

Strengthening Information Warfare Capability and Capacity: The Case for Information Operations Warrant Officers in the U.S. Army

CW4 William Bryant, Special Forces

The United States Army is at a pivotal point in its evolution, facing unprecedented challenges in modern warfare. With increasing threats from cyber and space domains, including the information and cognitive dimensions, the information environment (IE) has morphed into a complex space where information advantage can shape and dictate outcomes. To navigate this increasingly intricate terrain, the Army must evolve its personnel structure by establishing a specialized role for Information Operations Warrant Officers (IOWOs). This article posits that establishing IOWOs will cultivate enduring and dedicated information professionals beyond the Army's Functional Area 30 (FA30) Information Operations (IO) Officers, significantly strengthen the Total Army's effectiveness from competition to large-scale combat operations (LSCO), and enhance information advantage in multidomain operations (MDO).

To establish the IOWO within the Army, senior decision-makers must understand the urgency and significance of this initiative. This proposal uses established doctrine and processes to facilitate a collaborative and unified approach to developing an IOWO. A thorough understanding of IO should underpin the advocacy for creating IOWOs, ensuring that transparency and accountability remain central to the decision-making process. A deep understanding of strategic Army policy and systems thinking will be essential in navigating the complexities and challenges of implementing this crucial role. By evaluating this concept through the Army's Capabilities-Based Assessment (CBA) process and recommending changes through Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P), the Army can foster a more resilient, adaptable, and informed force capable of meeting contemporary and future IE challenges (Department of the Army, 2021).

