



# **NAVAL POSTGRADUATE SCHOOL**

**MONTEREY, CALIFORNIA**

## **THESIS**

**INFORMATION OPERATIONS IN CURRENT AND  
FUTURE WARFARE**

by

Jonathan P. Wood and Bradley W. Young

December 2020

Thesis Advisor:

Ryan Maness

Co-Advisor:

Edward L. Fisher

**Approved for public release. Distribution is unlimited.**

THIS PAGE INTENTIONALLY LEFT BLANK

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                 |                                                                |                                                            |  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|----------------------------------------------------------------|------------------------------------------------------------|--|
| <b>REPORT DOCUMENTATION PAGE</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                 |                                                                | <i>Form Approved OMB<br/>No. 0704-0188</i>                 |  |
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                 |                                                                |                                                            |  |
| <b>1. AGENCY USE ONLY<br/>(Leave blank)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                 | <b>2. REPORT DATE</b><br>December 2020                         | <b>3. REPORT TYPE AND DATES COVERED</b><br>Master's thesis |  |
| <b>4. TITLE AND SUBTITLE</b><br>INFORMATION OPERATIONS IN CURRENT AND FUTURE WARFARE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                 |                                                                | <b>5. FUNDING NUMBERS</b>                                  |  |
| <b>6. AUTHOR(S)</b> Jonathan P. Wood and Bradley W. Young                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                 |                                                                |                                                            |  |
| <b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b><br>Naval Postgraduate School<br>Monterey, CA 93943-5000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                 |                                                                | <b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>            |  |
| <b>9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b><br>N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                 |                                                                | <b>10. SPONSORING / MONITORING AGENCY REPORT NUMBER</b>    |  |
| <b>11. SUPPLEMENTARY NOTES</b> The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                 |                                                                |                                                            |  |
| <b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b><br>Approved for public release. Distribution is unlimited.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                 |                                                                | <b>12b. DISTRIBUTION CODE</b><br>A                         |  |
| <b>13. ABSTRACT (maximum 200 words)</b><br><p>The U.S. Army recognizes the ongoing threat posed by our adversaries' strategic efforts to integrate information operations (IO), cyberspace operations, and emerging technologies that challenge U.S. freedom of maneuver across all domains. As a result, the U.S. Army is posturing for a doctrinal shift toward multi-domain operations, which will increase the role of information in warfighting. As it does, the U.S. Army faces challenges and disparities regarding IO in design and practice. Current U.S. Army IO doctrine, terminology, and overall structure is insufficient and does not facilitate a conceptual shared understanding. This leads to systemic underperformance of tactical units in the information environment and suboptimal integration of IO in strategy and plans. Similarly, the U.S. Army community of IO practitioners faces an identity crisis that degrades the profession's cohesion, influence, and overall ability to operate effectively. To overcome these challenges, a critical examination of U.S. Army IO in design and practice is first required to reveal the scope of the disparity. Then, the application of social network analysis and social identity theories reveals potential solutions in IO training, education, and organization that will enable the U.S. Army to become more competitive in the information environment. This investment will enhance the Army's ability to seamlessly integrate and execute information warfare in current and future conflicts.</p> |                                                                 |                                                                |                                                            |  |
| <b>14. SUBJECT TERMS</b><br>information operations, IO, multi-domain operations, MDO, cyber, cyberspace, information warfare, IW                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                 |                                                                | <b>15. NUMBER OF PAGES</b><br>89                           |  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                 |                                                                | <b>16. PRICE CODE</b>                                      |  |
| <b>17. SECURITY CLASSIFICATION OF REPORT</b><br>Unclassified                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <b>18. SECURITY CLASSIFICATION OF THIS PAGE</b><br>Unclassified | <b>19. SECURITY CLASSIFICATION OF ABSTRACT</b><br>Unclassified | <b>20. LIMITATION OF ABSTRACT</b><br>UU                    |  |

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release. Distribution is unlimited.**

**INFORMATION OPERATIONS IN CURRENT AND FUTURE WARFARE**

Jonathan P. Wood  
Major, United States Army  
BS, U.S. Military Academy, 2009

Bradley W. Young  
Major, United States Army  
BA, Pennsylvania State University, 2009

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION STRATEGY AND POLITICAL  
WARFARE**

from the

**NAVAL POSTGRADUATE SCHOOL  
December 2020**

Approved by: Ryan Maness  
Advisor

Edward L. Fisher  
Co-Advisor

Douglas A. Borer  
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

The U.S. Army recognizes the ongoing threat posed by our adversaries' strategic efforts to integrate information operations (IO), cyberspace operations, and emerging technologies that challenge U.S. freedom of maneuver across all domains. As a result, the U.S. Army is posturing for a doctrinal shift toward multi-domain operations, which will increase the role of information in warfighting. As it does, the U.S. Army faces challenges and disparities regarding IO in design and practice. Current U.S. Army IO doctrine, terminology, and overall structure is insufficient and does not facilitate a conceptual shared understanding. This leads to systemic underperformance of tactical units in the information environment and suboptimal integration of IO in strategy and plans. Similarly, the U.S. Army community of IO practitioners faces an identity crisis that degrades the profession's cohesion, influence, and overall ability to operate effectively. To overcome these challenges, a critical examination of U.S. Army IO in design and practice is first required to reveal the scope of the disparity. Then, the application of social network analysis and social identity theories reveals potential solutions in IO training, education, and organization that will enable the U.S. Army to become more competitive in the information environment. This investment will enhance the Army's ability to seamlessly integrate and execute information warfare in current and future conflicts.

THIS PAGE INTENTIONALLY LEFT BLANK



## TABLE OF CONTENTS

|             |                                                                       |           |
|-------------|-----------------------------------------------------------------------|-----------|
| <b>I.</b>   | <b>INTRODUCTION.....</b>                                              | <b>1</b>  |
| A.          | BACKGROUND INFORMATION .....                                          | 1         |
| B.          | RESEARCH QUESTION .....                                               | 2         |
| C.          | METHODOLOGY .....                                                     | 2         |
| <b>II.</b>  | <b>LITERATURE REVIEW .....</b>                                        | <b>7</b>  |
| A.          | ARMY IO IN CURRENT PRACTICE (WHERE WE ARE) .....                      | 7         |
| B.          | IO IN MDO (WHERE WE ARE GOING).....                                   | 9         |
| <b>III.</b> | <b>ARMY IO IN DESIGN: A CRITICAL EXAMINATION OF IO DOCTRINE .....</b> | <b>13</b> |
| A.          | INTRODUCTION: UNDERSTANDING IO .....                                  | 13        |
| B.          | IO DEFINED.....                                                       | 13        |
| C.          | INFORMATION RELATED CAPABILITIES (IRCS) AND IO .....                  | 15        |
| D.          | THE ROLE OF IO OFFICERS (FA30S).....                                  | 19        |
| E.          | TRAINING AND EDUCATION OF IO OFFICERS.....                            | 20        |
| F.          | IO PLANNING AND ASSESSMENT .....                                      | 24        |
| G.          | EMERGING CONCEPTS: IO, CYBERSPACE, AND MDO.....                       | 24        |
| <b>IV.</b>  | <b>IO IN PRACTICE.....</b>                                            | <b>29</b> |
| A.          | CHALLENGES OF EFFECTIVE AND COMPLETE INTEGRATION.....                 | 29        |
| B.          | TACTICAL IO TRAINING AT ARMY COMBAT TRAINING CENTERS.....             | 30        |
| C.          | IO EDUCATION IN PROFESSIONAL MILITARY EDUCATION (PME).....            | 34        |
| D.          | MILITARY DECEPTION AS AN IO CORE COMPETENCY .....                     | 36        |
| <b>V.</b>   | <b>SNA AND SOCIAL IDENTITY THEORY IN THE ARMY IO PROFESSION .....</b> | <b>41</b> |
| A.          | INTRODUCTION.....                                                     | 41        |
| B.          | THE FA30 COMMUNITY AND SOCIAL NETWORK ANALYSIS.....                   | 41        |
| 1.          | Brokers, Cutpoints, and Bridges .....                                 | 42        |
| 2.          | Social Capital.....                                                   | 43        |
| 3.          | Strength of Weak Ties .....                                           | 45        |
| C.          | SOCIAL IDENTITY IN THE FA30 COMMUNITY.....                            | 46        |
| 1.          | What is Social Identity and What are the Benefits? .....              | 47        |

|     |                                                                  |    |
|-----|------------------------------------------------------------------|----|
| 2.  | Social Identity in U.S. Army Information Operations .....        | 49 |
| 3.  | Social Identity and Organizational Symbolism.....                | 52 |
| 4.  | Organizational Symbolism in Army Information<br>Operations ..... | 54 |
| 5.  | Mercury and Hermes Symbolism in the Army IO<br>Profession.....   | 57 |
| D.  | IMPLICATIONS AND RECOMMENDATIONS.....                            | 58 |
| E.  | WAY AHEAD .....                                                  | 60 |
| VI. | CONCLUSION .....                                                 | 61 |
|     | LIST OF REFERENCES.....                                          | 65 |
|     | INITIAL DISTRIBUTION LIST .....                                  | 71 |

## LIST OF FIGURES

|           |                                                                   |    |
|-----------|-------------------------------------------------------------------|----|
| Figure 1. | IO trends at maneuver CTCs.....                                   | 32 |
| Figure 2. | USAIOP symbol. ....                                               | 54 |
| Figure 3. | 1st Information Operations Command shoulder sleeve insignia. .... | 55 |
| Figure 4. | Sword and lightning bolt imagery in Army IO unit symbolism .....  | 56 |
| Figure 5. | Army Cyber Corps branch insignia .....                            | 57 |
| Figure 6. | Selection of Army IO imagery depicting Mercury and Hermes.....    | 58 |
| Figure 7. | Proposed IO branch insignia. ....                                 | 59 |

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF ACRONYMS AND ABBREVIATIONS

|           |                                                                                       |
|-----------|---------------------------------------------------------------------------------------|
| AAR       | after action review                                                                   |
| ARCYBER   | Army Cyber Command                                                                    |
| C2W       | command and control warfare                                                           |
| C3CM      | command, control, communication countermeasure                                        |
| CAO       | civil affairs operations                                                              |
| CEMA      | cyber and electromagnetic activities                                                  |
| CGSC      | Command and General Staff College                                                     |
| CJCSI     | Chairman of the Joint Chiefs of Staff Instruction                                     |
| CMO       | civil military operations                                                             |
| CNO       | computer network operations                                                           |
| CO        | cyberspace operations                                                                 |
| COE       | center of excellence                                                                  |
| CTC       | combat training center                                                                |
| D3A       | decide, detect, deliver, assess                                                       |
| DA PAM    | Department of the Army pamphlet                                                       |
| DOD       | Department of Defense                                                                 |
| DOTMLPF-P | doctrine, organization, training, material, leadership, personnel, facilities, policy |
| EMS       | electromagnetic spectrum                                                              |
| EW        | electronic warfare                                                                    |
| FA30      | functional area 30                                                                    |
| FM        | field manual                                                                          |
| GEC       | Global Engagement Center                                                              |
| GLE       | graduate level education                                                              |
| HRC       | Human Resources Command                                                               |
| IA        | information assurance                                                                 |
| IEAA      | information environment advanced analytics                                            |
| IIA       | inform and influence activities                                                       |
| ILE       | intermediate level education                                                          |
| IO        | information operations                                                                |

|        |                                              |
|--------|----------------------------------------------|
| IOQC   | information operations qualification course  |
| IPA    | Information Professionals Association        |
| IRC    | information related capability               |
| IW     | information warfare                          |
| JEMSO  | joint electromagnetic spectrum operations    |
| JFSC   | Joint Forces Staff College                   |
| JIOPC  | Joint Information Operations Planners Course |
| JMRC   | Joint Multinational Readiness Center         |
| JOPP   | joint operations planning process            |
| JP     | joint publication                            |
| JRTC   | Joint Readiness Training Center              |
| KLE    | key leader engagement                        |
| LSCO   | large scale combat operations                |
| MDMP   | military decision-making process             |
| MDO    | multi-domain operations                      |
| MDTF   | multi-domain task force                      |
| MILDEC | military deception                           |
| MISO   | military information support operations      |
| MOS    | military occupation specialty                |
| NDU    | National Defense University                  |
| NPS    | Naval Postgraduate School                    |
| NTC    | National Training Center                     |
| OC/T   | observer controller/trainer                  |
| OIE    | operations in the information environment    |
| OPSEC  | operations security                          |
| P3     | presence, posture, and profile               |
| PA     | public affairs                               |
| PME    | professional military education              |
| PSYOP  | psychological operations                     |
| RTU    | rotational unity                             |
| SAMS   | School of Advanced Military Studies          |
| SC     | strategic communication                      |

|        |                                                     |
|--------|-----------------------------------------------------|
| SLE    | soldier-leader engagement                           |
| SNA    | social network analysis                             |
| SSC    | Senior Service College                              |
| STO    | special technical operations                        |
| TAC-D  | tactical deception                                  |
| TIC    | Theater Information Command                         |
| TIOH   | The U.S. Army Institute of Heraldry                 |
| TRADOC | Training and Doctrine Command                       |
| ULO    | unified land operations                             |
| USAIOP | United States Army Information Operations Proponent |
| USCC   | United States Cyber Command                         |

THIS PAGE INTENTIONALLY LEFT BLANK



## ACKNOWLEDGMENTS

Jon: My sincerest thanks and appreciation to my incredible wife and sons for their continued support throughout my career and this endeavor especially. I must also extend a special thanks to Brad, “Juicebox,” for his dedication and work throughout this project and both his and Kristin’s friendship over the years.

Brad: First and foremost, words cannot convey my gratitude to my amazing superhero wife, Kristin, for her unending love and support throughout this challenging year and beyond. Additionally, thanks to my thesis partner, Jon, and his family for their continued friendship and support. Kristin and I wish you guys the best and we’ll see you the next time our paths cross.

To our thesis advisors, Professors Ryan Maness and Edward Fisher, thank you for your invaluable guidance and wisdom and for helping us navigate the thesis process. To LTC Roland Miraco, who has been a guide and mentor from the very beginning of our IO careers, thank you for your continued leadership and support. Thanks to all the other faculty and staff in the Defense Analysis department and throughout NPS who granted us a first-class education. Additionally, thank you to the Graduate Writing Center and the Thesis Processing Office for your roles in helping us communicate our ideas and research.

We would like to thank our fellow students—Army, Navy, Marines, Air Force, civilian, and international—with whom we were lucky enough to share the past 18 months. We cannot express how much we have enjoyed learning from one another, and we wish you the best in the next phase of your journeys. Stay in touch!

Last but not least, we owe a sincere debt of gratitude to the global community of IO and cyber professionals. Throughout this project, we constantly sought insight and feedback from this vast network, and the support was always overwhelmingly above and beyond our expectations. In particular, we’d like to thank our fellow military and civilian IO community members, past and present, at the U.S. Army IO Proponent, 1st IO Command, Combat Training Centers, Command and General Staff College, and the Information Professionals Association. We chose this thesis topic because we wanted to

give something back to the profession, as well as contribute to the ongoing discourse surrounding the future of Army IO. With that goal in mind, we hope the reader finds some value in the following pages. Please don't hesitate to reach out to us and keep the conversation going.

*“All In!”*

*“The Power of Information!”*

# I. INTRODUCTION

## A. BACKGROUND INFORMATION

The United States Army recognizes the ongoing threat posed by our adversaries' ability to integrate information operations (IO), cyberspace operations, and emerging technologies into their strategic efforts to compete with the U.S. below the threshold of armed conflict as well as during competition and open warfare. *The 2018 Department of Defense (DOD) Cyber Strategy* warns that adversaries of the U.S., particularly China and Russia, are already integrating malicious cyber activity with cyber-enabled IO to undermine and threaten the U.S. and its interests, allies, and partners.<sup>1</sup> Undeniably, adversaries of the U.S. will continue to challenge U.S. freedom of maneuver and action in all domains in the near future, to include both cyberspace and the information environment, as acknowledged by the U.S. Army's doctrinal shift towards multi-domain operations (MDO). In the foreword of the Training and Doctrine Command pamphlet *The U.S. Army in Multi-Domain Operations (MDO), 2028*, General Milley illustrates his vision regarding how the U.S. Army must adapt to the new reality and develop multi-domain formations to "pose multiple and compounding dilemmas on the adversary."<sup>2</sup> This paradigm shift will require the Army to seamlessly integrate and execute cyberspace operations, deception, and information operations to achieve effects at all levels of war, from tactical to strategic.

However, these changes are not yet reflected in either U.S. Army IO doctrine nor the professional training and education of its Functional Area 30 (FA30 - IO Officer) force. Indeed, across the U.S. Army, there is a potential disparity between IO in design and how it is currently applied in ongoing operations, to say nothing about future operations. This manifests in IO often being marginalized, with IO officers and organizations performing functions outside of their specialty, often at the cost of integrating IO into operations.

---

<sup>1</sup> Department of Defense, *Summary: Department of Defense Cyber Strategy 2018* (Washington, DC: Department of Defense, 2018), 1, [https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER\\_STRATEGY\\_SUMMARY\\_FINAL.PDF](https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF).

<sup>2</sup> U.S. Army Training and Doctrine Command, *The U.S. Army in Multi-Domain Operations 2028*, Training and Doctrine Command Pamphlet 525-3-1 (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2018), iii.

Looking to the future, as Army Cyber Command (ARCYBER) seeks to become the Army's first Information Warfare Command, the Army must reconcile the disparity between IO in design versus in practice and prepare for executing information operations in future conflict and MDO. Even though the Army recognizes the critical role that information operations can have in operations, there are obstacles and challenges that preclude the Army from effectively integrating IO.

