimately, the past few years have demonstrated a shift from thinking about information as an afterthought to making it the starting and ending points of military planning and execution.

Air Force Approaches to Integrating Information

In April 2019, General Mike Holmes, then commander of Air Combat Command (ACC), announced the merger of the 24th and 25th numbered Air Forces into one numbered air force (NAF) to "better integrate cyber effects, intelligence, surveillance and reconnaissance operations, electronic warfare operations and information operations."[6] The 16th Air Force was subsequently formally activated on October 11, 2019, at Joint Base San Antonio-Lackland in Texas as an "information warfare-focused numbered air force."[7] The idea behind this merger was to take advantage of how the Air Force had already integrated cyber and intelligence, surveillance, and

---

[3] Office of the Secretary of Defense, "Information as a Joint Function", September 15, 2017.

[4] Chairman of the Joint Chiefs of Staff, "Joint Publication 3-0: Joint Operations", 22 October 2018.

[5] Chairman of the Joint Chiefs of Staff, "Joint Publication 3-04: Information in Joint Operations", September 2022.

[6] Air Combat Command Public Affairs, "ACC announces 24th and 25th NAF merger", April 5, 2019.

[7] Sixteenth Air Force Public Affairs, "Air Force integrates missions, strengthens information warfare capabilities", October 11, 2019.

reconnaissance (ISR) capabilities, and expand that integration into other areas such as electronic warfare (EW) and information operations (IO). In several ways, the integration effort has been successful, but challenges remain that need to be overcome order to fully take advantage of this new approach, as we will discuss further in the next chapter.

Chapter 2. Challenges Facing the Air Force

In this chapter we describe some of the key challenges facing the U.S. Air Force as it attempts to integrate information into Air Force operations. These challenges can be binned in to three main categories: policy (including leadership), personnel, and resources. The findings presented here were derived from a series of interviews and conversations with subject matter experts, senior leaders, operators, and analysts involved in developing USAF information warfare capabilities and forces, as well as an interview with subject matter experts from the Joint community.[8] We summarize the set of interviews in the table below.

Table 2.1 Summary of Interview Sources

MAJCOM/NAF		Headquarters Air Force		Other	
Air Combat Command (ACC)	7	HAF A2/6	4	OSI	1
16th Air Force	10	HAF A3	4	NASIC	4
AETC	1	HAF A5	2	JIOWC	2

We note that there are also other efforts within the Air Force to identify and overcome these challenges; namely, the development of Command and Control for Operations in the Information Environment (C2OIE), led by HAF A3,[9] and USAF-funded project, "Integrating Information into Joint Operations (IIJO)," conducted by the Strategic Multilayer Assessment group in Joint Staff J39.[10] Our analysis is meant to be complementary to those efforts.

The research method for these interviews included a protocol that focused on understanding how the organization being interviewed perceived what IW is, their organization's role within IW, and the challenges they perceived in pursing IW. The organizations that were interviewed were chosen due to their alignment to IW within the Air Force or the Greater Joint Force.

[8] Joint Information Operations Warfare Center

[9] Mulgund, Sandeep and General Mark D. Kelly, "Command and Control of Operations in the Information Environment: Leading with Information in Operational Planning, Execution, and Assessment", Air and Space Power Journal, Winter 2020. As of August 18, 2022: https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-4/SLP-Mulgund_Kelly.pdf

[10] Joint Staff J39, Strategic Multi-layer Assessment, "Strategic Multilayer Assessment - Integrating Information in Joint Operations (IIJO)", October 26, 2020. As of August 18, 2022: https://apps.dtic.mil/sti/citations/AD1118926.

Policy and Lexicon

Perhaps the biggest challenge facing the Air Force as it moves to fully integrate information into operations is how to define the concept. While on the surface this might seem like a minor issue and simple to overcome, throughout our interviews we found that it is the number one disagreement among stakeholders, resulting in confusion and hindering implementation.