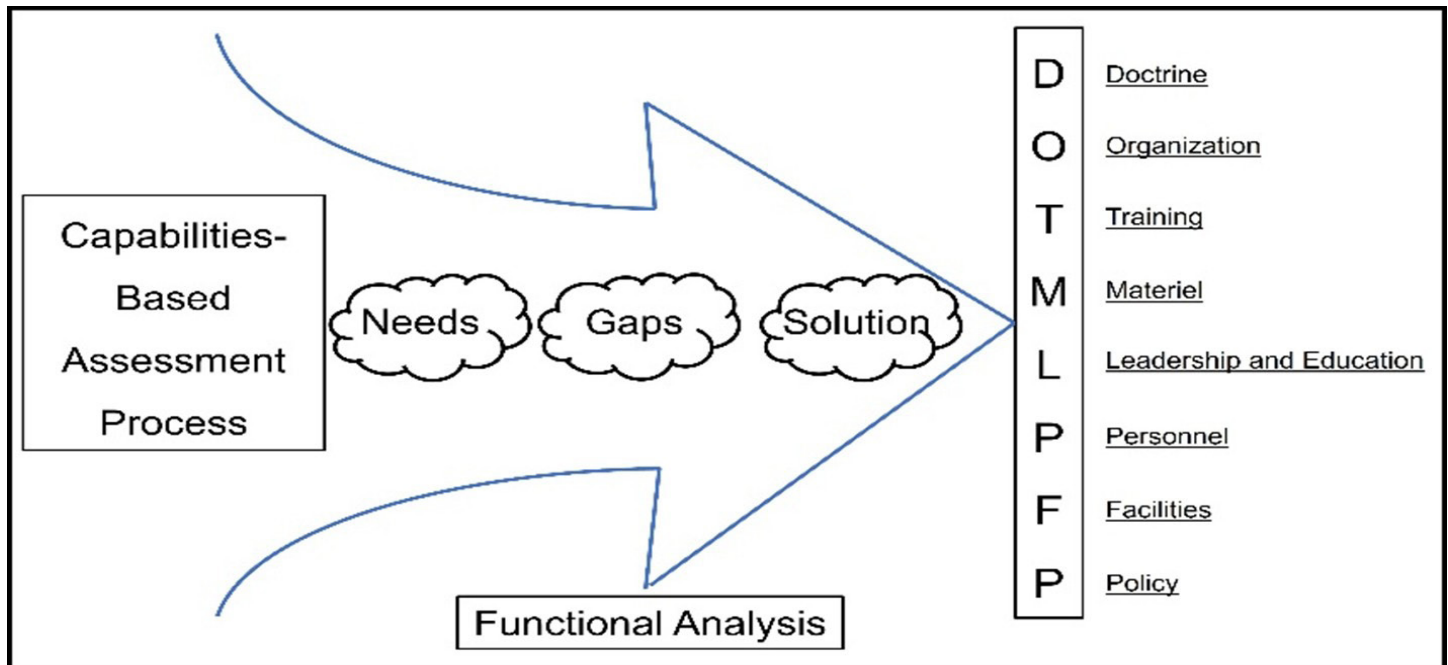


Figure 1. The CBA Process. Created by author from Department of the Army. (2021). How the Army runs: A senior leader reference handbook. Army Publishing Directorate.

The Imperative of Information Operations

IO has transcended the conventional purview of warfare, incorporating emerging technology into operations in the information environment (OIE). Effective IO requires a sophisticated integration of psychological operations (PSYOP), electronic warfare, cyber capabilities, and other influence activities that aim to influence perceptions and enemy decision-making processes (Armistead, 2004). This complexity is echoed by Qiao Liang and Wang Xiangsui (1999), who argue that concepts like unrestricted warfare venture far beyond traditional battlefields, using information and cyberspace to deceive, disrupt, and attrit the enemy. The contemporary IE underscores the necessity for dedicated, highly skilled professionals who can effectively manage and employ diverse capabilities like deception, influence, propaganda, precision messaging, and targeted information campaigns.

In an era characterized by rapid technological advancements, the need for a structured approach to information warfare against human and system behavior is critical (Dept of the Air Force, 2023). The selective use of information can shape how history is interpreted and presented, significantly affecting our understanding of events (Gaddis, 2002). This underscores the importance of recognizing how IO narratives can influence perceptions, manipulate public opinion, and shape political or military outcomes in information warfare. The flow of information and the timing of its dissemination can influence or disrupt enemy decision-making, create uncertainty, and manipulate perceptions on the battlefield (Leonhard, 2017).

The recognition of information forces in Joint and Army doctrine highlights the criticality of those units and codifies it in recent publications like ADP 3-13 (2023) and JP 3-04 (2022). However, current structures often leave a gap in sustained expertise and tactical execution, particularly at lower echelons of command. In the age of rapid communication, understanding and leveraging information force capabilities is as crucial as traditional military tactics. Joint doctrine currently identifies the following types of information forces: PSYOP, Civil Affairs, Public Affairs, Electromagnetic Spectrum Operations (EMSO) units, Cyber forces, and Space forces (Joint Chiefs of Staff, 2022). Current Army IO doctrine includes the same forces and adds FA30 to the Army's list of information forces (Dept of the Army, 2023).

Analyzing the Current Model: FA30 vs IOWO

The Army relies heavily on the FA30 community (CPT, MAJ, LTC, and COL) for IO integration. While FA30s are trained to perform crucial information-related tasks, this model has inherent limitations. The broad scope of responsibilities assigned to FA30 Officers can dilute their focus, leading to a lack of depth in the specialized areas essential for effective information warfare. Additionally, the rotation and transition of FA30s can create inconsistencies in organizational knowledge and continuity.

In contrast, establishing an IOWO professional would fill critical gaps by providing dedicated personnel who can integrate IO into broader operations consistently, at the echelon, and with a longer time in a unit. These warrant officers would serve not only as subject matter experts but also as commissioned officers and trainers who can integrate, communicate, operate, lead, and advise (ICOLA) on information targeting, ensuring that the Army possesses a cohort with experience and knowledge in managing the multifaceted aspects of information warfare. The complexities of joint and combined operations highlight the need for better interoperability, especially in IO missions. The emerging threats posed by adversaries in cyberspace and information realms mandate that units operate cohesively to meet common objectives (Brose, 2020).