## **B. RESEARCH QUESTION**

How can the U.S. Army better train and educate FA30s and the Army to conduct successful information operations now and in future operations or conflict?

## **C. METHODOLOGY**

We examine this research question using a three-part approach. First, we establish a baseline of the U.S. Army's current organizational understanding of IO. Second, we compare that baseline with contemporary applications of IO in the Army to determine the extent of disparity there is, if any, between IO in design and in practice. Finally, using contemporary social network analysis and social identity theories, we describe the current identity and organizational issues with the U.S. Army community of IO practitioners that degrade the profession's cohesion, influence, and overall ability to operate effectively. These findings inform the recommendations that, if implemented, will enhance the Army's ability to integrate and execute information warfare in current and future conflicts.

First, to fully understand the extent to which a disparity exists between IO design and practice, we establish a baseline of how IO is currently perceived by senior leaders, staffs, and soldiers throughout the U.S. Army, how these populations are educated about IO in their formal professional military education (PME), and how U.S. Army units currently conduct IO. During this phase of the research project, we conduct a wide variety of simultaneous research methods to gather quantitative and qualitative data to establish this baseline. The following focus areas are intended to establish an understanding of IO perceptions in the U.S. Army:

1. How effectively does the U.S. Army plan and execute IO?

2. What are the biggest strengths of U.S. Army IO?
3. What are the biggest challenges, shortfalls, and gaps regarding the way that the U.S. Army conducts IO?
4. What formal IO-related educational practices exist in Army PME?
5. How effective are the Functional Area 30 (FA30) IO planners?
6. What IO related skills, traits, or competencies should IO officers have?
7. How can the U.S. Army better task organize to conduct IO in multi-domain warfare (MDO)?
8. How can IO best support the U.S. Army in multi-domain operations (MDO)?

Another method is to examine IO education at professional military education institutions. To accomplish this, we contacted Army intermediate and senior PME schools, including the CGSC to assess the current state of IO-related education available to mid/senior-level leadership. Additional sources of data include the various Army Centers of Excellence, SAMS, IO-related graduate-level education programs at the Naval Postgraduate School and the National Defense University, and the Army IO Qualification Course at the USAIOP.

In addition to those focus areas, the research team used publicly available data and/or private data from the following institutions:

1. Human Resources Command (HRC) non-PII data related to the Information Dominance branch, including duty titles, ranks, billet locations, prior MOS, and similar demographics.
2. Combat training center (CTC) after-action-reviews (AARs).
3. RAND Corporation studies.

After we establish a baseline understanding of the current state of Army IO in practice, we compare the data with current and projected IO doctrine in order to assess the disparity, if any, between Army IO in doctrine and design. Key source documents with

which to compare our findings include both Joint Publication (JP) 3–13 and Field Manual (FM) 3–13, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3210.01, Department of the Army (DA) Pamphlet 600-3, and Training and Doctrine Command (TRADOC) Pamphlet 525-3-8. We focus on examining the following questions to determine the level of disparity:

1. To what degree do U.S. Army command and staff leadership understand the role of IO in both current operations and future multi-domain operations (MDO)?
2. Does current IO education in U.S. Army PME institutions sufficiently prepare Army leaders and staffs to plan and execute IO in accordance with JP 3-13 and FM 3-13?
3. How and where are FA30s being employed across the force?
4. Does current FA30 training and education sufficiently prepare FA30s to conduct their functional competencies as outlined in DA PAM 600-3?
5. What are the challenges, shortfalls, and gaps associated with the U.S. Army's current organization to conduct IO?
6. What are the current challenges associated with adapting the U.S. Army's IO framework to better support MDO in an evolving, increasingly cyberspace-focused information environment?

By examining these questions, we identify the extent and severity of the disparity between IO in design, current practice, and future operations to inform potential solutions. We also identify obstacles and challenges to effective integration of information operations in the Army.

Achieving effective integration of IO will require full unity of effort amongst the U.S. Army's array of capabilities that create effects in the information environment. Presently, this is difficult to achieve because the multitude of these capabilities operate separately in their own stove-piped organizations, units, commands, and communities. Within this disjointed network of capabilities, Army IO Officers serve a vital role as

brokers and bridges to synchronize otherwise disparate capabilities towards a unifying goal. To understand the role that identity and social networks play in affecting Army IO, we apply social network analysis and social identity theory to the Army IO community. As part of this section, we identify how social networks, organizational symbols, narratives, and lineage can be leveraged to promote unity of effort within the Army and IO.

Finally, based on our research findings and assessment of IO shortfalls in design and practice, we develop and present recommendations on how to reconcile any disparity between IO in design and current practice, as well as how to better prepare FA30s and the force to conduct IO in future operations. Ultimately, to adequately prepare our FA30 force for success in current operations as well as multi-domain operations, we must reconcile the disparity between what IO is and what it needs to be.

The next chapter examines the literature around the research question, to include academic writing, doctrine, and government documents to establish a framework for the research. Chapter III seeks to describe how the Army designed the integration of IO into operations while Chapter IV outlines how IO is planned and executed in practice. Chapter IV also outlines a few challenges and obstacles for the information operations community and the Army. Chapter V describes the information operations network and personnel through social network analysis and social identity theory to depict both challenges and opportunities for the Army and IO. Through this research, we seek to identify any disparity between IO in design and practice as well as the challenges to its effective integration in the Army. With a global increase in the prevalence of information operations and associated activities in geo-politics and warfare, this research aims to depict how the Army can better integrate IO into Army operations to better poise for current and future conflict and competition.

THIS PAGE INTENTIONALLY LEFT BLANK



## II. LITERATURE REVIEW

The purpose of this literature review is to develop a common picture of Army Information Operations (IO) and is organized into two parts. First, we provide an overview of the current body of research and doctrine regarding Army IO in current design and practice. Second, we summarize the body of published work concerning the changing threat landscape in the information environment and the projected role of Army IO in future operations, specifically multi-domain operations (MDO). This literature review demonstrates that there is a noticeable absence of published work between those two subsets, indicating a potential organizational gap of knowledge regarding how to transform current Army IO into what IO needs to be.

### A. ARMY IO IN CURRENT PRACTICE (WHERE WE ARE)

In “Chapter III: Army IO in Design: A Critical Examination of IO Doctrine,” we conduct an in-depth, critical review of U.S. Army IO doctrine and its implications with regards to the successful implementation of IO. Therefore, in this literature review, we only briefly outline the scope and purpose of IO as described in doctrine to inform further discussion. As outlined in Field Manual 3-13, *Information Operations*, the U.S. Army currently uses the joint definition of IO as “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.”<sup>3</sup> This definition designates IO as a military activity to be conducted exclusively during military operations, which is a self-imposed restriction that adversaries of the United States do not similarly observe. The definition also makes clear that U.S. military IO should focus on impacting the decision making of adversaries and potential adversaries. Missing from this definition is the broad spectrum of friendly and neutral activities in the information environment that the U.S. Army typically

---

<sup>3</sup> Department of the Army, *Information Operations*, FM 3-13 (Washington, DC: Department of the Army, 2016), 1-2, [https://armypubs.army.mil/epubs/DR\\_pubs/DR\\_a/pdf/web/FM%203-13%20FINAL%20WEB.pdf](https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/FM%203-13%20FINAL%20WEB.pdf).

categorizes as IO. In Chapter III, we discuss this discrepancy as well as other inconsistencies and issues concerning the doctrinal design and structure of U.S. Army IO.

Perhaps due to the vague, widely misunderstood doctrinal definition of IO, it is no surprise that IO is a divisive topic within the U.S. Army. The body of literature involving differing interpretations of the purpose, scope, and utility of IO is broad and encompasses nearly every imaginable position on the subject. However, authors tend to agree nearly universally that the military's current doctrinal IO concept is either misguided, insufficient, misinterpreted, or some combination of all three. For example, in his 2017 paper for *The Strategy Bridge* titled "Speed, Volume, and Ubiquity: Forget Information Operations & Focus on the Information Environment," former Army IO Officer Michael Williams offers that the U.S. military doctrine has wrongfully emphasized specific IO capabilities which overshadows the concept itself. Instead, the author offers that "we should encourage those not familiar with information operations to see it as a vital component of planning in an information environment that is much more important to military planning and operations with each passing day,"<sup>4</sup> while arguing that the current capability-focused paradigm does more to confuse and distract from the intended purpose of IO.

Similarly, multiple authors and researchers recognize the growing importance of the information environment in current and future conflict and have thus identified that the U.S. Army's current IO design is no longer sufficient. For example, even before the U.S. Army Cyber Command (ARCYBER) announced its intentions to transform into a more holistic information warfare command, author Conrad Crane explained the ubiquity of an information warfare command in his *War on the Rocks* article "The United States needs an Information Warfare Command: A Historical Examination."<sup>5</sup> Conrad, who was chief of historical services for the U.S. Army Heritage and Education Center of the U.S. Army War

---

<sup>4</sup> Michael Williams, "Speed, Volume, and Ubiquity: Forget Information Operations & Focus on the Information Environment," *The Strategy Bridge*, July 26 2017. <https://thestategybridge.org/the-bridge/2017/7/26/speed-volume-and-ubiquity-forget-information-operations-focus-on-the-information-environment>.

<sup>5</sup> Conrad Crane, "The United States Needs an Information Warfare Command: A Historical Examination," *War on the Rocks*, June 14, 2019, <https://warontherocks.com/2019/06/the-united-states-needs-an-information-warfare-command-a-historical-examination/>.

College, argues that the establishment of such a command would “encourage decision-makers to think of information warfare in the holistic sense that has long eluded the service and the nation.”<sup>6</sup> The author contends that the action would finally move the U.S. towards a united understanding of IO that we certainly lack and our adversaries seem to have already attained.

Indeed, IO is perhaps one of the most contested military topics amongst scholars and practitioners in modern military doctrine, partly due to the rapidly changing nature of the information environment. The current design and structure of Army IO facilitates a wide variety of interpretations while emerging technology and the onset of widespread cyberspace operations create diverging potential paths for the future of Army IO. Meanwhile, adversaries of the United States, particularly China, Russia, North Korea, and Iran, have seized upon the opportunities provided by an evolving cyberspace-enabled information environment, and are already exploiting it while the U.S. struggles with terminology and definitions. How the U.S. Army transforms to meet this new challenge will be crucial to its overall success in multi-domain operations. In the following section, we examine the current body of literature which predicts how this transformation could unfold.

## **B. IO IN MDO (WHERE WE ARE GOING)**

In the foreword of the Training and Doctrine Command pamphlet on *The U.S. Army in Multi-Domain Operations (MDO)*, 2028, General Milley illustrates that adversaries of the United States, particularly China and Russia, are integrating technology to increase the stand-off across all the domains, to include cyber.<sup>7</sup> Adversaries and potential adversaries of the United States will challenge our freedom of maneuver and action in all domains in the near future, to include both cyberspace and the information environment. For example, during its military operations in Ukraine starting in 2014, Russia successfully tested its ability to integrate information operations, electronic warfare, and cyberspace operations with maneuver and special operations to achieve their objectives in dynamic hybrid

---

<sup>6</sup> Crane, “The United States Needs an Information Warfare Command.”

<sup>7</sup> U.S. Army Training and Doctrine Command, *The U.S. Army in Multi-Domain Operations 2028*, iii.

warfare.<sup>8</sup> Similarly, China appears increasingly willing to employ cyberspace as a way to both subvert U.S. technical supremacy and counter U.S. influence on a global scale.<sup>9</sup> Clearly, the body of evidence suggests that adversaries of the U.S. are bringing information warfare to scale.

In response, the U.S. Army in MDO will strive to develop multi-domain formations to “pose multiple and compounding dilemmas on the adversary.”<sup>10</sup> The information environment, consisting of the physical, information, and cognitive dimensions will become increasingly more congested as forces become more reliant on technology and digital communications.<sup>11</sup> In a degraded, denied, or congested information environment or electromagnetic spectrum, complete freedom of maneuver in cyberspace will not be guaranteed. During competition or armed conflict, the Army in MDO must effectively manage its cyber, space, and information related forces to protect its relatively unimpeded use of the dimensions of the information environment while simultaneously creating advantage and opportunity for the commander.

TRADOC Pamphlet 525-3-1 discusses another evolution of contemporary information operations to information environment operations (IEO). In IEO, commanders and their staff will synchronize information related capabilities to seek advantage over adversaries and consolidate gains in the information environment.<sup>12</sup> While conducting multi-domain operations, the Army will rapidly execute operations and integrate capabilities in all domains, including the EMS and the information environment to

---

<sup>8</sup> Aaron F. Brantly, Nerea M. Cal, and Devlin P. Winkelstein, *Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW*, Report Number AD1046052 (West Point, NY: Army Cyber Institute, 2017), 3, <https://apps.dtic.mil/dtic/tr/fulltext/u2/1046052.pdf>.

<sup>9</sup> Brandon Valeriano, Benjamin Jensen, and Ryan Maness, *Cyber Strategy: The Evolving Character of Power and Coercion*, (New York: Oxford University Press, 2018), loc. 3353, Kindle.

<sup>10</sup> U.S. Army Training and Doctrine Command, *The U.S. Army in Multi-Domain Operations 2028*, iii.

<sup>11</sup> U.S. Army Training and Doctrine Command, *U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045*, TRADOC PAM 525-3-8. (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2018), 7.

<sup>12</sup> U.S. Army Training and Doctrine Command, *The U.S. Army in Multi-Domain Operations 2028*, C-9.

maximize effects on the enemy. These synergistic operations will seek to create overmatch with the enemy with mutually reinforcing effects.<sup>13</sup>

A 2018 Congressional Research Service Report on information warfare outlines a bifurcation of information strategy and cyberspace operations at the national level, explaining that the Department of Defense support structures for information operations and cyberspace operations are treated separately, both organizationally and doctrinally.<sup>14</sup> In the report, the author posits whether the Defense Department and U.S. structures are configured in a manner that maximizes the potential of both information warfare and cyberspace operations. Moreover, this report cites that U.S. Cyber Command (USCC) focuses more on offensive cyber operations than the “cognitive and strategic effects of information.” As the Army plans a doctrinal shift to multi-domain operations, the Army must maximize the interoperability and growing relationship between cyberspace operations and information operations to properly and effectively create multiple and compounding effects on the enemy.

Clearly, current DOD policy and doctrine guidance on the employment of IO does not yet reflect the rapidly occurring shift towards MDO and information warfare. To adequately prepare our IO professionals for success in the information environment, we must reconcile this disparity between what IO is and what it needs to be. In the following chapter, “Army IO in Design: A Critical Examination of IO Doctrine,” we further examine the shortfalls, challenges, and other issues regarding the U.S. Army’s IO structure, and the implications towards its ability to execute IO in current and future conflict.

---

<sup>13</sup> U.S. Army Training and Doctrine Command, *The U.S. Army in Multi-Domain Operations 2028*, vii.

<sup>14</sup> Theohary, Catherine. *Information Warfare: Issues for Congress*, R45142 (Washington, D.C., Congressional Research Service, 2018), 16.

THIS PAGE INTENTIONALLY LEFT BLANK

### **III. ARMY IO IN DESIGN: A CRITICAL EXAMINATION OF IO DOCTRINE**

#### **A. INTRODUCTION: UNDERSTANDING IO**

Without a doubt, IO is a challenging concept to comprehend. Understanding IO requires a technical familiarization with a variety of existing and emerging capabilities, an understanding of the dynamics of information transmission in a given operating environment, and the ability to comprehend the cognitive nuances of both friendly and adversary decision-making. By design, IO requires a blending of technical and abstract concepts that are made even more challenging to understand due to the evolving nature of the information environment and rapid advancements in technology. As a result, the U.S. Army lacks a shared understanding of IO across the entire force, impacting its ability to leverage information in combat. In this chapter, our purpose is to outline key components of IO in design through a critical examination and commentary of applicable doctrine, training, and education. The intent is to provide an analysis of where the U.S. Army's doctrinal approach to IO both succeeds and fails to bring about a shared understanding of IO as well as create a coherent strategy to accomplish information operations. This analysis provides a baseline understanding of the U.S. Army's IO concept and introduces the issues described later in this research project. Because the scope of this research project is limited to the U.S. Army, we will focus on Joint and U.S. Army doctrine, although it is beneficial for U.S. Army IO practitioners to familiarize themselves with the concepts employed by the U.S. Navy, Marine Corps, and Air Force.

#### **B. IO DEFINED**

The most central place to begin a discussion about Army IO is the doctrinal definition. The primary Department of Defense (DOD) IO policy document, DOD Directive (DoDD) 3600.01, *Information Operations*, describes IO as “the principal mechanism used during military operations to integrate, synchronize, employ, and assess a wide variety of information-related capabilities (IRCs) in concert with other lines of operations to effect adversaries’ or potential adversaries’ decision-making while protecting

our own.”<sup>15</sup> Joint doctrine similarly describes IO as “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.”<sup>16</sup> In a prudent effort to align U.S. Army and Joint IO doctrine, the U.S. Army currently uses the Joint definition of IO as its formal definition.<sup>17</sup>

Although IO is an amorphous concept, from these definitions one can easily extrapolate two defined goals of IO: Attack the enemy’s decision making and protect friendly decision making. If this were solely the case, it would be neither challenging to explain Army IO, nor would it be difficult to convince leaders, staffs, and soldiers of its utility in combat operations. However, this simplified definition inadequately captures the true scope of the application of IO in the U.S. Army. Notably, immediately following the Joint definition listed above, U.S. Army IO doctrine adds a less-cited expansion to its definition of IO: “This manual uses the term IO comprehensively to capture all activity employed to affect the information environment and contribute to operations in and through the information environment.”<sup>18</sup> With this small addition to the description, the U.S. Army now effectively expands IO to encompass any activity that impacts, transits, and leverages the information environment.