Over the past decade, Joint doctrine and USAF policy have both evolved with respect to information and may even be diverging. From the Joint perspective, we note that "information warfare" is deliberately not defined, and "information operations" is becoming a legacy term. The currently approved Air Force definition of "information warfare," shown in Table 2.2, emphasizes military capabilities, mirroring earlier versions of Joint doctrine rather than the current approach which focuses on information as a Joint function. While some difference in definitions is to be expected as Services tailor Joint doctrine to their specific needs and operations, for the Air Force, the churn in Joint doctrine has resulted in two separate and somewhat competing concepts: information warfare and operations in the information environment.

Table 2.2 Information-Related Terms and Definitions

Term	Source	Definition
Information	JP 3-04	"Data in context to which an observer assigns meaning"
	HAF A2/A6[11]	Stimuli that have meaning in some context for its receiver
Information Environment (IE)	JP 3-04	"The aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information"
	HAF A3[12] HAF A2/6	The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information
Information Warfare (IW)	HAF A3 HAF A2/6	The employment of military capabilities in and through the information environment (IE) to deliberately affect adversary human and system behavior and to preserve friendly freedom of action during cooperation, competition, and conflict.
Operations in the Information Environment (OIE)	JP 3-04	"Military actions involving the integrated employment of multiple information forces to affect drivers of behavior"
	HAF A3 HAF A2/6	The sequence of actions that use information to affect behavior by informing audiences; influencing external relevant actors; and affecting information, information networks, and information systems.

[11] Air Force Operations in the Information Environment Tiger Team. "United States Air Force Operations in the Information Environment Report". October 2019.

[12] Head Quarters United States Air Force A3. MEMORANDUM FOR:C2 of Operations in the Information Environment (OIE) Working Group. 15 September 2020.

Information Operations (IO)	JP 3-04	Legacy term - removed
	HAF/A3	The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.

Although there are only nuanced differences between the definitions of IW and OIE, we discovered through interviews with USAF senior leaders that there is a substantial divergence about the interpretation of and preference for the two concepts. The term IW tends to be used to describe an expansion of the classic information-related capabilities to include ISR and weather—a capabilities-centric approach to defining how to affect the information environment (IE). From interviews, RAND researchers found that it is perceived that OIE differs from IW by being described as the actions required to affect the IE rather than any specific capability—an operations-centric approach to defining how to affect the IE. The divergence between the two concepts has negative implications for the USAF's ability to fully incorporate information into operations. The debate has become about definitions, rather than about how to move forward with integration.

In addition, as units work towards integrating information into air operations, the absence of a concerted implementation effort outside of the 16th AF has resulted in confusion and hesitation to move forward. The challenge is not too few champions, but rather too many. Although there is some collaboration and coordination at various seniority levels within the Air Force (e.g., general officer steering groups, working groups, and task forces), this "coalition of the willing" is not enough to make up a unified approach. Each senior leader brings a perspective shaped by their current role and the equities they are charged with representing, thus focusing their attention on specific capabilities rather than on the larger question of how to make information a foundational part of Air Force operations. This diversity of perspectives makes it difficult to train and equip airmen to incorporate information into operations.

Personnel and Training

The second major challenge facing the Air Force as it moves forward with integrating information is that there simply are not enough people with the appropriate training and experience to develop and implement IW strategies. Several interviewees mentioned the need for more trained IW personnel, particularly the need for more trained officers in the newly created 14F career field (information operations). The first class graduating from the 14F IO initial skills training course in December 2020 consisted of only nine Airmen. Across the USAF, as of early 2021, there were only 135 officers in the 14F career field. While we expect this pipeline to increase, it is currently too small to meet the demand across the USAF for Airman capable and comfortable to plan for and conduct operations in the information environment.