The integration of IOWOs would improve this interoperability by embedding information professionals

and technical IO experts within every level of tactical and operational planning. As noted in Air Force Doctrine Publication 3-13 (2023), the integration of IO across different domains enhances operational effectiveness for the Joint Force. By training IOWOs to serve as liaisons with joint and combined partners, the Army can ensure a more synchronized effort in MDO.

DOTMLPF-P: Building a New IOWO MOS

Figure 2 highlights a basic DOTMLPF-P model that can be used to further discussion and informed decision-making for the creation of the IOWO.

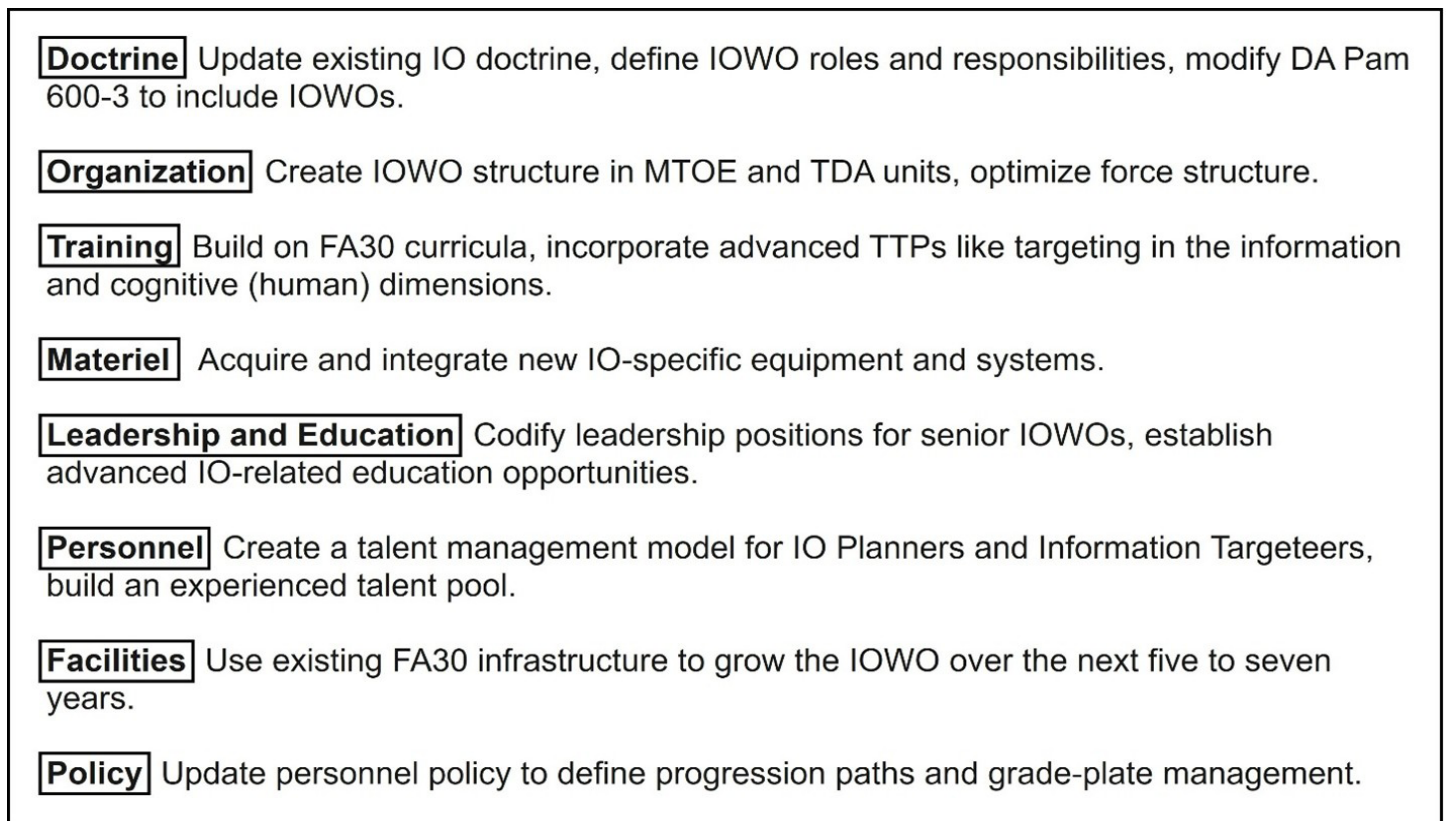


Figure 2. IOWO DOTMLPF-P. Note. Created by author. (2025).