The U.S. Army’s expanded definition more accurately reflects its application of IO than the original definition. It also more accurately underscores the prevalence of IO across all military operations and the monumental impact of the information environment on military outcomes. Furthermore, the U.S. Army’s extremely broad paradigm on IO is rightfully designed so that commanders and IO planners are not constrained, at least by

---

<sup>15</sup> Department of Defense, *Information Operations*, DoDD 3600.01, (Washington, DC: Department of Defense, 2013), [https://fas.org/irp/doddir/dod/d3600\\_01.pdf](https://fas.org/irp/doddir/dod/d3600_01.pdf).

<sup>16</sup> Joint Chiefs of Staff, *Information Operations*, JP 3-13, (Washington, DC: Joint Chiefs of Staff, 2014), ix, [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_13.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf).

<sup>17</sup> Department of the Army, *Information Operations*, FM 3-13 (Washington, DC: Department of the Army, 2016), [https://armypubs.army.mil/epubs/DR\\_pubs/DR\\_a/pdf/web/FM%203-13%20FINAL%20WEB.pdf](https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/FM%203-13%20FINAL%20WEB.pdf).

<sup>18</sup> Department of the Army, *Information Operations*, 1-2.



doctrine. However, the vague expanded definition does little to alleviate confusion as to the mandate, scope, and boundaries of IO, which contributes to an overall lack of shared understanding in the U.S. Army.

### **C. INFORMATION RELATED CAPABILITIES (IRCS) AND IO**

The answer to “who conducts IO” is equally as vague and potentially confusing as defining IO. As stated previously, IO itself is simply an umbrella term for a category of operations which impact, transit, or leverage the information environment, according to the U.S. Army. More specifically, it is important to understand that IO is not a capability itself but rather an integrating and coordinating function in which the goal is to synchronize information effects with each other and with maneuver operations. Military units conduct IO through both kinetic activities and a variety of information related capabilities (IRCs).<sup>19</sup> Therefore, to answer the above question, IRCs are the “doers” that physically execute information operations, each one affecting a different aspect of the information environment or using different ways or means to leverage the information environment and support accomplishment of military objectives.

However, much like defining IO itself, the boundaries surrounding the categorization of IRCs are broad and vague. Perhaps the most concise description resides in the 2003 version of Field Manual (FM) 3–13, *Information Operations*, which outlines five “core capabilities” of IO: electronic warfare (EW), computer network operations (CNO - encompassing computer network attack, defense, and exploitation), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC).<sup>20</sup> Though outdated, this list of core IRCs provides a simple, clearly defined explanation of the U.S. Army’s larger IO construct. Of course, as the scope of U.S. Army IO increased, these core capabilities alone could not sufficiently account for the breadth of activities that impact and transit the information environment. This is why the previous version of FM 3-13 also included “supporting elements:” physical destruction, information assurance

---

<sup>19</sup> Department of the Army, 1-3.

<sup>20</sup> Department of the Army, 1-13.

(IA), physical security, counterintelligence, counter-deception, and counter-propaganda.<sup>21</sup> Of note, according to this version of FM 3-13, it is important to distinguish that the employment of any one of these activities does not comprise IO itself, but rather “independent activities that, when taken together and synchronized, constitute IO.”<sup>22</sup> In other words, an IRC by itself is not IO and does not become IO until synthesized with other capabilities towards a unified information-related end state, according to U.S. Army doctrine.

Unfortunately, this explanation does little to clarify exactly when and where an information operation starts and ends. For example, how many IRCs must be employed before an operation becomes an information operation? Why should the employment of a single IRC, such as a PSYOP broadcast or EW jamming, not be considered an information operation even though it is clearly impacting the information environment? When is “physical destruction” considered an IRC, as opposed to just physical destruction? The open-ended nature of the description of these IRCs invites ambiguity and general confusion. The legal ramifications of this confusion could be significant. Depending on the mission or geographic region, there are normally specific legal authorities associated with IO. Unclear boundaries regarding when the unit is engaging in IO or not can create legal complications that can hinder mission accomplishment. Even so, these boundaries remain largely under-defined and poorly understood.

The current version of FM 3-13 provides some answers to these questions while raising new issues. FM 3-13 defines an IRC as “a tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions.”<sup>23</sup> Although this definition is still extraordinarily broad, the current manual clarifies that IRCs are generally those activities whose effects are primarily based in the information environment, to include cyberspace. In the manual, these are referred to as twelve “daily practice” IRCs, which are MILDEC, military

---

<sup>21</sup> Department of the Army, 1-14.

<sup>22</sup> Department of the Army, 2-1.

<sup>23</sup> Department of the Army, 1-3.

information support operations (MISO—formerly PSYOP), soldier and leader engagement (SLE), civil affairs operations (CAO), combat camera (embedded units that capture and produce battlefield still and video imagery), OPSEC, public affairs, cyberspace electromagnetic activities (CEMA), EW, cyberspace operations, space operations, and special technical operations (STO).<sup>24</sup> These IRCs constitute what would generally be considered the “core” capabilities of IO in today’s Army.

Additionally, current IO doctrine elaborates that supporting activities in the physical dimension can indeed impact the information environment, and thus outlines additional enabling activities: commander’s communication strategy, presence, posture, and profile (P3), foreign disclosure, physical security, physical maneuver, special access programs, civil-military operations (CMO), intelligence, and destruction or lethal actions.<sup>25</sup> Clearly, the addition of these enabling activities broadens the scope of IO capabilities to nearly all military activity. The document acknowledges this, offering the following analogy:

The formal definition of IRCs encourages commanders and staffs to employ all available resources when seeking to affect the information environment to operational advantage. For example, if artillery fires are employed to destroy communications infrastructure that enables enemy decision making, then artillery is an IRC in this instance.<sup>26</sup>

To be clear, most commanders and staffs would likely not consider artillery an IRC under almost any circumstance. However, the point is well taken. In fact, the increasingly broad scope of what can be considered an IRC is very beneficial for IO practitioners, who otherwise might find themselves too constrained to develop plans that sufficiently impact the information environment based on available capabilities. Conversely, the aforementioned uncertainty regarding the boundaries of IO remains, which creates implications for the U.S. Army’s ongoing efforts to develop a coherent IO strategy.

---

<sup>24</sup> Department of the Army, 1-3.

<sup>25</sup> Department of the Army, 1-3.

<sup>26</sup> Department of the Army, 1-3.

Because the U.S. Army approach to IO is largely modeled after Joint doctrine, it is not surprising that the definition and scope of IRCs in JP 3-13 is similarly broad. Joint doctrine outlines fourteen military capabilities that either directly create effects in the information environment or otherwise factor significantly into IO planning and integration: strategic communication (SC), joint interagency coordination, public affairs, CMO, cyberspace operations, information assurance, space operations, MISO, intelligence, MILDEC, OPSEC, joint electromagnetic spectrum operations (JEMSO), and key leader engagement (KLE).<sup>27</sup> Similarly, JP 3-13 acknowledges that there are “many” other capabilities that contribute to IO and therefore the list is not all-inclusive.<sup>28</sup> Like the other doctrinal references we examine in this section, this caveat indicates that military units can leverage nearly any military capability or activity as an IRC.

This examination of IRCs in doctrine reveals several notable insights. First, the scope of what the U.S. Army considers an IRC has expanded significantly from the original five core IRCs to the fourteen core IRCs in today’s Joint publication. Additionally, modern Joint and Army IO doctrine universally includes caveats that military units can leverage nearly any type of capability or activity towards operations in the information environment. Therefore, much like the U.S. Army expanded definition of IO that encompasses nearly any operations that create effects within the information environment, so too are IRCs defined as nearly any capability that impacts the information environment. This broad paradigm has both positive and negative implications. On the one hand, military commanders are not doctrinally constrained with what capabilities they can leverage to plan and execute IO. This is both convenient for military planners and accurately representative of the reality of the modern information environment. On the other hand, just as the expanded definition of IO falls short of providing a clear shared understanding of the concept, the nearly limitless scope of IRCs creates ambiguity at an institutional level regarding who participates in IO. This negatively impacts the U.S. Army’s ability to

---

<sup>27</sup> Joint Chiefs of Staff, *Information Operations*, II-5 through II-13.

<sup>28</sup> Joint Chiefs of Staff, II-5.

develop an identity amongst its IO professionals, which we will examine in detail in Chapter V – SNA and Social Identity Theory in the Army IO Profession.

#### **D. THE ROLE OF IO OFFICERS (FA30S)**

Considering the involvement of dozens of individual IRCs in IO, it is not surprising that the U.S. Army prudently created an occupational specialty whose primary duty is to synchronize, coordinate, and integrate information effects into unit operations. This position is the IO Officer, sometimes referred to as an FA30, which is short for its career field designation of Functional Area 30. FM 3-13 explains the IO Officer as the “staff focal point for IO,” responsible for analyzing the information environment, identifying IRCs for each operation, synchronizing those IRCs with each other and the overall operation, and assessing the effectiveness of IO throughout, among many other specified and implied tasks.<sup>29</sup> The Department of the Army Pamphlet (DA PAM) 600–3 section on IO similarly describes that the “IO officer is the staff expert for military information environment effects, military deception, operations security, information protection, social media interaction, and information-focused military and civil engagement,” and that “IO planning and coordination also supports cyberspace operations and electronic warfare, presence, posture and profile, physical destruction and deliberate influencing of foreign target audiences in support of operations conducted in a designated area of operations.”<sup>30</sup> The DA Pamphlet also outlines eight “Unique Knowledge and Skills of an Information Operations Officer” as well as nine “Functional Competencies.” Duties and responsibilities of the IO Officer include leading the IO working group and serving as the leader of the IO cell on larger staffs. On smaller staffs, such as brigade-sized elements that are still authorized the position, the IO Officer may be the sole advocate for operations in the information environment on the entire staff.

To continue the discussion on the design and application of IO, it is important to distinguish the role of the Army IO Officer from that of individual IRCs. IO Officers serve

---

<sup>29</sup> Department of the Army, *Information Operations*, 3-4.

<sup>30</sup> Department of the Army, *Information Operations Functional Area*, DA PAM 600-3 Smartbook (Washington, DC: Department of the Army, 2017), <https://www.milsuite.mil/book/groups/smartbook-da-pam-600-3>, 1-2.

on staff elements to plan, integrate, and assess IO while IRCs execute information related effects in support of operations, IO or otherwise. In one of the great ironies of U.S. Army IO design, IO Officers do not actually execute IO themselves. On occasion, an IO Officer might bear responsibility for a certain technical IRC if that capability is owned at the staff level, but this is rare and typically by exception. Instead, IO Officers perform their duty as coordinators, synchronizers, and assessors with neither the authority nor the mandate to dictate the actions of IRCs on the battlefield. Additionally, IO Officers do not “own” any IRCs, which generally subscribe to their own chain of command. The relationship is well summarized in JP 3-13, where “IO is not about ownership of individual capabilities but rather the use of those capabilities as force multipliers to create a desired effect.”<sup>31</sup> This is an important distinction because otherwise there is a potential for conflict between IO Officers and IRCs if the relationship is misunderstood or not well-defined from the beginning. The personal experiences of the authors indicate that this misconception is prevalent in the U.S. Army and should be considered an important issue regarding IO in design.

#### **E. TRAINING AND EDUCATION OF IO OFFICERS**

Army IO Officers do not commission directly into the career field, as is the case with most U.S. Army basic branches. Instead, the U.S. Army IO career field is known as a functional area, which is “a grouping of officers by technical specialty or skills other than an arm, service, or branch that usually requires unique education, training, and experience.”<sup>32</sup> This means that Army IO Officers serve in an Army basic branch for the beginning of their career before applying to transfer to become an IO Officer. Although the requirements fluctuate by application cycle, generally an officer is eligible to transfer upon completion of their branch key developmental assignments at the rank of O-3 or O-4. As a result, the earliest that an officer may request a transfer into the IO career field is around the seven-year mark, while most transfers occur either as a senior captain or a junior major.

---

<sup>31</sup> Joint Chiefs of Staff, *Information Operations*, II-5.

<sup>32</sup> Department of the Army, *Officer Professional Development and Career Management*, DA PAM 600-3, (Washington, DC: Department of the Army, April 3, 2019), 11.

Nearly any officer from any basic branch may request a transfer to become an IO officer, provided that their originating branch authorizes them to pursue the transfer application. A top-secret/sensitive compartmented information access is also required to be considered for the position, and the U.S. Army encourages applicants who can operate with unified action partners, are “culturally astute” and understand the “challenges and complexities of the operational environment.”<sup>33</sup>

Notably, there is no requirement to have served in an IRC career field to apply for a transfer into the FA30 career field. Furthermore, no requirement exists for applicants to have any other training, education, or academic background in any information-related vocation or field of study, although the application board would likely view those backgrounds favorably. As a result, the IO profession consists of an expansive and diverse set of backgrounds from nearly every basic branch in the Army, but very few individuals have prior hands-on experience with IRCs before becoming an IO Officer.

Once selected to become an IO Officer, students attend the U.S. Army IO Qualification Course (IOQC) at the earliest opportunity to become certified to perform their new duties. The IOQC consists of 12 weeks of instruction designed to certify individuals to become IO and MILDEC officers.<sup>34</sup> The course focuses on the familiarization and integration of IRCs, application of IO into the Military Decision Making Process (MDMP), IO targeting and assessment, and a capstone event designed to “develop the students’ ability to plan, prepare, execute, and assess the integration of IRCs and to adapt tactics, techniques, and procedures throughout Unified Land Operations within a decisive action training environment.”<sup>35</sup> Recently, the U.S. Army IO Proponent (USAIOP), which oversees the IOQC, conducted an extensive curriculum review which resulted in an enhanced emphasis on large scale combat operations (LSCO) as well as an extensive 10-day MILDEC block of instruction.<sup>36</sup>

---

<sup>33</sup> Department of the Army, *IO Functional Area*, 1.

<sup>34</sup> “IO Qualification Course (IOQC),” United States Army Combined Arms Center, accessed October 10th 2020, <https://usacac.army.mil/organizations/mccoe/iop/ioqc>.

<sup>35</sup> United States Army Combined Arms Center, “IO Qualification Course (IOQC).”

<sup>36</sup> United States Army Combined Arms Center, “IO Qualification Course (IOQC).”

The 12-week IOQC is the only formal IO education course required to perform duties as an IO Officer. However, like most vocations, the U.S. Army expects IO professionals to seek out continuing education in the form of advanced IO training and specialized courses regarding individual IRCs. Many IO Officers attend courses offered by the 1st IO Command Training and Analysis Branch, which conducts both resident and mobile IO-related training and education courses. 1st IO Command offers these courses to both IO Officers and non-IO Officers alike, including integration courses on key IRCs such as EW, MISO, and Cyberspace Operations, planners' courses on military deception and tactical IO, and even an IO fundamentals course.<sup>37</sup> The Training and Analysis Branch also produces adversary information warfare seminars, focusing on Russia, China, North Korea, and Violent Extremist Organizations (VEOs).<sup>38</sup> Through these courses, 1st IO Command provides opportunities for Army IO Officers to build on their education from the IOQC and develop their planning skills in specific areas of expertise.

Besides the IO training available at 1st IO Command, many FA30s attend a multitude of other advanced training and education opportunities offered by various organizations throughout the Army, Joint Force, and Interagency. The Joint Forces Staff College (JFSC) at the National Defense University (NDU) offers the Joint IO Planners' Course (JIOPC), the purpose of which is to educate IO Officers and others "to plan, integrate, and synchronize IO into joint operational-level plans and orders."<sup>39</sup> JFSC also offers the Joint MILDEC Training Course, which provides crucial training on how to plan and integrate MILDEC.<sup>40</sup> Another example of advanced IO training is the Information Environment Advanced Analysis (IEAA) course, sponsored by JMark Services, Inc., which trains students to "characterize, forecast, target, wargame and assess the information

---

<sup>37</sup> "1st IO Cmd Training and Analysis Branch," 1st IO Command, accessed October 10th 2020, <https://www.1stiocmd.army.mil/Home/iotraining?csrt=9958488605993639674>.

<sup>38</sup> 1st IO Command, "1st IO Cmd Training and Analysis Branch."

<sup>39</sup> "Joint Information Operations Planners' Course," Joint Forces Staff College, accessed October 5, 2020, <https://jfsc.ndu.edu/Academics/Joint-C2-Information-Operations-School-JC2IOS/Information-Operations-Division/JIOPC/>.

<sup>40</sup> "Joint MILDEC Training Course (JMTC)," Joint Forces Staff College, accessed October 5, 2020, <https://jfsc.ndu.edu/Academics/Joint-C2-Information-Operations-School-JC2IOS/Information-Operations-Division/JMTC.aspx>.



environment in support of a commander's decision-making process.”<sup>41</sup> These are just several examples of additional IO training. Numerous other training and education opportunities exist on almost any IRC or aspect of the information environment, including STO, space, OPSEC, and interagency support.