Increasing the pipeline will require not only resources and prioritization of training for USAF personnel engaged in IW capabilities (cyber operations, IO, ISR, EW, etc.), usually referred to as "IW Professionals," but also an increase in IW-related training for all Airmen. Acknowledging that all operations, kinetic and non-kinetic, affect the information environment implies that all Airmen need to at least be aware of IW and OIE concepts, though not proficient in the use of IW capabilities. Some interviewees noted that the Air Force performs well when it comes to training and developing cyber personnel, particularly by leveraging relationships with Cyber Command (CYBERCOM) and the National Security Agency (NSA), so perhaps a similar approach with leveraging relationships with Special Operations Command (SOCOM) and the Army would increase access to IW-related training.

Like some of the gaps between intelligence analysts and cyber operators that have been discovered in prior research,[13] there is a similar gap between those conducting IW operations and the analysts providing the intelligence support to them. In some cases, warfighters do not know how to ask questions that are answerable by intelligence analysts, and in others, the close relationship between operational and support units, and the larger IC, may not even exist. For example, supporting intelligence analysts may not be fully aware of actual IW capabilities, plans, and programs due to classification and Title 10/Title 50 constraints. In a few instances, we found that individual units may have been able to leverage informal networks to gain access to the right support and analysis within the IC, usually through prior postings within CYBERCOM.

From the intelligence perspective, we found that there is sometimes a lack of understanding of the need for convergence of different IW capabilities, and the challenges posed by increasing demands for intelligence products related to diverse questions and especially cross-cutting issues where deep technological expertise is needed. Overall, interviewees pointed to the need to have a better understanding of how our adversaries think and operate in the information environment to better conduct IW. Increased collaboration and contact between IW operational units and NASIC (and other parts of the IC) may go a long way to improving the quality and quantity of intelligence support provided.

Resources

The third challenge facing the Air Force with respect to IW is scarce resources, especially with respect to the prioritization of requirements for IW capabilities. Interviewees noted that required capabilities that are not currently adequately resourced include but are not limited to the following:

[13] Snyder, Don, et al., "Wing-Level Mission Assurance for a Cyber-Contested Environment", RR-A580-1, RAND Corporation, 2021.

- Tools specifically for integrating IW capabilities into operational concepts as opposed to enabling them in isolation[14]
- Data visualization and collaboration platform for IW-related operations[15]
- Measures of effectiveness (not just performance) for operations in the IE and tools for tracking them
- Capabilities to merge strategic narrative building with IO execution
- Additional tools for data sharing and fusion across information "silos"

One area that could be improved is increased synergy from labs such as Air Force Research Labs and those developing the requirements for IW capabilities. In particular, the path for new capabilities to be fielded is not agile enough to respond to the rapidly changing needs of operators. One interviewee pointed out that coordinating Combatant Commander requirements at the national level would be helpful. There needs to be better understanding of the prioritization of IW requirements across Joint and Combatant Commands – what really is needed from an IW perspective and how should the AF prioritize those capabilities compared to other, non-IW needs?

The current fractured approach limits the USAF's ability to properly resource specific IW capabilities, much less those needed for integration into plans, programs, and training related activities. The Program Objective Memorandum (POM) process poses challenges since IW capabilities are sometimes split across multiple panels. Many of the capabilities needed to effectively sense and affect the IE are multi-use, and some support non- information functions in addition to the IW mission set. To be adequately resourced, IW requirements need to have a strong advocate throughout the POM process, something they currently lack. The next chapter provides recommendations for surmounting this resourcing challenge as well as those related to policy and personnel.

---

[14] For example, tools that help planners show how the IE might be affected by combining cyber, IO, and EW capabilities in a single integrated operation, as opposed to a specific lens showing only cyber, etc.

[15] We note that Project IKE is moving in the right direction by providing a visualization with operational architecture superimposed, but it is largely focused on cyber operations, not all IW capabilities. For more information on Project IKE, see Pomerleau, Mark, "A cyber tool that started at DARPA moves to Cyber Command", C4ISRNET, April 20, 2021.

Chapter 3. Recommendations

In this chapter we summarize a few recommendations that could help the USAF solve the challenges described earlier. Among these, the two most important are to designate a single voice to be the lead for integrating information across the Air Force and standardize the Air Force approach and associated lexicon.

