

FUTURE BATTLEFIELD TRENDS IN THE REALM OF INFORMATION OPERATIONS
AND INSTITUTIONALIZING INFORMATION OPERATIONS ARCHITECTURE
FOR THE BANGLADESH ARMY AND WAY FORWARD

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

ABU MD SHAHNOOR SHAWON, MAJOR, BANGLADESH ARMY
MSMS, Bangladesh University of Professionals, Bangladesh, 2018

Fort Leavenworth, Kansas
2019

Approved for public release; distribution is unlimited. United States Fair Use determination or copyright permission has been obtained for the use of pictures, maps, graphics, and any other works incorporated into the manuscript. This author may be protected by more restrictions in their home countries, in which case further publication or sale of copyrighted images is not permissible.

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this 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 Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 14-06-2019		2. REPORT TYPE Master's Thesis		3. DATES COVERED (From - To) AUG 2018– JUN 2019	
4. TITLE AND SUBTITLE Future Battlefield Trends in the Realm of Information Operations and Institutionalizing Information Operations Architecture for the Bangladesh Army and Way Forward				5a. CONTRACT NUMBER +8801769006915	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Major Abu Md Shahnoor Shawon				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301				8. PERFORMING ORG REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for Public Release; Distribution is Unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT With rapidly proliferating technology, the Bangladesh (BD) Army is increasingly becoming vulnerable in the information environment. Recognizing the urgency, the army has already established a few structures for dealing with Information domain. This research considers that the existing infrastructure is not sufficient for providing adequate protection to its information environment. At this milieu, the researcher carried out this research through a quantitative analysis involving document study, content analysis, and researcher's first-hand experience about the subject matter. The research reflected an accurate picture of the existing structure of the BD Army and drew the necessity of devising an architecture for Information Operations (IO). In the beginning, the researcher studied the evolution of IO doctrines keeping the requirement of future warfare in the realm of IO. Then, the researcher identified the vulnerabilities of the present system. Through an analysis of different army doctrine, the researcher painted a comprehensive view of the latest trends of IO. Finally, in search of a pragmatic solution, this research suggests measures to overcome the limitation and develop an IO architecture. In the end, some recommendations were proposed. It is expected that this suggested IO architecture will help the BD Army to operate well in the information domain.					
15. SUBJECT TERMS Information Operation architecture of Bangladesh Army, Characteristics and Nature of Future Warfare in the realm of Information Operation, Information Environment.					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT (U)	b. ABSTRACT (U)	c. THIS PAGE (U)			19b. PHONE NUMBER (include area code)
			(U)	141	

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Abu Md Shahnoor Shawon

Thesis Title: Future Battlefield Trends in the Realm of Information Operations and
Institutionalizing Information Operations Architecture for the Bangladesh
Army and Way Forward

Approved by:

_____, Thesis Committee Chair
Steven A. Boylan, D.M.

_____, Member
Lieutenant Colonel Philip D. Martin, M.A.

_____, Member
Lieutenant Colonel Aljone D. Lopes, M.A., MMSc

Accepted this 14th day of June 2019 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

FUTURE BATTLEFIELD TRENDS IN THE REALM OF INFORMATION OPERATIONS AND INSTITUTIONALIZING INFORMATION OPERATIONS ARCHITECTURE FOR THE BANGLADESH ARMY AND WAY FORWARD, by Major Abu Md Shahnoor Shawon, 141 pages.

With rapidly proliferating technology, the Bangladesh (BD) Army is increasingly becoming vulnerable in the information environment. Recognizing the urgency, the army has already established a few structures for dealing with Information domain. This research considers that the existing infrastructure is not sufficient for providing adequate protection to its information environment. At this milieu, the researcher carried out this research through a quantitative analysis involving document study, content analysis, and researcher's first-hand experience about the subject matter. The research reflected an accurate picture of the existing structure of the BD Army and drew the necessity of devising an architecture for Information Operations (IO). In the beginning, the researcher studied the evolution of IO doctrines keeping the requirement of future warfare in the realm of IO. Then, the researcher identified the vulnerabilities of the present system. Through an analysis of different army doctrine, the researcher painted a comprehensive view of the latest trends of IO. Finally, in search of a pragmatic solution, this research suggests measures to overcome the limitation and develop an IO architecture. In the end, some recommendations were proposed. It is expected that this suggested IO architecture will help the BD Army to operate well in the information domain

ACKNOWLEDGMENTS

The journey of MMAS has been immeasurably rewarding for my professional development. At the time of selecting my subject for the thesis, I did not have adequate knowledge of the subject matter. However, in the process of developing my thesis, I learned commendable knowledge of the subjects that led me to the end of my research. I am sanguine this work is going to be very valuable for the Bangladesh Army as a start point of Information Operations Infrastructure.