Implementing an IOWO Career Development Model

Entry-level IOWOs will attend a Warrant Officer Basic Course that contains many of the same learning outcomes and training objectives that FA30s receive. These new IOWOs will be adept at integrating information into planning and target sets, serving as an Information Targeteer or IO Plans Officer for their respective commands. The recommendations outlined for career development are summarized in a proposed IOWO (370A) career development model (see figure 3). This 370A model displays an example of a 30-year career as an IOWO, with years of warrant officer service, PME, education and training, key developmental (KD) assignments, and broadening assignments.



370A Career Development Model

Rank	WOIC						WOAC					WOSC				WOMC															
Years	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
PME	WOBC		WOIC				WOAC					WOSC				WOMC															
Training and Education	Airborne MDPC Air Asslt OPSEC ASCBC		IWC SLJM JFC STO Planner Cyber Planner POQC				JIPC JTSC SOMILDEC JMTC DOPC					HTARC AMSP NDU / NPS PCC				Capstone education and seminars															
	Tactical IO training →						← Operational and Strategic IO training										→														
Key Developmental Assignments	Co, Bn, Bde IO Planner or Targeteer						Div IO Planner					Corps IO Planner				Bde CCWO		WOCC Commandant		ASCC CCWO											
	SA IO Planner at Bn / Bde						Div IO Targeteer					Corps IO Targeteer				IO CWOB		Regt CCWO		Army 011A		CAC CCWO									
Broadening Assignments							WOCC Instructor IOWO Instructor CTC OCT CTC Plans Officer Fellowship					Doctrine Writer IO Course Director HRC Career Manager DA G-3/5/7 Staff Officer				Army 011A Billets Joint 011A Billets															
							ASCC Staff Officer, TSOC Staff Officer, CAC IO Developer,					MAJCOM Staff Officer, COCOM Staff Officer, Student (SAMS / NDU / NPS)																			
Civilian Education and Certifications	Associate Degree		Bachelor's Degree				Master's Degree																								

Figure 3. 370A Career Development Model. Created by the author. (2025).

KD Assignments: Company grade warrant officers must serve at the company, battalion, or brigade-level for three to seven years, or until they are selected for promotion to CW3. KD positions for WO1s and CW2s include IO Plans Officer, Information Targeteer, and Sensitive Activities Planner. CW3s and CW4s should fill KD Planner or Targeteer billets at the Division and Corps levels (or equivalent). Additionally, CW4 KD should include a Senior Warrant Officer Advisor (SWOA) position, as part of a battalion command team. Finally, CW5 IOWOs should serve in nominative leadership positions within their field, such as Command Chief Warrant Officer (CCWO), and Chief Warrant Officer of the Branch (CWOB).

Broadening Assignments: The company grade IOWO should serve at echelons below division. Field grade IOWO broadening assignments include service as a Plans Officer or Targeteer at Army Service Component Commands, Army Major Commands, Theater Special Operations Commands, and Combatant Commands. Additional field grade IOWO opportunities include service at Combat Training Centers, Warrant Officer Career College, Combined Arms Center, Army Human Resources Command, and Headquarters Department of the Army. The IOWO should strive to serve in a variety of Army and Joint positions, to include special operations and conventional units.