Designate a Single Voice for Information Warfare

The USAF needs a unified voice to lead the development and full integration of information into air operations to address the policy, personnel, and resource challenges described above. Good will and good intentions will not be enough. One way forward would be for the Chief of Staff of the Air Force to designate a single person or office as the lead for integrating information into operations, allowing airmen to look to one place for guidance. While such a designation would of course require input and balancing of equities from different communities, it would go a long way toward resolving differences and would allow for unified forward movement. Several options exist, including delegating the authority for integration to an existing Air Staff position such as A2/6 or A3, expanding the mandate of a Secretariat office such as SAF/CN or SAF/PA to include integration, or even creating a new Air Staff position to focus exclusively on integration. Regardless of who or what office is chosen as the lead, our recommendation is that it be only one, and their responsibilities should include the following tasks.

Developing guidance on how the USAF will functionally integrate informational aspects into air operations. This guidance should consider that operations are the result of planning, concepts of employments, concepts of operations, training, and exercises. Guidance needs to be developed to make information an integral part of all these aspects. This guidance would also benefit current efforts to mature related doctrine.

Advocating for resources needed to affect the IE within the POM process. A single voice for resources will advocate for key priorities and help information-centric inputs survive the POM process.

Leading USAF efforts to develop the processes required to fully integrate information capabilities, including generating narratives. While the USAF has technical expertise in many of the individual capabilities that influence the IE, it lacks sufficient knowledge of what the overall narrative or message should be, and how to move beyond synchronization to full integration of capabilities to achieve a larger goal. Part of the solution for this challenge lies outside of the USAF. The overall U.S. narrative for foreign and domestic audiences must be driven by objectives set at the national level through a whole-of-government approach involving

other parts of the DoD, interagency, and IC. Even absent this whole-of-government leadership, though, the USAF needs a single point for the development and synchronization of narratives that shape the IE to meet USAF and Joint requirements.

Establishing and articulating USAF perspectives on information as a joint function to the Joint Force. Outside of the USAF, a designated lead for integrating information in operations would enable the USAF to present a single perspective to the Joint community, the DoD, and other parts of the USG, clearly articulating USAF policy, priorities, desired roles, and capabilities. Once the USAF gets its own house in order, it can better present its needs and become a leader in fully incorporating information as a foundational element in operations.

Standardize the USAF Approach to Information Warfare

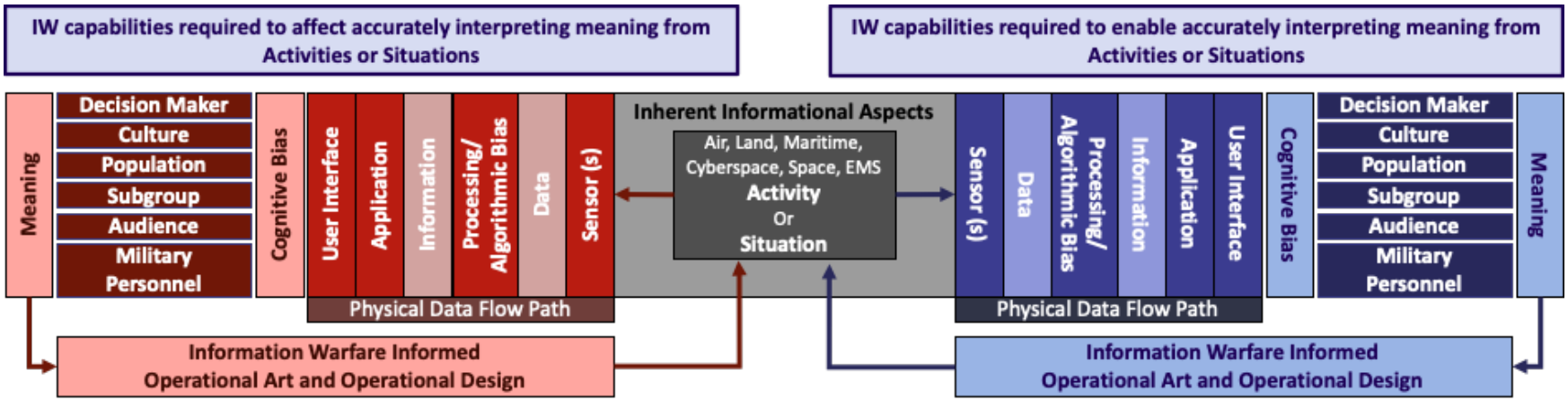
Interviews with senior Air Force personnel revealed that there are numerous definitions of information warfare and even more varying interpretations of the concept. Given this ambiguity, we developed a framework to provide a way to practically characterize the information environment so that a warfare approach can be taken to it.