I want to express my deepest gratitude to my wife, Sumaiya Sharmin Hridi, who relentlessly supported me by taking care of our home and reinvigorating my energy to let me work to the best of my ability. All the way, she dedicated her time for the grooming up for our daughter to spare me for studies. Her dedication and sacrifices worked as an inspiration for me. The lovely ever-smiling face of my three years old bundle of joy, Fatima was my source of inspiration and liveliness. She is the reason for our happiness. The priceless memories that we acquired in the last one year by being part of such a prestigious institution and U.S. military family are something we will cherish all our life.

I am pleased to express my heartfelt respect and profound gratitude to chairperson and committee for their keen interest, worthy supervision, inspiration, relentless support, helpful comment, and constant direction throughout the working period. The thesis would not have seen the light of success without their active involvement and care for me. The committee mentored, coached, and directed me to the appropriate direction in a methodical way to acquire adequate knowledge on the subject and devise appropriate approaches to reach its objectives.

Last but not the least; I would like to express my heartfelt thanks to the Command and General Staff College and Combined Arms Research Library for assisting me by supplying necessary documents for this study. Without their dedicated and invaluable support, the research would not come to success. I am grateful to all whom I, formally or informally, discussed, interviewed, surveyed, and consulted in connection with his research. Above all, I am thankful to the Almighty Allah for His eternal mercy.

TABLE OF CONTENTS

	Page
MASTER OF MILITARY ART AND SCIENCE THESIS APPROVAL PAGE	iii
ABSTRACT.....	iv
ACKNOWLEDGMENTS	v
TABLE OF CONTENTS.....	vii
ACRONYMS.....	x
ILLUSTRATIONS	xii
CHAPTER 1 INTRODUCTION AND OVERVIEW	1
The Purpose of the Study.....	1
Statement of the Problem.....	3
Research Questions	4
Primary Research Question.....	4
Secondary Research Question.....	4
The Significance of the Research	5
Assumptions.....	5
Important Definitions.....	5
Scope.....	12
Limitations	13
Delimitations.....	13
Author’s Qualifications and Justification	13
Summary	15
Conclusions.....	15
CHAPTER 2 LITERATURE REVIEW	17
Chapter Introduction	17
International Military Doctrines Published on IO	18
Bangladesh Army Publications.....	26
Domestic Research Work and Journal Articles	27
International Publications, Journal Articles, and Books works	29
International Research Papers.....	32
Summary	34
CHAPTER 3 RESEARCH METHODOLOGY	36
Chapter Introduction	36

Research Methodology	37
Primary Data	39
Secondary Data	39
Scope and Limitations	40
Definitions and Terminologies	41
Chapter Summary	43
 CHAPTER 4 FUTURE BATTLEFIELD TRENDS, THREAT PERCEPTION, AND EVOLVING DOCTRINAL CONCEPTS AND INTERNATIONAL EVOLUTION OF IO ORGANIZATION	44
Chapter Introduction	44
Characteristics of Future Operations	46
Effects of IO in Future Warfare	53
Assessment of Threats and Vulnerabilities: Bangladesh Army Perspective	55
Potential IO Threat Scenario of Bangladesh: Regional Context	56
Force Management Aspects	59
Advantages for the Bangladesh Army for Incorporating IO	60
Organizational Comparison and Contrast between All Doctrines	64
The U.S. Army Doctrine	65
The NATO	75
The British Army Doctrine	75
Canadian Doctrine	80
Australian Doctrine	86
Russian Doctrine	90
Chapter Summary	92
Recommendations to Establish an IO Architecture for Bangladesh Army	94
Integration at the National Level	94
Integrating IO Architecture Organizationally	95
Establishing an IO Brigade under the Army Headquarters	96
Formulation a Viable Command and Staff Network	97
Introducing the IO as a Career Field for the Officers	98
Conversion of Soldiers to Information Operations (IO) Trade	99
Developing an Information Operation Doctrine	100
Establishing a Training Facility for Imparting Institutional Training	101
Material Acquisition for Information Operation	101
Policy Development	102
Develop a Defensive IO Architecture	102
Establishing Active Directory	104
Chapter Conclusion	104
 CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS	106
Chapter Introduction	106
Conclusion	107
Recommendation	115