Finally, IO Officers may seek graduate-level IO education opportunities, as outlined in the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3210.01C, *Joint IO Proponent*. The Joint IO Proponent reviews and approved IO-related graduate-level education (GLE) programs for the joint force. The aforementioned programs at NDU as well as the graduate programs at the Naval Postgraduate School (NPS) are currently the only GLE programs approved by the Joint IO Proponent.<sup>42</sup> Many U.S. Army IO Officers attend the curriculum 698 program at NPS, Information Strategy and Political Warfare, which educates students on “the psychological and social dimensions of war emphasizing information strategy, political warfare, military deception, defense support to public diplomacy analytical methods, and regional studies.”<sup>43</sup> Together, these IO GLE programs are “designed to provide OSD, the Joint Staff, and the CCMDs with a cadre of academically educated professionals who are prepared to provide IO related policy expertise at the strategic and strategic-operational levels.”<sup>44</sup>

Several potential challenges exist in the U.S. Army's current model of training, educating, and employing IO Officers. Although a multitude of additional training and education opportunities exist for IO Officers, an IO Officer might not have the opportunity to attend due to mission requirements, deployments, scheduling conflicts, temporary duty (TDY) funding constraints, or any other potential issues. As a result, in those cases, their only formal IO education is the 12-week IOQC. An alternative model might involve a

---

<sup>41</sup> “Information Environment Advanced Analysis Course,” JMark Services, Inc, accessed October 5, 2020, <https://www.jmarkservices.com/information-environment-advanced-analysis-course/>.

<sup>42</sup> Joint Chiefs of Staff, *Joint Information Operations Proponent*, CJCSI 3210.01, (Washington, DC: 2014). D-4.

<sup>43</sup> “Information Strategy and Political Warfare - Curriculum 698,” Naval Postgraduate School, accessed October 5, 2020, <https://nps.smartcatalogiq.com/en/Current/Academic-Catalog/Graduate-School-of-Operational-and-Information-Sciences-GSOIS/Department-of-Defense-Analysis/Information-Strategy-and-Political-Warfare-Curriculum-698>.

<sup>44</sup> Joint Chiefs of Staff, *Joint Information Operations Proponent*, D-4.

shifting of resources to incorporate some of these additional and advanced training opportunities into the IOQC itself, thereby eliminating the possibility that an IO Officer might not be able to receive the opportunity later. This investment in education could produce significant dividends towards the overall competency and confidence of the U.S. Army's IO profession. Additionally, the IO Officer position's status as a functional area is potentially inadequate given the ever-increasing importance of the information environment on military operations. We further explore this recommendation and the concept of social identity in the Army IO profession in Chapter V.

#### **F. IO PLANNING AND ASSESSMENT**

By design, Army IO Officers are responsible for planning, integrating, and assessing IO. In U.S. Army IO doctrine, the process for planning IO largely mirrors the military decision-making process (MDMP), with IO-related tasks alongside each step of the planning process.<sup>45</sup> Similarly, Joint doctrine superimposes the IO planning process onto the Joint Operations Planning Process (JOPP).<sup>46</sup> Army IO targeting integration likewise reflects existing targeting methodology, including Decide, Detect, Deliver, Assess (D3A).<sup>47</sup> Unquestionably, it is prudent for U.S. Army IO doctrine to reflect maneuver operations whenever possible. Aside from the obvious advantage of optimally synchronizing and coordinating effects, any common language between IO and maneuver operations helps the U.S. Army as an institution move closer towards a common, shared understanding of IO.

#### **G. EMERGING CONCEPTS: IO, CYBERSPACE, AND MDO**

U.S. Army doctrine is transitioning to concepts that demand an increased emphasis on the information environment, particularly cyberspace. Currently, U.S. Army doctrine is developed to support unified land operations (ULO). In ULO, Army practitioners seek to employ IO and cyberspace operations to garner and create conditions that will support

---

<sup>45</sup> Department of the Army, *Information Operations*, 4-1 through 4-28.

<sup>46</sup> Joint Chiefs of Staff, *Information Operations*, IV-1 through IV-10.

<sup>47</sup> Department of the Army, *Information Operations*, 7-1 through 7-7.

achieving success for the force. As Army Field Manual 3-12 describes, cyberspace operations, properly coordinated with similar and complementary capabilities, will “provide a decisive advantage to commanders at all levels in modern combat.”<sup>48</sup> However, the Army is currently planning for a transition from ULO to multi-domain operations (MDO), in which a significant portion of all operations in the information environment are expected to utilize, transit, or otherwise leverage cyberspace in some form. As a result, U.S. Army and practitioners of both CO and IO must understand and shape the role that each will play to continue to provide support to the Army and the joint force.

In the foreword of the Training and Doctrine Command pamphlet on *The U.S. Army in multi-domain operations (MDO), 2028*, General Milley illustrates that adversaries of the United States, particularly China and Russia, are integrating technology to increase the stand-off across all the domains, to include cyber.<sup>49</sup> Adversaries of the United States will challenge our freedom of maneuver and action in all domains in the near future, to include both cyberspace and the information environment. The U.S. Army in MDO will strive to develop multi-domain formations to “pose multiple and compounding dilemmas on the adversary.”<sup>50</sup> This will require the Army to integrate and execute cyberspace operations and information warfare to achieve effects at all levels of war, from tactical to strategic. To do so, the relationship between cyberspace operations and information warfare will be more integrated than it is currently. Cyberspace operations will extend the influence and range of information warfare, and information warfare will provide complementary effects for cyberspace operations. Both functions must retain flexibility and adaptability to respond to agile adversaries in contested environments.<sup>51</sup>

The U.S. Army in MDO must understand the information environment to include cyberspace, space, and the electromagnetic spectrum (EMS).<sup>52</sup> Army Field Manual 3-12

---

<sup>48</sup> Department of the Army, *Cyberspace and Electronic Warfare Operations*, FM 3-12 (Washington, DC: Department of The Army: 2017), 1-1.

<sup>49</sup> U.S. Army Training and Doctrine Command, *The U.S. Army in Multi-Domain Operations 2028*, iii.

<sup>50</sup> U.S. Army Training and Doctrine Command, iii.

<sup>51</sup> U.S. Army Training and Doctrine Command, C-9.

<sup>52</sup> U.S. Army Training and Doctrine Command, C-9.

describes cyberspace as a global domain that resides within the information environment.<sup>53</sup> This supports the inherent relationship between the two functions and their codependence. The adversary enjoys relative freedom of maneuver in these dimensions and therefore the friendly force must understand their activities to fully appreciate the operational environment. To gain an advantage in either competition or conflict, leaders and practitioners in the Army must fully understand, analyze, and integrate operations in cyberspace, space, and the EMS. These areas are inherently related, and none can fully realize maximum potential when operations are isolated each individually. As Valeriano et al. indicate, operations in cyberspace are more effective when they are conducted in coordination with other efforts.<sup>54</sup>

The information environment, consisting of the physical, information, and cognitive dimensions will become increasingly more congested as friendly, neutral, and enemy forces become more reliant on technology and digital communications.<sup>55</sup> In a degraded, denied, or congested information environment or electromagnetic spectrum, complete freedom of maneuver in cyberspace will not be guaranteed. The Army Field Manual on CEMA describes superiority in cyberspace as the ability for the force to freely conduct operations in cyberspace.<sup>56</sup> During competition or armed conflict, the Army in MDO must effectively manage its cyber, space, and information related forces to protect its relatively unimpeded use of the dimensions of the information environment. To ensure this freedom of maneuver for Army cyber forces, IO practitioners must ensure that sufficient deconfliction and coordination of operations are conducted to avoid degrading the effects of the disparate information related capabilities.

Furthermore, a key aspect of Army IO is to enable and protect friendly decision making.<sup>57</sup> With a growing relationship and integration of cyberspace operations into Army operations, IO will increasingly develop techniques and processes for protecting the

---

<sup>53</sup> Department of the Army, *Cyberspace and Electronic Warfare Operations*, 1-2.

<sup>54</sup> Valeriano et al., *Cyber Strategy: The Evolving Character of Power and Coercion*. 112.

<sup>55</sup> Department of Defense, *Multi-Domain Combined Arms Operations at Echelons Above Brigade*, 7.

<sup>56</sup> Department of the Army, *Cyberspace and Electronic Warfare Operations*, 1-1.

<sup>57</sup> Department of the Army, *Information Operations*, 1-1.

cyberspace element of friendly decision-making. Protecting our forces' ability to use the EMS and the information environment, including digital communications and networks will be paramount to the Army and joint force in both competition and throughout the range of military operations.

As the United States Army continues to understand, develop, and integrate the relationship between cyberspace operations, information operations, and information warfare, practitioners must understand the role of each in Army and Joint operations. TRADOC Pamphlet 525-3-1 suggests that in MDO, information operations must transition to operations in the information environment (OIE). There are nuanced, but clear differences between the two definitions. OIE includes operations "to influence enemy formations and populations to reduce their will to fight; and influence friendly and neutral populations to enable friendly operations."<sup>58</sup> OIE as a function highlights the core responsibility to "influence, deceive, disrupt, corrupt, or usurp the decision-making of enemies and adversaries."<sup>59</sup> Although already considered a function of information operations, OIE seeks to formalize the function of deception in its definition. An important aspect of both definitions is that both OIE and IO are conducted "in concert with other lines of operations"<sup>60</sup> to achieve outcomes favorable to friendly forces. These other lines of operation will continue to take advantage of the capabilities of the Army's cyber forces, as well as joint, inter-agency, national, and multi-national assets.

The emergence of OIE onto an already crowded field of inter-related terms and definitions is a continuation of the identity crisis that has plagued Army IO for years; a point we examine further in Chapter V. In the following chapter, we examine these issues in IO design that have impacted the U.S. Army's ability to plan and execute IO and the implications for future conflict.

---

<sup>58</sup> U.S. Army Training and Doctrine Command, *The U.S. Army in Multi-Domain Operations 2028*, C-9.

<sup>59</sup> Department of Defense, *Information Operations*, X.

<sup>60</sup> U.S. Army Training and Doctrine Command, *The U.S. Army in Multi-Domain Operations 2028*, C-9.

THIS PAGE INTENTIONALLY LEFT BLANK

## IV. IO IN PRACTICE

### A. CHALLENGES OF EFFECTIVE AND COMPLETE INTEGRATION

In a time when great power competition, hybrid warfare, and gray zone conflict are commonplace topics of discussion in political and military circles of the United States, the U.S. Army must examine its current training and education systems in order to poise for future operations. In most recent circumstances, the United States was able to employ a significant technical and military overmatch in conflicts it has been a part of. This overmatch allowed for a tactical and operational advantage in almost every situation where the U.S. military employed its conventional capabilities to achieve its objectives. As contemporary adversaries and potential adversaries continue to close the technological and military capabilities gap between themselves and the United States, the U.S. Army should revisit some of its marginalized capabilities in order to maintain this advantage and remain competitive. During situations where the United States Army cannot apply its full force, or political considerations limit the application of kinetic weapons, military deception and information operations can be an effective complementary effort towards achieving Army objectives. These capabilities must be fully and deliberately integrated within Army operations and rehearsed and practiced thoroughly to be an effective combat multiplier.

At the institutional level, the U.S. Army is beginning to elevate information operations to the level necessary to compete with its adversaries. Army Cyber Command (ARCYBER) is enhancing its capabilities and scope with the goal of transforming into a multi-domain-capable information warfare command by 2028.<sup>61</sup> Simultaneously, revolutionary Army-wide organizational concepts such as the Multi-Domain Task Force (MDTF), Theater Information Command (TIC), and Information Warfare Brigades will bring rapid, adaptive information effects to expeditionary units on future battlefields.<sup>62</sup>

---

<sup>61</sup> Shannon Vavra, “Here’s how Army Cyber Command plans to take on information warfare,” *Cyberscoop*, July 29, 2020, <https://www.cyberscoop.com/army-cyber-command-plan-transition-information-war/>.

<sup>62</sup> Stephen Fogarty, and Bryan Sparling, “Enabling the Army in an Era of Information Warfare,” *The Cyber Defense Review*, Volume 5, No. 2 (Summer 2020). Pages 17-25.

Why then, if the U.S. Army is finally beginning to emphasize IO and invest more resources at the institutional level, does it still face significant challenges implementing IO at the tactical level? Unfortunately, the U.S. Army remains locked in an archaic cultural mindset that disproportionately favors combat power, lethal effects, and technical overmatch in the physical dimension while marginalizing or even ignoring the information environment. Instead, the U.S. Army should adjust its organizational culture to align with the reality of combat in the information age, where combatants who are proficient in the art of IO can neutralize or counterbalance the overwhelming military force of their opponent. This chapter summarizes the various challenges that the U.S. Army faces implementing IO at the tactical maneuver unit level based on recurring trends from the Army's maneuver combat training centers, and then describes how emphasizing IO in junior to intermediate-level professional military education (PME) can facilitate cultural change and reverse those trends. It also addresses the education and training of Army information operations officers in a core competency of the IO field, military deception, and recommends a revitalized focus on this capability.

## **B. TACTICAL IO TRAINING AT ARMY COMBAT TRAINING CENTERS**

Information operations in the U.S. Army is a complementary function to maneuver warfare that integrates and synchronizes information-related capabilities in order to create unique effects and conditions for the friendly force by coordinating operations in the information environment.<sup>63</sup> As Matthew Fecteau discusses in his Global Security Review article, there are differences between how many interpret and understand the role of information operations, but the general characteristics of IO remain largely the same.<sup>64</sup> These operations and activities are executed in the information environment, but their effects and purposes are likely, and generally intended to, affect and introduce conditions across the domains of warfare. Information operations, by leveraging the expertise and capabilities of the experts across the information warfare community and integrating them

---

<sup>63</sup> Department of the Army, *Information Operations*, 1-2.

<sup>64</sup> Matthew Fecteau, *Understanding Information Operations and Information Warfare: The Muddled Meaning of IO (and IW)*, Global Security Review, last modified June 7, 2019, <https://globalsecurityreview.com/understanding-information-operations-information-warfare/>.



into operations, can introduce conditions and effects that will allow for the U.S. Army to continue to operate with a tactical and operational advantage. For Army IO to perform this function, it must be conducted in concert with other lines of operation. As McArdle points out in her War on the Rocks article, information operations and specifically military deception, must be seamlessly integrated with operations.<sup>65</sup> Reinforcing this, Walter Jajko recommends that “the planning, and practice of deception ought to be systematically integrated into military strategy.”<sup>66</sup>

Understanding that Army information operations are executed in support of achieving friendly force objectives as a complementary effort, how does the Army get closer to fully realizing and understanding the role, function, and importance of IO in its operations? Much like it employs and validates its other tasks and missions, the Army’s Combat Training Centers (CTC) may provide the appropriate venue. A great resource for understanding the strengths and weaknesses of information operations capabilities in tactical maneuver units are these three maneuver CTCs: The Joint Readiness Training Center (JRTC), the Joint Multinational Readiness Center (JMRC), and the National Training Center (NTC).<sup>67</sup> These sprawling, state-of-the-art training centers simulate realistic combat environments in which tactical maneuver units undergo complex training scenarios. In many cases, these exercises serve as the final validation mechanism for tactical maneuver units before assuming a real-world mission. More so, when consolidated over time, CTC data can provide valuable insight into broader recurring trends throughout the U.S. Army. By examining these trends concerning the tactical application of IO, one gains an understanding of the unfortunate scope of the problem.

In practice, the Army understands the importance of rehearsals and exercises in verifying and validating its units’ critical tasks and prioritizes these exercises accordingly.

---

<sup>65</sup> Jennifer McArdle, “Pioneers of Deception: Lessons from the Ghost Army,” *War on the Rocks*, last modified May 2018, <https://warontherocks.com/2018/05/pioneers-of-deception-lessons-from-the-ghost-army/#:~:text=In%20short%2C%20the%20soldiers%20of,artillery%2C%20jeeps%2C%20and%20airplane s.>

<sup>66</sup> Walter Jajko, “Deception: Appeal for Acceptance; Discourse on Doctrine; Preface to Planning,” *Comparative Strategy*, Volume 21 (2001): 351-363.

<sup>67</sup> “Combined Training Center Directorate,” United States Army Combined Arms Center, accessed August 17, 2020, <https://usacac.army.mil/organizations/cact/ctcd>.

The U.S. Army brigade is the unit bridges the tactical and operational levels. Commanded by an O-6, brigades are deployed to execute their assigned missions. Pre-deployment, brigades conduct a validating exercise at one of the Army's CTCs. These CTCs provide the terrain, opposition force (OPFOR), and observer controller-trainers (OC-Ts) for the rotational unit (RTU) to conduct its validating exercise pre-deployment. It is during these CTC exercises that the RTU, the deploying brigade, receives its most accurate and realistic assessment of its ability to conduct the warfighting functions and execute its critical and mission essential tasks. For this section, we examine IO-related trends from each maneuver CTC based on exercise after-action reviews to gain an understanding of widespread issues regarding IO application at the tactical level. Figure 1 outlines the most frequently occurring IO-related trends.<sup>68</sup>

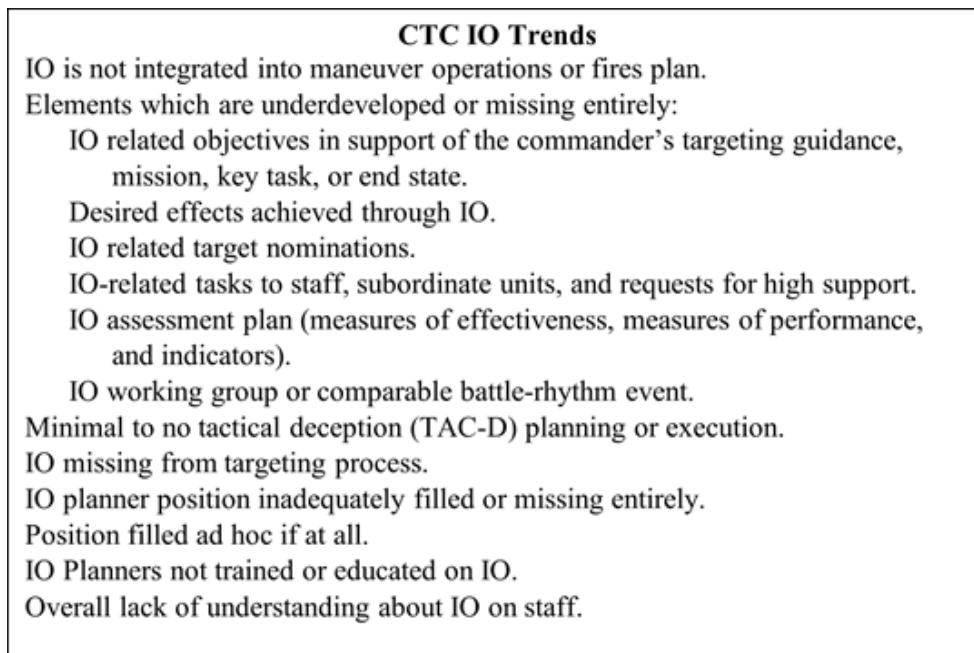


Figure 1. IO trends at maneuver CTCs<sup>69</sup>

<sup>68</sup> Felix Figueroa, personal communication, May 26, 2020.