Rather than relying on one of the current IW or OIE definitions, the framework is focused on the definition of information. Specifically, we draw on an idea gaining traction in joint doctrine, that "information is data in context to which an observer assigns meaning."[16] Data, then, are sensed inherent informational aspects. According to Joint Publication 3-04, "inherent informational aspects refer to the features and details that are characteristic of a situation or an activity…. used to derive meaning from that situation or activity."[17] These could include physical attributes, temporal characteristics, or anything else sensed by an observer.

With these definitions in hand, we can then fully describe the information environment by tracing its constituent parts: going from a physical world activity or situation to the cognitive meaning that is derived from that activity or situation. The specific components illustrated in the framework in Figure 3.1 can be customized to represent a particular information flow, noting that not every flow and every IE is the same. The framework is intended to be a basis upon which an analyst can build out and understand a specific portion of the IE.

[16] Chairman of the Joint Chiefs of Staff, "Joint Publication 3-04: Information in Joint Operations", September 2022.
[17] Ibid.

Figure 3.1. RAND Information Framework



Once the inherent informational aspects are observed the sensor produces data that represents the collected inherent informational aspects of the event. That data is transported along a physical data flow path to the observer. Along that path the data can be processed. This can include combining with other data, comparing data with database information, and/or applying algorithms to the data. This processing is part of what enables the data to be put into context at which point it becomes information.

The information that is presented to the observer usually comes from an application through a user interface. An observer then assigns meaning to the information, considering the context and circumstances within which the information is presented. As the user receives the information the observer's cognitive bias will also influence how meaning is assigned to the information. (In the case of a machine-based observer, the algorithms used to assign meaning create cognitive bias.) With this perspective in mind, we note that the IE is more than just a reflection of an event. It encompasses how the perception of that event is transformed by the mechanisms that present it and how it may be interpreted through the lenses of bias.

Note that the information an observer receives is most likely not going to be a complete or a fully accurate representation of the activity or situation. Even the most technologically advanced sensors cannot fully represent every aspect of reality; human perception provides even less. Additionally, the IE that informs one observer is likely going to present a different perspective of information for a given event when compared to the IE surrounding a separate observer. Even the exact same IE can still result in different meanings by two separate observers due to biases.

The RAND information framework presents a standardized way to dissect the information environment in such a way that it is useful for capabilities investment, providing situational awareness, and enabling operations. From a Blue perspective, analysts can leverage it to prioritize components of the IE for investment and defense, to enable the most accurate representation of events in such a way that supports the commander's operational art and design. From a Red perspective, it can be used to identify segments of the IE for attack or manipulation, to affect how an adversary observer assigns meaning to a given event in a way that meets Blue objectives.

Additional Recommendations

The USAF needs to continue to grow and expand the 14F officer career field. The current workforce is too small and too junior to meet the demand for IO professionals. Further investment is needed to add more officers, and special attention needs to be paid to their career development to ensure that they receive appropriate specialized training as well as have the opportunity for command positions.

As stated earlier, IW training should not be limited to IW professionals, i.e., those involved in the planning, support or execution of IW operations. All Airmen should be aware of how what they do affects the information environment, and in turn, how the information environment can affect their ability to perform the mission. Basic training in IW fundamentals to make all Airmen "IW-aware" is needed.