Recommendations for Future Research	116
Closing Thoughts	117
GLOSSARY	119
REFERENCE LIST	121

ACRONYMS

AFD	Armed Forces Division
AHQ	Army Headquarters
ARTDOC	Army Training and Doctrinal Command
BMS	Battlespace Management System
BTRC	Bangladesh Telecommunication Regulatory Commission
BOS	Battlefield Operating System
CAF	Canadian Armed Forces
CIS	Communication Information System
C2W	Command and Control Warfare
C3I	Command Control Communication and Information
CUC	Common User Core
DoD	Department of Defense
EW	Electronic Warfare
GoB	Government of Bangladesh
HQ	Headquarters
IBW	Information Based Warfare
ICT	Information and Communication Technology
IO	Information Operation
IA&O	Information Activities and Outreach
IIA	Information and Influence Activities
IRC	Information Related Capabilities
IT	Information Technology
IW	Information Warfare

JTFHQ	Joint Task Force Headquarters
MDMP	Military Decision Making Process
MISO	Military Information Support Operation
MOD	Ministry of Defence
MoU	Memorandum of Understanding
MS Br	Military Secretary Branch
NCW	Network Centric Warfare
NIC	National Intelligence Council
NSC	National Security Council
OPSEC	Operational Security
RMA	Revolution in Military Affairs
SJS	Strategic Joint Staff
(UAS)	Unmanned Aerial Systems
UN	United Nations
WMD	Weapon of Mass Destruction

ILLUSTRATIONS

	Page
Figure 1. Information Environment.....	6
Figure 2. Information Related Capabilities	8
Figure 3. IO Relationship over Time.....	10
Figure 4. EW in Integrated IO.....	11
Figure 5. Operationalization Diagram.....	40
Figure 6. Operational Approach	42
Figure 7. Comprehensive Mobile Threat Model	58
Figure 8. Problem-solving Construct Widely Used by U.S. Military	59
Figure 9. Multi-Domain Extended Battlefield.	61
Figure 10. When a Cyber Attack Encircles the Rings of Protection.....	63
Figure 11. Dynamic Continuum of Information Operations	66
Figure 12. National Information Operation Cell	68
Figure 13. U.S. Army Cyber Command Deployment.....	69
Figure 14. The 1st IO Command (Land) Organization	70
Figure 15. IO Cell.....	72
Figure 16. IIA Running Estimate and the MDMP	74
Figure 17. Organization of 1st ISR Brigade, UK.....	77
Figure 18. The Structure of British 77th Brigade.....	78
Figure 19. Deployment of the 77th Brigade.....	79
Figure 20. IO Structure Division and Below.....	80
Figure 21. Components of IO Structure	82
Figure 22. Integration of IO within the Strategic Communication Framework	83

Figure 23. Architecture at the Operational Level.....	85
Figure 24. Components of IO in Canadian Doctrine.....	86
Figure 25. Relationship between Domains.....	87
Figure 26. Coordination of Information Activities	88
Figure 27. The Information Environment	93
Figure 28. Linkage between System	95
Figure 29. Proposed IO Architecture for Bangladesh Army.....	96
Figure 30. IO Command and Staff Structure	98
Figure 31. The Procedure of Conversion to IO Trade.....	99
Figure 32. Information Operation according to U.S. Doctrine	100
Figure 33. Typical Commercial Multiple-Layer Network Security Architecture.....	103

CHAPTER 1

INTRODUCTION AND OVERVIEW

All warfare is based on deception . . . victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to will . . . the supreme art of war is to subdue the enemy without fighting.