<sup>69</sup> Source: Felix Figueroa, personal communication, May 26, 2020.

Most notably, IO is systemically desynchronized, underdeveloped, or missing entirely from overall unit operations. This directly conflicts with IO planning guidance described in both Joint and Army IO doctrine, which uniformly emphasizes the importance of integrating IO planning with maneuver operations early and throughout the mission.<sup>70</sup> Additionally, units rarely include an IO working group into their regular planning cycle, and IO target nominations are either underdeveloped or unused. Furthermore, tactical units rarely consider IO when developing their overall mission statements, key tasks, desired end-state, or guidance to subordinate units. These omissions undoubtedly signal a lack of importance to subordinate units at the ground level. Unsurprisingly, these subordinate units are therefore more likely to perform their simulated missions without concern for inevitable ramifications in the information environment.

The Army's decision within the last decade to eliminate the full-time Brigade IO Officer position,<sup>71</sup> which had previously been the sole advocate for IO in the entire tactical maneuver unit, further compounds the problem. Today, units executing CTC rotations either leave the position vacant or fill it on an ad hoc basis, sometimes designating an unqualified individual as the IO planner immediately before or even during the training exercise. Simply restoring the Brigade IO Officer position would be a welcome step in the right direction, but it is an incomplete solution regarding fixing the overall culture problem. A single staff officer is most likely not empowered enough to reverse a deeply rooted cultural issue like the one the U.S. Army currently faces regarding IO. A more suitable solution to achieve lasting change should include both a top-down approach through leadership emphasis and a bottom-up approach through education. As mentioned earlier, the U.S. Army's improving attitude towards IO at the highest institutional level must continue to gain momentum and then permeate down to the level of tactical implementation.

With no organic information operations officer on the brigade staff and information operations being a mere footnote in Army professional education, the brigade is going to

---

<sup>70</sup> Joint Chiefs of Staff, *Information Operations*, IV-1.

<sup>71</sup> David J. Zallo, "Ready, Willing, and Able: Picking a Brigade Combat Team Information Operations Officer," *Center for Army Lessons Learned Newsletter*, No. 17-18 (June 2017): 51-56.

enter CTC rotations at a relative disadvantage for incorporating information operations. These disadvantages can be overcome through a deliberate effort by the commander and staff to understand the information environment of the training center. It is also incumbent on the brigade's higher headquarters, the division, to adequately prepare the brigade to conduct operations in the information environment. With a more aptly suited IO staff section at the division level, this section must take appropriate measures to prepare their subordinate brigades for CTC rotations through training and education.

### **C. IO EDUCATION IN PROFESSIONAL MILITARY EDUCATION (PME)**

Undoubtedly, the concerning trends regarding the tactical performance of IO at CTCs are partly a result of the inadequate level of IO-related education that mid-level officers receive during their PME. For example, at the Command and General Staff College (CGSC), students attending intermediate level education (ILE) receive only two hours' worth of dedicated IO instruction out of the entire year-long curriculum.<sup>72</sup> Furthermore, military deception is only offered as an elective, and many students graduate without understanding, let alone becoming proficient in this art. Since the officers attending ILE at CGSC are likely to become the next tactical operations officers, executive officers, and commanders at the brigade level, one could reasonably hypothesize a correlation between the lack of intermediate-level IO education and the performance of IO by tactical maneuver units during CTC rotations.

Therefore, it follows that perhaps the single most important step towards improving the U.S. Army's culture and performance in the information environment is to prioritize IO and deception in military education programs, especially ILE. This can help the U.S. Army achieve a cultural mindset of what RAND Corporation social scientist Christopher Paul calls "communication mindedness," a mentality where effects in and through the information environment are always at the forefront of operations and in the decision-making of commanders and staff.<sup>73</sup> Dr. Paul further advocates that "PME for even junior

---

<sup>72</sup> U.S. Army Command and General Staff College, "Advance Sheet for Lesson M333: Information Operations," M333 AS, Leavenworth, KS: U.S. Army Command and General Staff College, October 2019.

<sup>73</sup> Christopher Paul, "On Strategic Communication Today: Enhancing U.S. Efforts to Inform, Influence, and Persuade." *Parameters*, 46, no. 3 (2016), 87-97.

officers should include introductory material on the possible contributions of informing, influencing, and persuading.”<sup>74</sup> An ideal revision of junior to mid-level officer PME programs would elevate IO to the level of “core competency” akin to other aspects of leadership and tactics emphasized throughout the curriculum. This model would retain the existing block of instruction dedicated to IO while adding the consideration of effects and impacts on the information environment as a critical learning objective to all other relevant blocks of instruction. Additionally, all practical exercises in any PME course should challenge students to integrate information-related effects and shape the information environment to the maximum extent possible. This curriculum reform strategy would naturally mesh IO into the existing course structure without inundating students and instructors with additional classes. Such an overhaul would still prove to be a significant endeavor. Therefore, it should be included in any planned upcoming curriculum revisions pertaining to the transition to multi-domain operations (MDO). This presents a prime opportunity to align any potential upcoming curriculum review with MDO 2028 emphasizing operations in the information environment.

An investment in IO education for junior to mid-level leaders in the U.S. Army would pay multiple dividends at the tactical level. Those leaders would be in a much better position to empower their IO planners and utilize IO resources and capabilities in tactical maneuver operations. This improvement would ensure that resources are not wasted at the level of implementation as the U.S. Army continues to build its IO force, field new information-related capabilities, and organize into new expeditionary formations in support of tactical units. Eventually, the U.S. Army could finally achieve the cultural change required to elevate IO to a level commensurate with the current reality in which the military’s actions in and through the information environment can mean the difference between success and failure.

---

<sup>74</sup> Paul, “On Strategic Communication Today,” 93.

#### **D. MILITARY DECEPTION AS AN IO CORE COMPETENCY**

The strategy of the United States will require more than a reliance on its sheer military prowess and capabilities to remain competitive and win in future conflict, operations, and competition. Great power competition and an increase in states employing political warfare and subversive acts to undermine the United States reintroduces a form of war that it has not recently focused on. The United States military must tune its forces to more adeptly analyze and create effects in the information environment in an effort to operate more effectively in the years to come. Although today's information environment is more congested and complicated than during historic wars, the principles of information operations, information warfare, and deception remain largely the same. New technologies present both a liability and an opportunity for military IO and deception practitioners. As Jennifer McArdle recommends in her War on the Rocks article, great power competition requires that the United States reexamine the lessons learned from the deception practitioners of its past and apply those lessons towards contemporary problem sets.<sup>75</sup> Military deception is a core competency of military information operations practitioners and will be a critically enhancing capability in future campaigns and operations.

Current doctrine of the United States prescribes that military deception is designed to cause an adversary decision maker to take an action or inaction that will support the friendly force accomplishing its mission. This is an enabling capability that can misrepresent the "capabilities, activities, limitations, and intentions" of military operations.<sup>76</sup> When executed successfully, military deception can help the force achieve an advantage during operations at a designated point in time. As Walter Jajko describes, military deception is also an effective tool for causing an adversary's operational advantage to be irrelevant.<sup>77</sup> In situations where the adversary possesses a distinct advantage, military deception can create conditions that cause this advantage to be immaterial during operations.

---

<sup>75</sup> McArdle. "Pioneers of Deception: Lessons from the Ghost Army."

<sup>76</sup> Joint Chiefs of Staff, *Military Deception*, JP 3-13.4, (Washington, DC: Joint Chiefs of Staff, 2017), ix.

<sup>77</sup> Jajko, "Deception: Appeal for Acceptance; Discourse on Doctrine; Preface to Planning," 351-363.

In times where the United States cannot apply the full force of its military, or political considerations limit the application of kinetic weapons, military deception can be an effective complementary effort towards achieving U.S. objectives. Although, as McArdle points out, military deception must be seamlessly integrated with operations.<sup>78</sup> For this capability to be effective, it must create unique conditions favorable for friendly forces and not necessarily be the operation itself. Great power competition and gray zone conflict will present situations where the United States is unable to bring the full force of its military to bear. It will require finesse and an understanding of the decision-making process of the adversary in order to create conditions and effects that support achieving the friendly force objectives.

The deception operation must not threaten or pose undue risk to the campaign or operation. Jajko recommends that “the planning, and practice of deception ought to be systematically integrated into military strategy.”<sup>79</sup> For this to be feasible, it is imperative that military leaders, planners, and units are conceptually aware of deception and both trained and educated to understand how to integrate deception into operations. Without this prerequisite, like many other enabling functions, deception operations are likely to be bolted onto operations in a *check the box* manner. To demonstrate the current lack of integration of deception into operations, Jajko points out that as a contrast to the thinking of both China and Russia where deception operations “create an end in themselves,” many in the United States military view deception as a “means to an end”.<sup>80</sup>

For deception to become mainstream in United States’ military planning, it is critical that our leaders and planners are suitably trained and educated in its capabilities and benefits. They must also be introduced to the fundamentals and basics of deception, much like infantry officers are aware of the core concepts of logistics and armor officers understand the idea of combat aviation. Advocates of military deception, information operations, and information warfare should lobby for an increased presence of deception

---

<sup>78</sup> McArdle, “Pioneers of Deception: Lessons from the Ghost Army.”

<sup>79</sup> Jajko, “Deception: Appeal for Acceptance; Discourse on Doctrine; Preface to Planning,” 353.

<sup>80</sup> Jajko, 351-363.

in our professional military education courses and institutions. If only a few individuals are ever presented with deception operations conceptually, then deception will never become a commonplace activity. This is not to say that all members of the Army must become deception planners, or that deception is required in all situations. However, our leaders and planners must be well versed enough to identify situations that the force may benefit from integrating deception into their plans.

Military leaders must also be cautious of the additional duty solution. Just because a planner attends a two-week familiarization course on logistics, does not mean they are qualified to become the logistics planner for a geographic combatant command. Much like logistics, deception planners require training, education, and experience to become proficient at their craft. To this end, current deception practitioners and information operations officers must make the effort to hone their proficiency and expertise. They should not sit idly by as campaigns and operations are planned waiting for the opportunity to present itself to become a part of the effort. They must take the proactive steps to ensure that deception is seamlessly integrated into operational planning from the onset.

Information operations and military deception are interconnected functions, both integrating means to affect the decision-making process of the enemy and to create unique advantages for the friendly force. U.S. military information operations planners are uniquely trained and educated in understanding the information environment as well as analyzing and affecting the decision-making process of the adversary. Each IO planner must seek opportunities to become better trained in military deception and strive for its integration into operations. Without effective and capable deception or IO planners, these functions will receive suboptimal to marginal attention during the planning process and in execution.

A principle tenant of U.S. military information operations is to protect the decision-making process of the force.<sup>81</sup> Whether or not the United States invests in the capability, capacity, and expertise to integrate deception operations, its adversaries are doing so. Michael Kofman presents his views on Russian hybrid warfare and deception in his War

---

<sup>81</sup> Joint Chiefs of Staff, *Information Operations*, ix.



on the Rocks article. Here, he discusses Russian integration of political warfare, deception, and propaganda in pursuit of its political objectives.<sup>82</sup> Russia, and other adversaries of the United States, will not pull punches in their efforts to disrupt the decision-making process of U.S. military leaders. In their 1995 article, *Tactical Deception in Air-Land Warfare*, Fowler and Nesbit warn that “the military group that is not devoting appropriate efforts to include tactics, R&D and plotting and scheming in general for deception is almost certain to be vulnerable to being deceived itself.”<sup>83</sup> For the United States military to be prepared to identify, understand, and counter the deception efforts of its adversaries, it must invest in its deception and information operations practitioners. Those planners that understand deception are more likely to identify when they are being deceived. With an understanding of the information environment, deception, and the adversary, today’s information operations and deception planners are poised to identify and counter deceptive efforts of U.S. adversaries. The institutions responsible for these individuals must invest in the counter-deception capability of its planners as well as that of the military on the whole.

Deception in warfare and in pursuit of a nation state’s political objectives will continue. The United States military must be prepared to integrate deception into plans and operations to remain competitive in great power rivalry and in non-permissive environments as well as to prepare for future wars. To do this, the U.S. military must invest in its deception and information operations practitioners and systems. Its planners must be suitably trained and educated to both plan these operations as well as identify and counter the deception efforts of its adversaries. Also, the military must raise its collective knowledge of deception and be prepared to identify opportunities for its integration.

In situations where the United States Army cannot apply its full force, information operations and military deception are an effective warfighting function that can support in achieving its objectives. When the United States Army faces an adversary that is at a near parity technologically and militarily, information operations and military deception may

---

<sup>82</sup> Michael Kofman, “Russian Hybrid Warfare and Other Dark Arts,” *War on the Rocks*, last modified March 11, 2016, <https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/>.

<sup>83</sup> Charles Fowler and Robert Nesbit, “Tactical Deception in Air-Land Warfare,” *Journal of Electronic Defense*, (June 1995): 37-79.

provide just enough advantage to achieve and maintain the competitive edge that it is accustomed to. Before that can occur, the Army must educate its force, train, practice, and become adept at integrating information operations in a controlled training environment. These efforts will enable a smoother transition from the training centers to integrating IO and maneuver operations in real-world conflict. Additionally, these activities will build a stronger identity and unity of purpose among the network of information operations personnel in the Department of Defense. Continued education, training, and integration of information operations and military deception will help to build a stronger identity within the community and a more consolidated front within the Army and the military.

## **V. SNA AND SOCIAL IDENTITY THEORY IN THE ARMY IO PROFESSION**

### **A. INTRODUCTION**

The United States Army recognizes the increasing importance of the information environment in modern conflict. As the U.S. Army postures for multi-domain operations (MDO), it is exploring how to best converge cross-domain capabilities, including information related capabilities (IRCs), to maximize effects against our adversaries.<sup>84</sup> To achieve convergence of IRCs, the U.S. Army needs to invest in its community of FA30s. The FA30's purpose is to synchronize and coordinate IRCs in pursuit of the commander's objectives in the information environment,<sup>85</sup> a role which will certainly become more crucial as the U.S. Army adopts MDO. In this chapter, we will examine how the U.S. Army can apply contemporary theories of social network analysis, social identity, and trust to improve the FA30 community's cohesion and organizational influence at a relatively low cost, thereby enabling the community to meet the increasingly challenging task of waging information warfare in future conflict. This chapter is divided into two sections: The first section uses social network analysis (SNA) concepts to describe the essential role that FA30s perform as brokers within the information warfare community. The second section recommends that building a strong social identity, potentially by elevating the FA30 to the status of a basic branch, can improve trust, influence, and unity of effort within the profession.

### **B. THE FA30 COMMUNITY AND SOCIAL NETWORK ANALYSIS**

This section of the analysis assesses the FA30 career field and its placement and role in the network of the information warfare community and the U.S. Army. The unique position of the FA30s in their organizations, as well as the relationships they garner, make them brokers between disparate parts of the network, allowing for enhanced cooperation and wider diffusion of information. The bridges that FA30s form allow agencies to cooperate in pursuit of common objectives more efficiently and with mutually supported operations. As

---

<sup>84</sup> U.S. Army Training and Doctrine Command, *The U.S. Army in Multi-Domain Operations 2028*, x.

<sup>85</sup> Department of the Army, *Information Operations*, 1-2.

integrators and synchronizers of IRCs, one of the greatest assets of the FA30 is their social capital and their ability to serve as an interlocutor between otherwise disconnected organizations. Finally, the network of communication between FA30s is unique and stronger because of the strength of weak ties. These characteristics of FA30s demonstrate their importance in the network and their ability to integrate information operations within the U.S. Army as well as broader U.S. government informational efforts.