To demonstrate the value of information warfare to all Airmen and to USAF missions, it is necessary to realistically incorporate IW capabilities into exercises and training. For example, "white-carding" cyber operations has resulted in a perceived lack of trust in cyber effects to actually affect adversary systems when needed. Other IW disciplines, such as IO, need to be fully incorporated into exercises so that Airmen understand not only how an adversary can affect them through the information environment, but also how to effectively plan for Blue IW operations. Table-top exercises and wargames should also be employed to explicitly explore various organizational constructs for presenting IW capabilities to combatant commanders in different scenarios, so that the USAF can ensure that it is moving in the right direction organizationally.

Finally, without resources, USAF IW capabilities and forces will never be able to achieve their full potential. Currently, most IW-related requests for resources do not survive the POM process, due to being split up and deprioritized across multiple panels. To solve this problem, the Air Force should consider establishing a specific program element for IW or creating an IW-specific panel. Such an approach would ensure appropriate attention is paid to IW capabilities together, rather than separately, and allow for more integration throughout the process.

Abbreviations

AFSC	Air Force Specialty Code
CYBERCOM	U.S. Cyber Command
DAF	Department of the Air Force
DoD	Department of Defense
EW	Electronic Warfare
IC	Intelligence Community
IE	Information Environment
IO	Information Operations
ISR	Intelligence, Surveillance and Reconnaissance
IW	Information Warfare
MILDEC	Military Deception
MISO	Military Information Support to Operations
NSA	National Security Agency
OIE	Operations in the Information Environment
OPSEC	Operational Security
PAF	RAND Project AIR FORCE
PAI	Publicly Available Information
POM	Program Objective Memorandum
SOCOM	U.S. Special Operations Command
USAF	United States Air Force

References

Air Combat Command Public Affairs, "ACC announces 24th and 25th NAF merger", April 5, 2019. As of October 28, 2021: https://www.af.mil/News/Article-Display/Article/1806838/acc-announces-24th-and-25th-naf-merger/

Bickell, Craig, "Operation FORITUDE SOUTH: An Analysis of its Influences upon German Dispositions and Conduct of Operations in 1944," *War & Society*, Vol. 18, No. 1, May 2000, pp. 91-121. As of September 26, 2022: https://doi.org/10.1179/war.2000.18.1.91.

Chairman of the Joint Chiefs of Staff, "Joint Publication 3-0: Joint Operations", 22 October 2018.

Chairman of the Joint Chiefs of Staff, "Joint Publication 3-04: Information in Joint Operations", September 2022.

Chairman of the Joint Chiefs of Staff, "Joint Publication 3-13: Joint Operations", 27 November 2012 Incorporating Change 1 20 November 2014.

Joint Staff J39, Strategic Multi-layer Assessment, "Strategic Multilayer Assessment - Integrating Information in Joint Operations (IIJO)", October 26, 2020. As of August 18, 2022: https://apps.dtic.mil/sti/citations/AD1118926.

Mulgund, Sandeep and General Mark D. Kelly, "Command and Control of Operations in the Information Environment: Leading with Information in Operational Planning, Execution, and Assessment", Air and Space Power Journal, Winter 2020. As of August 18, 2022: https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-4/SLP-Mulgund_Kelly.pdf

Office of the Secretary of Defense, "Information as a Joint Function", September 15, 2017.

Pomerleau, Mark, "A cyber tool that started at DARPA moves to Cyber Command", C4ISRNET, April 20, 2021. As of August 18, 2022: https://www.c4isrnet.com/cyber/2021/04/20/a-cyber-tool-that-started-at-darpa-moves-to-cyber-command/

Sixteenth Air Force Public Affairs, "Air Force integrates missions, strengthens information warfare capabilities", October 11, 2019. As of October 28, 2021: https://www.af.mil/News/Article-Display/Article/1987970/air-force-integrates-missions-strengthens-information-warfare-capabilities/

Snyder, Don, et al., "Wing-Level Mission Assurance for a Cyber-Contested Environment", RR-A580-1, RAND Corporation, 2021.