—Sun Tzu, *Art of War*

The Purpose of the Study

Sun Tzu captured the idea of how all warfare begins in what now has been conceptualized as the information environment. The famous theorist Carl Von Clausewitz also stated that the objective of war is to impose our will on the enemy (Clausewitz 1989). This maxim illustrates the importance of Information Operations (IO) by which one can effectively impose their will on the enemy. The achievements of the industrial and information ages are shaping a world to come that is both more dangerous and richer with opportunity than ever before (NIC 2017, 4). The IO, also known as influence operation in some Army doctrine, includes a collection of information about an adversary as well as dissemination of propaganda in pursuit of a competitive advantage over an opponent (RAND 2019). With rapidly proliferating technology, a myriad of new threats is emerging and making the operational environment more complex. For this reason, it is imperative for every Army to understand IO and integrate it methodically in the institution.

Moreover, ‘Information’ is also considered as one of the elements of national power. The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. Conceptually, the information environment encompasses both tangible (physical) elements and intangible

elements (such as human ideas, fears, perceptions, and decision-making (HQDA 2017, I-1). It influences the diplomacy, trade, and economy, and most importantly all political and territorial conflict scenarios for a country. The information environment is in constant evolution. It is ever changing with the invention of new technology. IO doctrinally has many core capabilities such as public affairs operations, military information support operations (MISO), combat camera, soldier and leader engagement, civil affairs operations, civil and cultural considerations, operations security (OPSEC), and military deception (HQDA 2013, 1-1).

The Bangladesh Army should establish a standing IO capability to deter any threat to its information environment. For many years, the world security matrix had a profound paradigm shift from state-centric to information-centric approach. However, the trend got the attention of the military only very recently. The Bangladesh Army has already established an organization to work for the IRC. However, there is a need for an integrated IO architecture to obtain a synergistic effect. Today, the wireless and wired mediums of communication are converging. For any military in the world, any hostile adversary can now wage information attacks anonymously from the global sphere. The ‘information’ support infrastructures are therefore becoming extremely vulnerable to hostile attacks if they are not protected well. These attacks can quickly paralyze any military organization and above all the nation that is severely dependent on information and information systems. Hence, it is imperative to understand the prevalent information environment to identify specific sectors that are vulnerable to information breach, manipulation, and exploitation.

Globally, the non-state actors have capitalized the information environment as the new battleground to dominate, and they are already making impacts. The threat from terrorism will expand in the coming decades as the growing prominence of small groups, and individuals use new technologies, ideas, and relationships to their advantage. Most of the modern Armies of the world have conceptualized the IO and are using it to shape the operational environment. For the United States (US) Army, over the last several years, the concept of IO had matured from abstract, embryotic concept into a fledging mainstream community of professional practitioners (Mannion 2018, 1). Therefore, Bangladesh Army needs a viable architecture for the IO to protect its information environment from the adversary.

Statement of the Problem

With the expansion of the Information environment, the future battlefield will be primarily in the spectrum of Information domain. Therefore, it is going to be short, intense, complex, net-centric, and intertwined with sophisticated technology. Profoundly the conduct of future warfare will be based on sensors, satellite, and modern communication gadgets. The added dimension in the spectrum of the IO is cyberspace, which is going to make the operational environment more complex and fragile. As such, transforming towards a well-constructed IO infrastructure will facilitate the Army in fulfilling the operational prerequisite of the future war in the realm of the information environment. Understanding the importance, most of the modern armies of the world have already established IO architecture to conform to future warfare. Identifying the necessity Bangladesh Army has already integrated different branches at headquarter level to incorporate different Information related

capabilities. Most importantly, this year Bangladesh has launched her satellite and Bangladesh Armed Forces got a significant share of the satellite through a transponder (BTRC 2018). On the other hand, Forces Goal-2030, which focuses on preparing the Bangladesh Army for future battlefield challenges, is being implemented phase by phase. As such, this is the right time to establish a viable IO architecture for the Bangladesh Army to conduct IO more systematically.

Research Questions

Primary Research Question

What should be the appropriate architecture of IO for the Bangladesh Army to conform to the future battlespace trends related to information environment?

Secondary Research Question

1. What are the trends of future warfare in the realm of IO and preparation of Bangladesh Army?
2. What are the potential IO threat scenario of Bangladesh Army in terms of IO in the regional and global context?
3. What is the present state of IO in the perspective of Russian, Canadian, United Kingdom, and U.S. Army?
4. Is the existing infrastructure of Bangladesh Army capable of establishing IO architecture?
5. What are the challenges of Bangladesh Army in developing an IO architecture?