### **1. Brokers, Cutpoints, and Bridges**

As the synchronizers and coordinators of information related capabilities, the purpose of the FA30 is to serve as brokers within the Army's network to facilitate and coordinate operations in the information environment between the information warfare community and their unit. Most organizations are billeted between one and a handful of Information Operations Officers, with anything more being an exception. It is these individuals' responsibility to coordinate internally and externally to the organization to develop and execute operations. Because of their unique external contacts, FA30s are cutpoints in the Army's network. Most FA30s are uniquely trained in the integration of IRCs including military deception, operations security, electronic warfare, special technical operations, and cyberspace operations. Through their training, various assignments, and cultivated relationships, FA30s eventually develop contacts within various other organizations. Some of these organizations are very niche in capability while others are broader in their mission sets. The variety of relationships that the FA30 develops is unique to the FA30 community. Few other career fields develop the types of relationships with similar signatures that FA30s do during their career. These unique relationships enable what Robert Putnam would describe as a benefit-rich network because it has "contacts established in the places where useful bits of information are likely to air."<sup>86</sup>

When assigned to an organization, FA30s bring their understanding of the IRC community, experience, and relationships. Because of these unique and nonredundant relationships, FA30s are a cutpoint in the network between their unit and the information

---

<sup>86</sup> Ronald Burt, "The Social Structure of Competition," in *Networks and Organizations: Structure, Form and Action*, ed. Nitin Nohria and Robert G Eccles. (Boston: Harvard University Press, 1992), 63.

warfare community. As cutpoints and brokers in this network, their removal would disconnect the network as they serve as a connection between the unit they are assigned and other organizations. In pursuit of operations of the unit to which they are assigned, FA30s must often coordinate for support from external agencies. It is then that FA30s leverage their expertise in understanding what unique organizations in the U.S. government are best suited to support the unit. In most cases, the FA30 is the only member of the organic unit that has these relationships. As such, these ties to external agencies are non-redundant and form structural links with the adjoining networks.<sup>87</sup> Without the FA30 in the network, both the unit to which they would be assigned and potentially affected external agencies would struggle to make the appropriate connections in the network to develop effective and well-coordinated operations in the information environment.

## **2. Social Capital**

In part because of the unique position of the FA30 in the network, they must rely heavily on their social capital. Oftentimes, units have very few organic IRCs at their disposal, and IO officers must exercise their social capital to be effective. In *The Social Structure of Competition*, Ronald Burt discusses three kinds of capital present in competitive arenas: financial, human, and social.<sup>88</sup> The FA30's relationships with other actors in the network are their social capital. Through their previously encountered associates, friends, and former colleagues, the FA30 has the opportunity to use their capital to develop concepts for operations in the IE. With stronger social capital, the FA30 has more opportunity to demonstrate effectiveness internally and externally to their organization or network. Robert Putnam, in *Tuning In, Tuning Out: The Strange Disappearance of Social Capital in America*, explores social capital in the United States. Here, he describes social capital as an attribute that allows individuals to increase their effectiveness in pursuit of common goals.<sup>89</sup>

---

<sup>87</sup> Burt, 65.

<sup>88</sup> Burt, 57-91.

<sup>89</sup> Robert Putnam, "Tuning In, Tuning Out: The Strange Disappearance of Social Capital in America," *PS: Political Science and Politics* 28-4, (1995): 665.

Well-coordinated and mutually supporting operations in the information environment are developed through the communication between different actors in the information warfare community and related interagency organizations. The FA30 must understand what organizations are best suited and poised to provide support to their unit during operations, and likewise, how their unit will affect the operations of the external organizations and broader U.S. government efforts. When support is requested from an external organization, the FA30 leverages their social capital to develop more efficient operations. In the information environment, coordinated and mutually supporting operations are to the benefit of both organizations. Because of social capital, where both actors have something to gain and lose, the involved organizations are able to increase their effectiveness in pursuit of shared objectives.

Bridging social capital is important because it helps groups break out of their insular echo chambers. Since FA30s do not belong to any specific IRC, they provide the bridging social capital needed for a unit to break down stovepipes and operate holistically in the information environment. Many members of the information warfare community are specialists in certain areas. PSYOP Soldiers excel at coordinating psychological operations while electronic warfare Soldiers excel at electronic warfare. The same holds true for the rest of the IW community. However, FA30s do not belong to any specific capability or function, and are therefore uniquely poised to assess the information environment more holistically than their counterparts. From this perspective, FA30s can support the integration and coordination of disparate information related capabilities in pursuit of achieving unique conditions and objectives for the commander. Information operations officers are well poised to identify key actors during any given operation in the information environment and integrate their specific functions to achieve unique and otherwise unidentified conditions. As Robert Putnam describes, this bridging function can provide “enhanced cooperation [that] is likely to serve broader interests and to be widely welcomed.”<sup>90</sup> The unique position, experience, and relationships of the FA30, brought by their social capital, serve as a bridge that connects the

---

<sup>90</sup> Putnam, “Tuning In, Tuning Out,” 665.

otherwise disconnected parts of the information warfare community. This enables the enhanced cooperation towards shared goals that Putnam describes.

FA30s also have the potential to serve as brokers between the Army and the Joint Force, as well as interagency partners that conduct operations in the information environment. The Department of State's Global Engagement Center (GEC) is tasked to "direct, lead, synchronize, integrate, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts."<sup>91</sup> An FA30 assigned to the GEC is well poised to provide their perspective on the information environment as a broker with bridging social capital. They can also leverage their experience working in the field to enhance both the GEC's operations and those of the U.S. Army, thus truly serving as a bridge to coordinate actions between the two organizations. In the information environment, it is critical to avoid conflicting messages. Not doing so can cause significant detriment to the effort. As a broker between the GEC and the Army, this FA30 has a vantage point to ensure that GEC operations do not conflict with the Army's, and likewise, that the Army does not detract from GEC operations. This individual can likely synchronize and coordinate operations to achieve mutually supporting and unique conditions for both networks and further support U.S. government efforts in the information environment.

### **3. Strength of Weak Ties**

In *The Strength of Weak Ties*, Granovetter discusses how weak ties between disparate parts of a system can enable a wider diffusion of information across the system.<sup>92</sup> He argues that "large-scale patterns" develop through "small-scale interactions."<sup>93</sup> To understand and analyze these small-scale interactions and their influence in diffusion and networks, he applies personal ties and their strength between the individuals. In this study, Granovetter uses the

---

<sup>91</sup> "Global Engagement Center, Core Mission & Vision," Department of State, accessed 07 June 2020, <https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/>.

<sup>92</sup> Mark Granovetter, "The Strength of Weak Ties," *American Journal of Sociology*, 73-6 (1973): 1366.

<sup>93</sup> Granovetter, "The Strength of Weak Ties," 1360.

time developing the tie, intensity, and reciprocity in the bond, among other characteristics, to determine the strength of the tie.<sup>94</sup> He concludes that the diffusion of information is more likely to “traverse greater social distance (i.e., path length), when passed through weak ties rather than strong.”<sup>95</sup> Accordingly, he argues that the removal of a weak tie, which subsequently forms a local bridge, can have greater damage to a network than the removal of a strong tie.<sup>96</sup>

This study by Granovetter presents evidence for the strength of the FA30 network in the information warfare community, the U.S. Army, and the broader U.S. government efforts in the information environment. Weak ties between FA30s develop bridges to parts of the system that are otherwise disconnected. These weak ties are created through previously associated contacts, colleagues met during professional education, or many other instances where a bond is formed. Because of the very low density of FA30s in the Army, they must rely on their weak ties to other parts of the system to maximize cross-communication and information diffusion across the system. As FA30s increase the amount of bonds they have with other FA30s, through events like professional education, deployments, or mutually shared assignments, the potential for future bridges in the network grows. As these individuals depart and are reassigned to disparate parts of the network, the number of weak ties connecting otherwise disconnected parts of the system grows. These ties serve as bridges between the otherwise disconnected system and enable a wider diffusion of information across U.S. government efforts in the information environment.

### **C. SOCIAL IDENTITY IN THE FA30 COMMUNITY**

The following section first outlines the positive impacts of social identity on organizations, specifically groups of occupational specialties and career fields within the U.S. Army. Second, this section describes the challenges that the FA30 community faces with developing a shared social identity, partly due to a lack of a consistent IO concept and formal organizational symbols, which can potentially undermine the FA30’s brokerage and

---

<sup>94</sup> Granovetter, 1361.

<sup>95</sup> Granovetter, 1366.

<sup>96</sup> Granovetter, 1365.



influence. The hypothesis is that a unified and distinct group identity amongst the U.S. Army's information warfare community would improve the trust, cohesion, and unity of effort between the FA30 community and the IRCs with whom they coordinate.

### **1. What is Social Identity and What are the Benefits?**

Social identity is an aspect of human psychology whose application transcends numerous fields of study. Two of the pioneers of social identity research were social scientist Henri Tajfel and his cohort John Turner, who described social identity as “those aspects of an individual's self-image that derive from the social categories to which he perceives himself as belonging.”<sup>97</sup> In other words, an individual's social identity is the degree to which they associate their own identity to that of the group, or groups, in which they belong. Thus, social identity theory is the study of how social identity impacts human relations within and between those groups.

Social psychologists use the theory to examine and understand human behavior as it relates to ingroup versus outgroup dynamics. Social identity researchers often focus on recognizing and mitigating the negative ramifications of social identity, which can lead to intergroup violence, prejudice, xenophobia, ethnocentrism, and racism. For example, social psychologists have previously demonstrated how members of one's social group, or “ingroup,” can develop hostilities towards a rival group, or “outgroup,” and vice versa. The Robber's Cave experiment demonstrated that social identity could facilitate hostile intergroup interactions under certain circumstances, by placing young boys into two competing groups (the “Eagles” and the “Rattlers”) who began to exhibit increasingly antagonistic behavior towards one another once their social identity became salient.<sup>98</sup> Furthermore, in her book *Uncivil Agreement: How Politics Became Our Identity*, author Lilliana Mason describes how identity-based partisan politics are increasingly dividing Americans and reducing

---

<sup>97</sup> Henri Tajfel, & J.C. Turner, “The Social Identity Theory of Intergroup Behavior,” in *Key readings in social psychology*, ed. J. T. Jost & J. Sidanius, (Psychology Press, 2004), 276-293, <https://doi.org/10.4324/9780203505984-16>.

<sup>98</sup> Muzafer Sherif, *The Robbers Cave Experiment: Intergroup Conflict and Cooperation*, originally published as *Intergroup Conflict and Group Relations*, (Middletown: Wesleyan University Press, 2010), chap. 5, ProQuest.

compromise, thereby impeding the American political system's ability to function properly.<sup>99</sup> These are just two examples of some harmful consequences of social identity.

However, social identity research also suggests that a well-established group identity can positively impact an organization's cohesion and effectiveness. Social identity theorists and researchers widely concur that positive group identity can improve cooperation, levels of effort and engagement, group decision-making, morale and motivation, information sharing and coordination, and the performance of tasks.<sup>100</sup> Simply put, members of an organization are more likely to perform their duties effectively and enthusiastically when they identify with the organization. This is especially true in the U.S. Army, where leaders commonly emphasize unit teamwork, cohesion, and morale to improve combat effectiveness and readiness. For this reason, military culture is infused with traditions and customs intended to maximize cohesion and group identity. Furthermore, members of the U.S. Army derive their social identity not only from their organizational unit, but also from their assigned duty position or military occupational specialty (MOS). The U.S. Army consists of 45 occupational branches and functional areas, each one with a unique identity of its own.<sup>101</sup> Upon qualification of their assigned tradecraft, group members assume their occupation's identity as part of their own, including its history, traditions, reputation, and credibility.

Furthermore, a group's identity facilitates trust-building, both within and outside of the organization. Granovetter describes five sources of trust in his book *Society and Economy: Framework and Principles*. Among these sources is trust based on memberships in groups and networks, which relates to the social identity and reputation of a group.<sup>102</sup> By cultivating a shared social identity amongst its group members, an organization builds both trust and influence. Indeed, an organization with a well-established identity is better positioned to

---

<sup>99</sup> Lilliana Mason, *Uncivil Agreement: How Politics Became Our Identity* (Chicago: The University of Chicago Press, 2018), 3.

<sup>100</sup> Blake Ashforth, Spencer Harrison, and Kevin Corley, "Identification in Organizations: An Examination of Four Fundamental Questions," *Journal of Management* 34, no. 3 (June 2008): 336-337, <https://doi.org/10.1177/0149206308316059>.

<sup>101</sup> "Officer Personnel Management Directorate," United States Army Human Resources Command, May 26, 2020, <https://www.hrc.army.mil/Officer/Officer%20Personnel%20Management%20Directorate>.

<sup>102</sup> Mark Granovetter, *Society and Economy: Framework and Principles*, (Cambridge, MA: Harvard University Press, 2017), chap. 3.

influence than an organization that lacks a shared purpose and identity. To illustrate, in their research article for *Academy of Management Review* titled “Social Identity Theory and the Organization,” authors Blake Ashforth and Fred Mael examined the existing body of theoretical and empirical work on social identity and influence, concluding:

[A] positive and distinctive organizational identity attracts the recognition, support, and loyalty of not only organizational members but other key constituents (e.g., shareholders, customers, job seekers), and it is this search for a distinctive identity that induces organizations to focus so intensely on advertising, names and logos, jargon, leaders and mascots, and so forth.<sup>103</sup>

In other words, organizations with reputable, trusted, and distinct identities are better able to wield external influence.

## **2. Social Identity in U.S. Army Information Operations**

The importance of an organization’s social identity carries enormous implications for the FA30 community’s ability to act as brokers and wield social capital in the information warfare community. As described earlier, most FA30s serve as either the sole IO officer or as members of a small section on a division or higher staff. Their specialized duty places FA30s in a unique position to interface directly with unit leadership, including the operations officer and even the commander. Because mission success could very well depend on the unit’s ability to conduct operations in the information environment, leadership places enormous trust in FA30s. Furthermore, FA30s operate in a coordinating capacity with neither the authority nor the mandate to direct the actions of IRCs on the battlefield. Thus, FA30s must rely on their influence and relationships to synchronize nested effects within the information environment in support of the commander’s objectives. To accomplish all of this, FA30s must have a strong, reputable, and consistent group identity which creates trust and influence with their peers and leadership. Unfortunately, this is not the current reality facing the FA30 community.

Instead, the FA30 community has struggled to establish a coherent social identity. This is not because of any failure on the part of the community’s leadership or members.

---

<sup>103</sup> Blake Ashforth and Fred Mael, “Social Identity Theory and Organization,” *The Academy of Management Review* 14, No. 1 (January 1989), 28, JSTOR.

Rather, the FA30 community faces unique challenges in creating a social identity, including the rapidly evolving nature of IO in military doctrine. In “Chapter 3 - IO in Design,” we discussed some of the issues created by the ever-changing terminology and definitions regarding IO in U.S. Army doctrine. Additionally, In COL Christopher Lowe’s monograph titled “From ‘Battle’ to ‘Battle of Ideas:’ The Meaning and Misunderstanding of Information Operations,” the author chronicles the history of the U.S. military’s attempts to define its operations in the information environment through such concepts as Command Control Communication Countermeasures (C3CM) and Command and Control Warfare (C2W) before designating the function as Information Operations in 1996.<sup>104</sup> Since then, the Army briefly replaced IO with Inform and Influence Activities (IIA) in the late 2010s before transitioning back to Information Operations in the latest edition of FM 3-13.<sup>105</sup> Today, the terms information dominance and information warfare have informally entered the lexicon, with neither clearly defined in doctrine, while the Joint Force appears ready to adopt the term Operations in the Information Environment (OIE) as part of the MDO concept.<sup>106</sup> With yet another potential name change on the horizon, it is only a matter of time before the term IO itself becomes outdated.

Admittedly, these frequent changes have been a necessary byproduct of “the rapidly changing nature of information, its flow, processing, dissemination, impact and [...] its military employment” as well as lessons learned from employing information in the persistent conflicts of the post-9/11 era.<sup>107</sup> Regardless, the frequent changes have created inconsistency and ambiguity about the fundamental purpose on which the FA30 profession is built, thereby contributing to its underdeveloped and muddled social identity. As a result, it is increasingly difficult for even the most articulate FA30s to explain their purpose clearly and concisely to

---

<sup>104</sup> Christopher Lowe, “From ‘Battle’ to ‘Battle of Ideas:’ The Meaning and Misunderstanding of Information Operations,” (Monograph, School of Advanced Military Studies, 2010), ii.

<sup>105</sup> Department of the Army, *Information Operations*, iv.

<sup>106</sup> Catherine Theohary, *Defense Primer: Information Operations*, CRS Report No. IF10771 (Washington, DC: Congressional Research Service, 2020), 2, <https://crsreports.congress.gov/product/pdf/IF/IF10771>.

<sup>107</sup> Department of the Army, *Information Operations*, vi.

their leaders and peers. This partially contributes to the widespread marginalization of the profession throughout the U.S. Army.

Undoubtedly, the lack of a clear and consistent organizational purpose can have severe ramifications both inside and outside of the organization. Ashforth and Mael describe the consensus amongst the existing body of work on social identity theory:

An organization has an identity to the extent there is a shared understanding of the central, distinctive, and enduring character or essence of the organization among its members. This identity may be reflected in shared values and beliefs, a mission, the structure and processes, organizational climate, and so on. The more salient, stable, and internally consistent the character of an organization [...] the greater this internalization.<sup>108</sup>

In contrast, the U.S. military's evolving approach to IO, far from creating a shared understanding, has instead generated ongoing confusion and ambiguity towards the FA30 community's purpose and identity. Without a clear purpose and identity amongst its information professionals, the U.S. Army consistently underperforms in the information environment. As discussed in the previous chapter, reflected in after-action reports from U.S. military combat training centers (CTCs), which indicate widespread misunderstandings and systemic illiteracy towards IO.<sup>109</sup> Truly, the issue extends beyond the social identity of the FA30 community and is creating operational problems for the U.S. Army.

Confusion surrounding IO terminology and definitions is not the only institutional hurdle that the FA30 community faces in pursuit of a group identity. Additionally, the FA30 community's small size and relative obscurity within the Army contributes to its lack of social identity. The active duty FA30 community consists of less than 300 commissioned officers, with no enlisted or warrant officer representation.<sup>110</sup> With an active duty Army of approximately 475,000, this means that the FA30 community amounts to approximately .06%

---

<sup>108</sup> Ashforth and Mael, "Social Identity Theory and the Organization," 27.

<sup>109</sup> Felix Figueroa, personal communication, May 26, 2020.