Company Grade Training and Education: WO1s and CW2s should complete at least four of the following courses to expand their IO skillsets: OPSEC Officer Course, Military Deception (MILDEC) Planners Course, Army Space Cadre Basic Course, Irregular Warfare Course, Special Technical Operations Planner Course, Cyber Effects Application Course, Cyber Operations Planners Course, Joint Firepower

Course, and the PSYOP Officer Qualification Course. Select IOWOs may also complete courses like Airborne, Air Assault, and Static Line Jumpmaster.

Field Grade Education and Training: CW3s and CW4s should complete at least three of the following courses: the Joint Information Planner Course, Joint MILDEC Training Course, Special Operations MILDEC Planner Course, Joint Targeting Staff Course, Joint Electronic Warfare Theater Operations Course, Defense OPSEC Planner Course, and Joint Operational Fires & Effects Course. CW3s and CW4s may also apply to attend advanced programs like the National Defense University or the School of Advanced Military Studies. Additionally, CW4s should strive to complete the How the Army Runs Course.

Civilian Education: Advanced civilian education fosters a well-rounded IOWO, enabling them to achieve a broader understanding of socio-political landscapes. It enhances their ability to analyze information from multiple viewpoints, fostering critical thinking that is vital in developing innovative strategies in IO. Company grade IOWOs should attempt to complete an associate degree as a WO1, a bachelor's degree as a CW2, and a master's degree as a CW3 or CW4. This educational progression allows IOWOs to study key principles of information warfare and theory, preparing them to assess threats and leverage opportunities more effectively. Professional reading lists complement this pathway by exposing IOWOs to IO-related theories, case studies, and lessons learned, promoting continuous learning and adaptive thinking essential to successful IO. Ultimately, civilian education empowers IOWOs to anticipate shifts in the information environment, respond proactively, and contribute meaningfully to their units and missions.

Conclusion

The establishment of IOWOs within the U.S. Army is imperative in light of the evolving complexities of current and future IEs. Modern conflicts increasingly hinge on information supremacy, with adversaries effectively leveraging information to manipulate perceptions and influence behaviors throughout the competition-crisis-conflict spectrum. The proposed IOWOs would transcend traditional roles, providing specialized expertise to understand and exploit the intersection between information and military operations. Their training would equip them to anticipate adversarial narratives, coordinate information campaigns, and enhance decision-making processes, allowing commanders to maintain an operational advantage through informed decision-making and effective influence strategies.

The IOWO is not just a response to the complexities of modern warfare; it is a proactive strategy for leveraging IO as a decisive component of military power. By developing a dedicated pool of information professionals, the Army can ensure it has the expertise necessary to navigate complex IEs while enhancing interoperability and achieving information advantage in MDO and Joint All-Domain Operations. This initiative aligns seamlessly with the Army's CBA Process and the DOTMLPF-P framework, promising a cohesive approach to addressing the challenges of information and influence in modern warfare. The time has come for the Army to recognize and act on the critical need for specialized personnel focused on IO—expanding beyond FA30s—to secure its future operational success.

References

- Armistead, E. L. (2004). *Information Operations: Warfare and the hard reality of soft power*. Potomac Books.
- Brose, C. (2020). *The kill chain: Defending America in the future of high-tech warfare*. Grand Central Publishing.
- Department of the Air Force. (2023). *Information in Air Force operations*. (Air Force Doctrine Publication 3-13). Air Force Publishing Directorate.
- Department of the Army. (2021). *How the Army runs: A senior leader reference handbook 2021-2022*. Army Publishing Directorate.
- Department of the Army. (2023). *Information*. (Army Doctrine Publication 3-13). Army Publishing Directorate.
- Gaddis, J. L. (2002). *The landscape of history: How historians map the past*. Oxford University Press.
- Joint Chiefs of Staff. (2022). *Information in joint operations*. (Joint Publication 3-04). https://jdeis.js.mil/jdeis/new_pubs/jp3_04.pdf
- Leonhard, R. R. (2017). *Fighting by minutes: Time and the art of war* (2nd ed.). CreateSpace Independent Publishing Platform.
- Qiao, L., & Wang, X. (1999). *Unrestricted warfare*. Echo Point Books.