<sup>110</sup> U.S. Army IO Proponent, "Functional Area 30 (FA30) Information Operations (IO) Personnel Update," Leavenworth, KS: U.S. Army IO Proponent, May 5, 2020.

of the total active duty force.<sup>111</sup> Furthermore, the small FA30 community is dispersed across the U.S. Army in individual nodes or small clusters, with the notable exception being 1st Information Operations Command, the only active duty IO unit in the Army.<sup>112</sup> The wide distribution of FA30s is a necessary outcome of their specialized position on unit staffs, but as a result, the FA30 network is far less dense and cohesive than most other occupational specialties in the U.S. Army. As mentioned in the previous section of this chapter, this only increases the importance of the relationships and bonds that FA30s build with each other.

### **3. Social Identity and Organizational Symbolism**

Organizational symbolism is an element of social identity that represents a group's shared stories, narratives, ceremonies, and logos which characterize "the underlying character, ideology, or value system of an organization."<sup>113</sup> The impact of symbolism on a group's identity, cohesion, and morale cannot be understated. In fact, "through the manipulation of symbols such as traditions, myths, metaphors, rituals, sagas, heroes, and physical setting, management can make the individual's membership salient and can provide compelling images of what the group or organization represents."<sup>114</sup> In other words, organizational symbols, narratives, and lineage create both an outward representation of the profession's social identity and a tool to promote internal unity of effort amongst the members of the community.

In the U.S. military, organizational symbolism manifests itself in the form of heraldry. The U.S. Army Institute of Heraldry (TIOH) describes the purpose of heraldry as "a communication system that uses colors and symbols for the purpose of personal or organizational identification," and traces its origins back to the practical requirement of

---

<sup>111</sup> "Active Duty Military Personnel by Rank/Grade," Department of Defense, accessed April 30, 2020, [https://www.dmdc.osd.mil/appj/dwp/dwp\\_reports.jsp](https://www.dmdc.osd.mil/appj/dwp/dwp_reports.jsp).

<sup>112</sup> "1st IO Command: Victory Through the Power of Information," Department of the Army, accessed February 18, 2020, <https://www.1stiocmd.army.mil/Home/index>.

<sup>113</sup> Thomas Dandridge, Ian Mitroff, and William Joyce, "Organizational Symbolism: A Topic to Expand Organizational Analysis," *The Academy of Management Review* 5, No. 1 (January 1980), 77, JSTOR.

<sup>114</sup> Ashforth and Mael, "Social Identity Theory and the Organization," 28.

needing to identify heavily armored soldiers on the 11th and 12th-century battlefields.<sup>115</sup> To identify unit capabilities, Army basic branches each carry their own unique insignia and colors as well as mottos, mascots, and songs that celebrate the profession's lineage and history. Some branches even carry additional items of adornment, such as the blue cord worn by the infantry branch,<sup>116</sup> which is another outward expression of the group's identity. Additionally, most branches have adopted one or more branch-specific awards to recognize outstanding achievements within the profession, such as the Saint Barbara Award for the Field Artillery and Air Defense Artillery branches.<sup>117</sup> These symbols help facilitate a strong social identity within the organization.

Unfortunately, the FA30 community has limited options when it comes to organizational symbols, due in part to its status as a functional area as opposed to a basic branch. A functional area is "a grouping of officers by technical specialty or skills other than an arm, Service, or branch that usually requires unique education, training, and experience."<sup>118</sup> Functional areas are distinguishable from basic branches in that they do not carry their own insignia, colors, or other uniquely identifying symbols, and have little to no heraldry associated with them. Once an individual applies and becomes designated into a functional area, they remain administratively associated with their basic branch, including its heraldry. Consequently, professionals within U.S. Army functional areas retain the insignia, colors, symbolism, and overall identity of their originating branch. This leaves the FA30 community with little to no outward symbolic representation of its own unique organizational identity. This point should not be misconstrued. The Army FA30 community includes professionals from 19 different basic branches across four competitive categories,<sup>119</sup> and its diversity of occupational backgrounds and breadth of experience constitutes one of its greatest

---

<sup>115</sup> "What is Heraldry?" Department of the Army, accessed June 6, 2020. <https://tioh.army.mil/Catalog/HeraldryIntro.aspx>.

<sup>116</sup> Department of the Army, *Guide to the Wear and Appearance of Army Uniforms and Insignia*, DA PAM 670-1, (Washington, DC: Department of the Army, May 25, 2017), 235-236.

<sup>117</sup> "United States Field Artillery Association (USFAA) Awards," USFAA, accessed June 6, 2020, <https://fieldartillery.org/awards/>.

<sup>118</sup> Department of the Army, *Officer Professional Development and Career Management*, DA PAM 600-3, (Washington, DC: Department of the Army, April 3, 2019), 11.

<sup>119</sup> U.S. Army IO Proponent, "FA30 Personnel Update," May 5, 2020.

strengths. The operational, technical, and leadership backgrounds of each member is an irreplaceable resource to the community. However, while all members of the FA30 community can and should take pride in their originating branch, the FA30 community would nevertheless benefit from adopting its own organizational symbols and social identity.

#### **4. Organizational Symbolism in Army Information Operations**

Although options are limited, there are existing symbols that the FA30 community that the profession could adopt to represent the entire organization. The U.S. Army Information Operations Proponent (USAIOP) is the primary Army organization charged with all IO-related doctrine, organization, training, material, leadership, personnel, facilities, and policy (DOTMLPF-P) requirements.<sup>120</sup> The USAIOP manages the U.S. Army Information Operations Qualification Course (IOQC), and thus is credited with training, educating, and certifying every MOS-qualified FA30 in the U.S. Army. Clearly, the symbol of the USAIOP, as depicted in Figure 2, is an image that every IO profession in the U.S. Army can incorporate into their own social identity.



Figure 2. USAIOP symbol.<sup>121</sup>

Notably, the symbolism behind this prominent symbol was previously undocumented, or at least was inaccessible to the wider IO profession as a whole, prior to the research

---

<sup>120</sup> “U.S. Army Information Operations Proponent (USAIOP),” United States Army Combined Arms Center, accessed June 7th 2020, <https://usacac.army.mil/organizations/mccoe/iop>.

<sup>121</sup> Source: “U.S. Army Information Operations Proponent (USAIOP),” United States Army Combined Arms Center, accessed June 7th 2020, <https://usacac.army.mil/organizations/mccoe/iop>.



associated with this thesis. During the course of our research on organizational symbolism in the IO profession, we interviewed retired Lieutenant Colonel Mark Garrett, an FA30 and one of the individuals who participated in the creation of the symbol. From this, the researchers generated a proposal to the U.S. Army Institute of Heraldry, which is pending final approval as of publication of this thesis.

The USAIOP symbol prominently features a sword and lightning bolt combination, which is a recurring image in the IO profession. The 1st IO Command unit insignia, as depicted in Figure 3, also prominently features this motif. 1st IO Command officially adopted this logo on May 21, 2004, and the symbolism is described as follows: “The lightning flash denotes speed and the Command’s ability to strike wherever and whenever needed. The sword denotes the unit’s responsibility and ability to defend and protect all forces.”<sup>122</sup>



Figure 3. 1st Information Operations Command shoulder sleeve insignia.<sup>123</sup>

Of course, numerous Army units and occupational specialties claim variations of sword and lightning bolt as their symbol, including Army Special Forces where those components are notably featured on their shoulder sleeve insignia.<sup>124</sup> However, the 1st IO

---

<sup>122</sup> “1st Information Operations Command,” Department of the Army, accessed June 6, 2020, [https://tioh.army.mil/Catalog/Heraldry.aspx?HeraldryId=11986&CategoryId=7197&grp=2&menu=Uniformed Services&ps=24&p=0](https://tioh.army.mil/Catalog/Heraldry.aspx?HeraldryId=11986&CategoryId=7197&grp=2&menu=Uniformed%20Services&ps=24&p=0).

<sup>123</sup> “1st Information Operations Command,” Department of the Army, accessed June 6, 2020, [https://tioh.army.mil/Catalog/Heraldry.aspx?HeraldryId=11986&CategoryId=7197&grp=2&menu=Uniformed Services&ps=24&p=0](https://tioh.army.mil/Catalog/Heraldry.aspx?HeraldryId=11986&CategoryId=7197&grp=2&menu=Uniformed%20Services&ps=24&p=0).

<sup>124</sup> “Special Forces Shoulder Sleeve Insignia,” United States Army Special Operations Command, accessed June 8, 2020, <https://www.soc.mil/USASFC/Sleeve.html>.

Command's unique version of this symbol, with its single lightning bolt canted roughly 45 degrees, also features in the insignia of many IO units in the National Guard and Reserve. Figure 4 depicts a selection of these IO units which also have adopted a variation of insignia.

|                                                                                     |                                                                                                                                                                                                                                                                  |                                                                                                               |                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <b>U.S. Army Information Operations Proponent</b><br>"The sword demonstrates support to the warfighter and the overlap of effects between the physical and information domains. The five lightning flashes represent the original five core capabilities of IO." |                              | <b>71st Information Operations Group</b><br>"The lightning bolt denotes both the unit's electronic and signal warfare capabilities and the speed and ability for the unit to strike whenever and wherever needed."                                         |
|    | <b>1st Information Operations Command</b><br>"The lightning flash denotes speed and the Command's ability to strike wherever and whenever needed. The sword denotes the unit's responsibility and ability to defend and protect all forces."                     |                              | <b>151st Information Operations Group</b><br>"The lightning bolt and sword are adopted from the 1st Information Command and are symbolic to the Information Operations community."                                                                         |
|    | <b>1st Information Operations Battalion</b><br>"The lightning bolt alludes to electronic warfare and computer networking operations, to attack, defend, and exploit. The sword denotes the unit's responsibility and ability to defend all forces."              |                              | <b>301st Information Operations Battalion</b><br>"The sword refers to the warrior spirit. The lightning bolt alludes to zeal, action, courage, communication, and the necessity to synchronize all forms of communication for the success of the mission." |
|    | <b>2d Information Operations Battalion</b><br>"The lightning flash denotes speed, agility, and exploitation of the adversary. The sword denotes strength and dominance of the information environment."                                                          |                              | <b>302d Information Operations Battalion</b><br>"The lightning bolt signifies swiftness to disseminate information; the sword symbolizes training and security operations."                                                                                |
|   | <b>56th Information Operations Group</b><br>"The lightning bolt denotes speed and the unit's ability to strike wherever and whenever needed. The sword denotes the unit's responsibility and ability to defend and protect all forces."                          |                             | <b>152d Information Operations Group</b><br>"The crossed lightning flash and sword indicates speed and protection."                                                                                                                                        |
|  | <b>156th Information Operations Battalion</b><br>"The dagger recalls the Special Operations branches from which the unit evolved and denotes resources of strength and purpose in the dominant role filled within the information environment."                  | <b>Source: U.S. Army Institute of Heraldry</b><br><a href="https://tioh.army.mil/">https://tioh.army.mil/</a> |                                                                                                                                                                                                                                                            |

Figure 4. Sword and lightning bolt imagery in Army IO unit symbolism<sup>125</sup>

In 2004, 11 years after 1st IO command adopted its unit insignia, the U.S. Army adopted a similar sword and lightning bolt image as the branch insignia for the new Cyber Corps basic branch, as depicted in Figure 5.<sup>126</sup> Considering the proliferation of the image throughout Army IO culture, it is reasonable to propose that the crossed sword and lightning bolts could expand to represent the identity of the entire information warfare community, including FA30s.

<sup>125</sup> Adapted from "Information Operations," Department of the Army, accessed June 6, 2020. <https://tioh.army.mil/Catalog/HeraldryList.aspx?CategoryId=371&grp=2&menu=Uniformed%20Services>.

<sup>126</sup> "Cyber Corps: Insignia and Plaques," Department of the Army, accessed June 6, 2020, <https://tioh.army.mil/Catalog/Heraldry.aspx?HeraldryId=17896&CategoryId=9362&grp=2&menu=Uniformed%20Services&ps=24&p=0>.



Figure 5. Army Cyber Corps branch insignia<sup>127</sup>

## 5. Mercury and Hermes Symbolism in the Army IO Profession

Another prominent symbol that already exists in Army IO culture is the Roman messenger god Mercury and its synonymous Greek counterpart Hermes. As depicted in Figure 6, the name Mercury is invoked in the unit crests of both the 56th IO Group and 156th IO Battalion, with the phrase “Defend/Protect Mercury” which signifies the unit’s mission to protect information, according to the U.S. Army Institute of Heraldry.<sup>128</sup> Among mythological figures, Mercury seems to be a reasonable choice to represent the modern IO profession, with his speed and duty to carry information a solid analogy for the fast paced, internet-enabled information environment of modern times.

Additionally, the Information Professionals Association (IPA), a collaborative civilian and military professional organization focused on cognitive and information security-related issues, recently partnered with 1st IO Command to develop the Order of Hermes honorary award for information professionals.<sup>129</sup> The Order of Hermes was first awarded in 2018 as a joint venture between the IPA and 1st IO Command to “recognize individuals for exceptional service and contributions in the field of cognitive security and information operations.”<sup>130</sup> Like Mercury in the aforementioned examples, Hermes

---

<sup>127</sup> “Cyber Corps: Insignia and Plaques,” Department of the Army, accessed June 6, 2020, <https://tioh.army.mil/Catalog/Heraldry.aspx?HeraldryId=17896&CategoryId=9362&grp=2&menu=Uniformed%20Services&ps=24&p=0>.

<sup>128</sup> “56th Information Operations Group,” Department of the Army, accessed June 6, 2020, <https://tioh.army.mil/Catalog/HeraldryMulti.aspx?CategoryId=7205&grp=2&menu=Uniformed%20Services>.

<sup>129</sup> “Information Professionals Association,” Information Professionals Association, accessed June 6, 2020, <https://information-professionals.org/>.

<sup>130</sup> “Order of Hermes Award,” Information Professionals Association, accessed June 6, 2020, <https://information-professionals.org/order-of-hermes/>.

represents the speed of information, as well as the messenger god's inclination towards using disguises, deception, and stratagem as portrayed in Homer's *The Iliad*.<sup>131</sup> This suits the Information Operations profession well, given their core capability of military deception planning.



Figure 6. Selection of Army IO imagery depicting Mercury and Hermes.<sup>132</sup>

Clearly, either the Roman or Greek incarnation of the messenger god is already a suitable candidate for a unifying symbol of the information warfare community.

#### D. IMPLICATIONS AND RECOMMENDATIONS

The U.S. Army could enhance the social identity of its FA30 community by elevating the community to the status of a basic branch, either on its own or combined with other IRCs within the information warfare community to promote unity of effort. Elevating the FA30 community to the status of a basic branch would symbolically and appropriately raise Army IO to meet the challenges of future conflict. Furthermore, reinventing the FA30 community as a basic branch would enable it to formally adopt its own organizational symbols, colors, and other items of heraldry reserved for U.S. Army basic branches, thus facilitating the IO officer profession to further define its own identity and improve its social capital within the information warfare community. This concept would reflect the “Information Dominance” competitive category at the Army Human

---

<sup>131</sup> 1st IO Command Order of Hermes Award Proposal.

<sup>132</sup> Adapted from “Information Operations,” Department of the Army, accessed June 6, 2020. <https://tioh.army.mil/Catalog/HeraldryList.aspx?CategoryId=371&grp=2&menu=Uniformed%20Services>.

Resources Command (HRC), allowing IO and CEMA to remain as unique coded specialties under a single MOS area of concentration. This would both promote a more unified social identity between FA30s and the Cyberspace Corps, as well as better organize our IRC career fields per MDO doctrine's concept of convergence of effects.

Whether the FA30 profession is elevated as a basic branch on its own, or consolidated with other information-related professions, it would require a branch insignia symbol as an outward representation of the organization. Previously in this chapter, the researchers identified the crossed sword and lightning flash motif as a potential unifying symbol of the IO profession. Figure 7 depicts a stylized version of this insignia which could potentially serve as a branch insignia.



Figure 7. Proposed IO branch insignia.

Admittedly, this recommendation itself is neither novel nor unique. Military professionals recommended and advocated for the consolidation of IRC career fields into an “Information Warfare” branch since at least 2005.<sup>133</sup> However, since then, entities within the U.S. Army’s information warfare community have only become more disparate. This research paper adds to the growing call for unity of effort within the information warfare community by demonstrating its benefits through the lens of social network analysis and social identity theory.

---

<sup>133</sup> George Brown, “Do We Need FA30? Creating an Information Warfare Branch,” *Military Review* (January-February 2005), 39-43, <https://www.hsdl.org/?view&did=451582>.

## **E. WAY AHEAD**

As the U.S. Army transitions to multi-domain operations, it will seek to impose “multiple and compounding”<sup>134</sup> problems for the adversary on land, sea, air, space, cyberspace, and through the information environment. Operations in the information environment will be synchronized with more traditional forms of maneuver warfare to seek positions of advantage over our enemies. It is through the information warfare community that these operations will be developed, synchronized, coordinated, and executed in support of the Army and joint force operations. The U.S. Army’s FA30 is uniquely trained, educated, and well-poised in the network to provide these functions for the U.S. Army in contemporary and future conflict in multi-domain operations. To maximize their role in the network, the strength of the FA30 must rely on more than just the capabilities and reputation of the individual. They must derive from the reputation and social identity of the greater Information Operations community to form a stronger collective presence in the Army and joint force. The FA30 career field must be elevated to a level appropriately commensurate with the recognition of the expanded role of the information environment in multi-domain operations. Through improved organizational cohesion and greater trust within and for the FA30 community, FA30s will be better able to perform their role as synchronizers and coordinators of operations in the information environment.

---

<sup>134</sup> U.S. Army Training and Doctrine Command, *The U.S. Army in Multi-Domain Operations 2028*, iii.

## VI. CONCLUSION

Adversaries of the United States will continue to integrate information operations, information warfare, deception, and cyberspace operations more effectively during conflict and warfare. To maintain the competitive advantage that it is accustomed to, the U.S. Army must become more proficient and ready to detect, defend against, and defeat these threats. Part of this will require the Army to adapt so the force can more wholly and deliberately make these functions and capabilities a more common facet of its operations. In support of these efforts and the doctrinal shift to multi-domain operations, the Army is realizing how it can “pose multiple and compounding dilemmas on the adversary.”<sup>135</sup> In pursuit of these efforts, the Army must recognize and overcome obstacles and challenges to rectify the disparity between information operations in design and in practice.

Partly because the contemporary information environment changes so quickly, IO is one of the most significant topics of discussion amongst scholars, practitioners, and warfighters. The field of information operations resides on a very broad spectrum of related activities and there are often quite distinct differences between how many interpret and understand the role of IO.<sup>136</sup> Much of the misinterpretation and misunderstanding is largely self-imposed by numerous changes in the doctrine and even changing the name of the function itself. What began as a concept of Command Control Communication Countermeasures and Command and Control Warfare, became Information Operations in 1996, spent a brief time as Inform and Influence Activities, only to return to Information Operations again in 2016.<sup>137</sup> With each of these changes in the field, aspects of the function changed as well, conflating both the purpose and perceptions of IO. On this journey of self-realization, soldiers and leaders form a variety of misaligned opinions on the meaning and function of IO. Overtime, the amorphous meaning and doctrine of IO creates an

---

<sup>135</sup> U.S. Army Training and Doctrine Command, *The U.S. Army in Multi-Domain Operations 2028*, iii.

<sup>136</sup> Fecteau, *Understanding Information Operations and Information Warfare*.

<sup>137</sup> Lowe, "From 'Battle' to 'Battle of Ideas,'" ii.

environment where the force as a whole does not have a collective understanding of what IO is or how to properly integrate it.

Further compounding this issue, units in the Army are undertrained and undereducated in IO and it is under-represented in tactical units at brigade and below as demonstrated during unit rotations at the CTCs.<sup>138</sup> Without properly training and rehearsing the integration of IO during tactical unit exercises and rehearsals, true integration of IO into operations is an untenable objective. Understandably, with IO as a mere footnote in Army PME, it is not surprising that the soldiers and leaders in the force have only a broad conceptual understanding of how IO can enhance and support operations.

Doctrine, education, and training only go so far explaining the disparity between the design of IO and its application. The FA30 community is at a disadvantage because it lacks a coherent social identity. This impacts the community's overall effectiveness because social identity is directly tied to an organization's cohesion, morale, information sharing, coordination, and overall effectiveness.<sup>139</sup> The FA30 identity crisis is partly due to an Army-wide misunderstanding of IO following years of constantly changing IO doctrine, terminology, and theories of execution, which hurts the community's ability to internalize a clearly defined organizational purpose. Additionally, as a functional area, the FA30 community lacks any insignia, colors, and other uniquely identifying heraldry with which to outwardly distinguish itself and build group identity. As a result, the U.S. Army lacks an institutional shared understanding of both IO and the purpose of FA30s. The impact on the FA30 community's ability to perform its function is enormous. The absence of a cohesive organizational identity negatively impacts FA30's professional cohesion, degrades the FA30's organizational influence and credibility, and hinders its ability to function as coordinators of IRCs. The result is that many FA30s are marginalized, ignored, under-utilized, or incorrectly utilized.

The scope of Army IO is ambiguous and ill-defined. This inhibits both the force's understanding of the field as well as the practitioners' ability to describe their craft

---

138 Joint Multinational Readiness Center, "JMRC IO Trends for CGSC," May 26, 2020.

139 Ashforth, Harrison, and Corley, "Identification in Organizations," 336-337.



accurately and concisely, let alone fully integrate to the extent required in contemporary warfare. A deliberate return to the Joint and Army definition and purpose of IO can help rectify this challenge while helping to consolidate a shared identity in the career field. This can be furthered by anchoring IO to two clear and definable functions, military deception and operations security. As described throughout this study and the definition of IO in FM 3-13, IO has two clear purposes, to attack the enemy's decision-making process and protect our own.<sup>140</sup> The intent of MILDEC to cause an adversary to take either an action or inaction favorable to the friendly force is congruent with the first half of the definition of IO.<sup>141</sup> Similarly, OPSEC closely aligns and supports the second half of the definition of IO as this function aims to protect the operations and decision-making of the friendly force.<sup>142</sup> By taking clear ownership of both MILDEC and OPSEC, IO practitioners will have a clear, definable, and quantifiable purpose that will both enable them to more efficiently execute their craft as well as help form an identity to rally behind.

MILDEC will continue becoming more critical in warfare as the U.S. Army operates in constrained or contested environments. An IO practitioner that is educated, trained, and capable of integrating MILDEC into operations will be a significant contribution to any operation or plan in future conflict or competition. As U.S. adversaries continue to execute deception operations, a dedicated IO officer who can identify adversary deception and plan for counter-deception is critical. Similarly, adversaries will continue to seek ways to disrupt the decision-making processes of the friendly force. Through OPSEC, where critical indicators of operations are identified and obfuscated as described in JP 3-13.3, an IO practitioner can support the protection of our own processes. Taking ownership of these two functions as a field and anchoring to their purpose supports both a shared identity as well as a collective purpose.

The degree to which the FA30 community can overcome its identity crisis will determine how well the U.S. Army can recruit, train, retain, and employ its IO professionals

---

<sup>140</sup> Department of the Army, *Information Operations*, 1-2.

<sup>141</sup> Joint Chiefs of Staff, *Military Deception*, I-4.

<sup>142</sup> Joint Chiefs of Staff, *Operations Security*, JP 3-13.3, (Washington DC: Joint Chiefs of Staff, 2012), II-1.

to meet the current and future challenges of information warfare. One crucial component of a solution is the standardization of Joint IO definitions, terminology, focus, and scope across the entire DOD. The *Joint Concept for Operations in the Information Environment (JCOIE)* is an important step towards standardizing joint IO and building cooperative efforts between service branch IO professionals. The JCOIE emphasizes information as a critical component of multi-domain operations in current and future warfare. Even more important, it calls for a greater shared understanding of IO within the Joint force, including “a common lexicon, standardization of processes, and establishment of relationships that reduce or eliminate barriers to the integration of physical power and informational power.”<sup>143</sup> The institutional standardization of IO across the DOD would help each service branch build a cohesive organizational identity within its community of IO professionals, as well as help create an overall Joint IO community which is currently non-existent.

For its part, the U.S. Army should consider elevating the FA30 profession to the status of a branch. The establishment of an IO branch would symbolically raise the importance of the Army IO profession to a level commensurate with the expanded role of information in MDO. Additionally, it would also enhance the organizational identity of the profession by creating branch insignia and other organizational symbolism with which to outwardly express itself.

Without a doubt, the U.S. Army FA30 performs an essential role in information warfare, and the importance of the position will only increase as the information environment becomes more central in current and future warfare. The U.S. Army will continue to require staff experts focused on the holistic integration of all information-related effects, and the FA30 will fill that role regardless of whatever form the position takes. By standardizing Joint and Army IO doctrine and terminology, as well as investigating the possibility of creating an IO branch, the Army can help build the identity and capability of its IO community, thus better empowering them to wage information warfare in future conflicts.

---

<sup>143</sup> Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (JCOIE)*, (Washington DC: Joint Chiefs of Staff, 2018), ix.

## LIST OF REFERENCES

- Ashforth, Blake, and Fred Mael. "Social Identity Theory and Organization." *The Academy of Management Review* 14, No. 1 (January 1989): 20–29. JSTOR.
- Ashforth, Blake, Spencer Harrison, and Kevin Corley. "Identification in Organizations: An Examination of Four Fundamental Questions." *Journal of Management* 34, no. 3 (June 2008): 325–374. <https://doi.org/10.1177/0149206308316059>.
- Brantly, Aaron F., Nerea M. Cal, and Devlin P. Winkelstein. *Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW*. Report Number AD1046052. West Point, NY: Army Cyber Institute, 2017. <https://apps.dtic.mil/dtic/tr/fulltext/u2/1046052.pdf>.
- Brown, George. "Do We Need FA30? Creating an Information Warfare Branch." *Military Review* (January-February 2005). 39–43, <https://www.hsdl.org/?view&did=451582>.
- Burt, Ronald. 1992. "The Social Structure of Competition." Pp. 57–91 in *Networks and Organizations: Structure, Form and Action*, edited by Nitin Nohria and Robert G Eccles. Boston: Harvard University Press.
- Crane, Conrad. "The United States Needs an Information Warfare Command: A Historical Examination." *War on the Rocks*, June 14, 2019. <https://warontherocks.com/2019/06/the-united-states-needs-an-information-warfare-command-a-historical-examination/>.
- Dandridge, Thomas, Ian Mitroff, and William Joyce. "Organizational Symbolism: A Topic to Expand Organizational Analysis." *The Academy of Management Review* 5, No. 1 (January 1980). JSTOR.
- Department of Defense. "Active Duty Military Personnel by Rank/Grade." April 30, 2020. [https://www.dmdc.osd.mil/appj/dwp/dwp\\_reports.jsp](https://www.dmdc.osd.mil/appj/dwp/dwp_reports.jsp).
- Department of Defense. *Information Operations*, DOD Directive 3600.01. Washington, DC: Department of Defense, 2013.
- Department of Defense. *Summary: Department of Defense Cyber Strategy 2018*. Washington, DC: Department of Defense, 2018. [https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER\\_STRATEGY\\_SUMMARY\\_FINAL.PDF](https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF).
- Department of State. "Global Engagement Center, Core Mission & Vision." Accessed June 7, 2020. <https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/>.

- Department of the Army. "1st Information Operations Command." Accessed June 6, 2020. [https://tioh.army.mil/Catalog/Heraldry.aspx?HeraldryId=11986&CategoryId=7197&grp=2&menu=Uniformed Services&ps=24&p=0](https://tioh.army.mil/Catalog/Heraldry.aspx?HeraldryId=11986&CategoryId=7197&grp=2&menu=Uniformed%20Services&ps=24&p=0).
- Department of the Army. "1st IO Command: Victory Through the Power of Information." Accessed February 18, 2020. <https://www.1stiocmd.army.mil/Home/index>.
- Department of the Army. "56th Information Operations Group." Accessed June 6, 2020. <https://tioh.army.mil/Catalog/HeraldryMulti.aspx?CategoryId=7205&grp=2&menu=Uniformed%20Services>.
- Department of the Army. "Cyber Corps: Insignia and Plaques." Accessed June 6, 2020. [https://tioh.army.mil/Catalog/Heraldry.aspx?HeraldryId=17896&CategoryId=9362&grp=2&menu=Uniformed Services&ps=24&p=0](https://tioh.army.mil/Catalog/Heraldry.aspx?HeraldryId=17896&CategoryId=9362&grp=2&menu=Uniformed%20Services&ps=24&p=0).
- Department of the Army. *Guide to the Wear and Appearance of Army Uniforms and Insignia*. DA PAM 670-1. Washington, DC: Department of the Army, 2017.
- Department of the Army. *Information Operations*. FM 3-13. Washington, DC: Department of the Army, 2016.
- Department of the Army. *Officer Professional Development and Career Management*. DA PAM 600-3. Washington, DC: Department of the Army, 2019.
- Department of the Army. *Information Operations Functional Area*. DA PAM 600-3 Smartbook. Washington, DC: Department of the Army, 2017. <https://www.milsuite.mil/book/groups/smartbook-da-pam-600-3>.
- Department of the Army. "What is Heraldry?" Accessed June 6th, 2020. <https://tioh.army.mil/Catalog/HeraldryIntro.aspx>.
- Fecteau, Matthew. *Understanding Information Operations and Information Warfare: The Muddled Meaning of IO (and IW)*. Global Security Review. Last modified June 7, 2019. <https://globalsecurityreview.com/understanding-information-operations-information-warfare/>.
- Fogarty, Stephen, and Bryan Sparling. "Enabling the Army in an Era of Information Warfare." *The Cyber Defense Review*. Volume 5, No. 2 (Summer 2020). 17–25.
- Fowler, Charles and Robert Nesbit. "Tactical Deception in Air-Land Warfare." *Journal of Electronic Defense*. (June 1995): 37–79.
- Granovetter, Mark. *Society and Economy: Framework and Principles*. Cambridge, MA: Harvard University Press, 2017.

- Granovetter, Mark. "The Strength of Weak Ties." *American Journal of Sociology*. 73–6. 1973.
- Information Professionals Association. "Information Professionals Association." Accessed June 6, 2020. <https://information-professionals.org/>.
- Information Professionals Association. "Order of Hermes Award." Accessed June 6, 2020. <https://information-professionals.org/order-of-hermes/>.
- Jajko, Walter. "Deception: Appeal for Acceptance; Discourse on Doctrine; Preface to Planning." *Comparative Strategy*, volume 21 (2001): 351–363.
- Joint Chiefs of Staff. *Information Operations*. JP 3-13. Washington, DC: Joint Chiefs of Staff, 2014.
- Joint Chiefs of Staff. *Joint Information Operations Proponent*. CJCSI 3210.01. Washington, DC: Joint Chiefs of Staff, 2014.
- Joint Chiefs of Staff. *Military Deception*. JP 3-13.4. Washington, DC: Joint Chiefs of Staff, 2017.
- Joint Chiefs of Staff. *Operations Security*. JP 3-13.3. Washington, DC: Joint Chiefs of Staff, 2012.
- Kofman, Michael. "Russian Hybrid Warfare and Other Dark Arts." *War on the Rocks* (March 2016).
- Lowe, Christopher. "From 'Battle' to 'Battle of Ideas:' The Meaning and Misunderstanding of Information Operations." Monograph, School of Advanced Military Studies, 2010.
- Mason, Lilliana. *Uncivil Agreement: How Politics Became Our Identity*. Chicago: The University of Chicago Press, 2018.
- McArdle, Jennifer. "Pioneers of Deception: Lessons from the Ghost Army." *War on the Rocks* (May 2018).
- Paul, Christopher. "On Strategic Communication Today: Enhancing U.S. Efforts to Inform, Influence, and Persuade." *Parameters* 46, no. 3 (2016): 87–97.
- Putnam, Robert. "Tuning In, Tuning Out: The Strange Disappearance of Social Capital in America." *PS: Political Science and Politics* 28, no. 4 (1995): 664–683.
- Sherif, Muzafer. *The Robbers Cave Experiment: Intergroup Conflict and Cooperation*, originally published as *Intergroup Conflict and Group Relations*. Middletown: Wesleyan University Press, 2010. ProQuest.

- Theohary, Catherine A. *Information Warfare: Issues for Congress*. R45142. Washington, D.C., Congressional Research Service, 2018.
- United States Army Combined Arms Center. “Combined Training Center Directorate.” Accessed August 17, 2020. <https://usacac.army.mil/organizations/cact/ctcd>.
- United States Army Combined Arms Center. “U.S. Army Information Operations Proponent (USAIOP).” Accessed June 7, 2020. <https://usacac.army.mil/organizations/mccoe/iop>.
- United States Army Command and General Staff College. “Advance Sheet for Lesson M333: Information Operations.” M333 AS, Leavenworth, KS: U.S. Army Command and General Staff College. October 2019.
- United States Army Human Resources Command. “Officer Personnel Management Directorate.” Accessed May 26, 2020. <https://www.hrc.army.mil/Officer/Officer%20Personnel%20Management%20Directorate>.
- United States Army IO Proponent. “Functional Area 30 (FA30) Information Operations (IO) Personnel Update.” Leavenworth, KS: U.S. Army IO Proponent. May 5, 2020.
- United States Army Special Operations Command. “Special Forces Shoulder Sleeve Insignia.” Accessed June 8, 2020. <https://www.soc.mil/USASFC/Sleeve.html>.
- United States Army Training and Doctrine Command. *The U.S. Army in Multi-Domain Operations 2028*. TRADOC PAM 525-3-1. Fort Eustis, Virginia: U.S. Training and Doctrine Command, 2018.
- United States Army Training and Doctrine Command. *U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025–2045*. TRADOC PAM 525-3-8. Fort Eustis, Virginia: U.S. Army Training and Doctrine Command, 2018.
- United States Field Artillery Association. “USFAA Awards.” Accessed June 6, 2020. <https://fieldartillery.org/awards/>.
- Valeriano, Brandon, Benjamin Jensen, and Ryan Maness. *Cyber Strategy: The Evolving Character of Power and Coercion*. New York: Oxford University Press, 2018. Kindle.
- Vavra, Shannon. “Here’s how Army Cyber Command plans to take on information warfare.” *Cyberscoop*. July 29, 2020. <https://www.cyberscoop.com/army-cyber-command-plan-transition-information-war/>.

Williams, Michael. "Speed, Volume, and Ubiquity: Forget Information Operations & Focus on the Information Environment." *The Strategy Bridge*, July 26 2017.  
<https://thestrategybridge.org/the-bridge/2017/7/26/speed-volume-and-ubiquity-forget-information-operations-focus-on-the-information-environment>.

Zallo, David J. "Ready, Willing, and Able: Picking a Brigade Combat Team Information Operations Officer." *Center for Army Lessons Learned Newsletter*. No. 17–18 (June 2017): 51–56.

THIS PAGE INTENTIONALLY LEFT BLANK



## **INITIAL DISTRIBUTION LIST**

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California