The Significance of the Research

This intellectual discourse endeavors to unveil viable doctrinal fundamentals of IO to help secure vital information domain of Bangladesh Army. This will allow the army to track, forecast, manipulate, exploit, or disable enemy information systems in order to defend its own crucial information resource. This research may particularly draw the attention of operations and intelligence community of Bangladesh Army in general, and communication and Information Technology (IT) professionals in particular. Identified doctrinal facets, imperatives, and deductions in regards to defensive IO (electronic defense) would contribute significantly to formulating full-fledged IO doctrine for Bangladesh Army.

Assumptions

To develop the thesis in the correct direction and fulfill its purpose, the author assumes that the developed armies like the US, Russian, Canadian, UK, and Australian Army have already reached to a comprehensive framework to operate effectively in the IO domain. Therefore, the researcher took those doctrines in a preview of the study.

Important Definitions

Information Environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. Conceptually, the information environment encompasses both tangible (physical) elements and intangible elements (such as human ideas, fears, perceptions, and decision-making (CJCS 2012, I-1). Figure-1 illustrates the information environment.

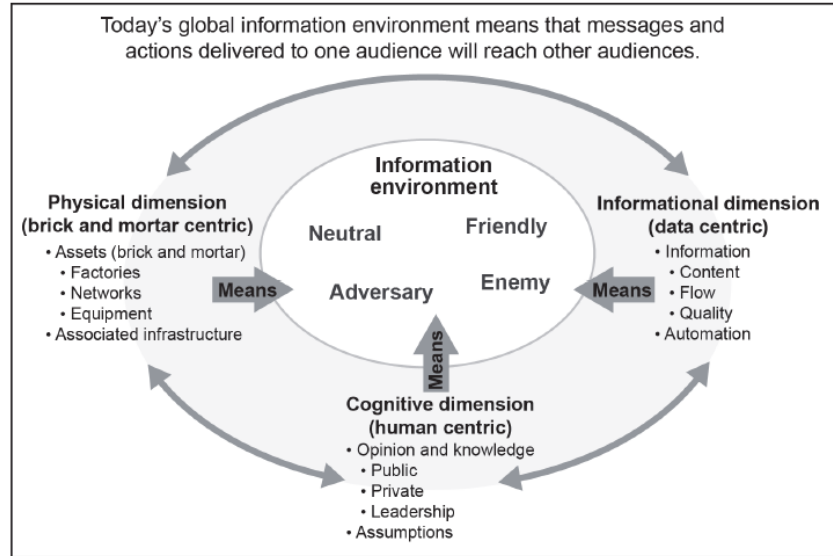


Figure 1. Information Environment

Source: CJCS 2012, I-1.

Inform and Influence Activities (IIA). The integration of designated information-related capabilities in order to synchronize themes, messages, and actions with operations to inform the United States and global audiences, influence foreign audiences, and affect adversary and enemy decision-making. (HQDA 2013, Glossary-2)

Information Operation (IO). 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. Also called IO. (CJCS 2012, GL-3). The IO, also known as influence operation in some Army doctrine, includes a collection of information about an adversary as well as dissemination of propaganda in pursuit of a competitive advantage over an opponent (RAND 2018). IO doctrinally has many core

capabilities such as public affairs operations, military information support operations (MISO), combat camera, soldier and leader engagement, civil affairs operations, public and cultural considerations, operations security (OPSEC), and military deception. (HQDA 2013, 1-1).

Information-Related Capability. A tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions. Also called IRC. (Approved for inclusion in JP 1-02.) Designated information-related capabilities that support IIA and its lines of effort typically include but are not limited to, public affairs operations, military information support operations (MISO), combat camera, soldier and leader engagement, civil affairs operations, civil and cultural considerations, operations security (OPSEC), and military deception. Additionally, other capabilities the commander may allocate—components of cyber electromagnetic activities, special technical operations, presence, posture and profile, physical attack, and physical security—are capabilities not solely designed to inform or influence, but may help in achieving effects and mission objectives. Success depends on commanders and staffs effectively employing all available operational assets to best shape the information environment. Figure-2 illustrates the IRC.

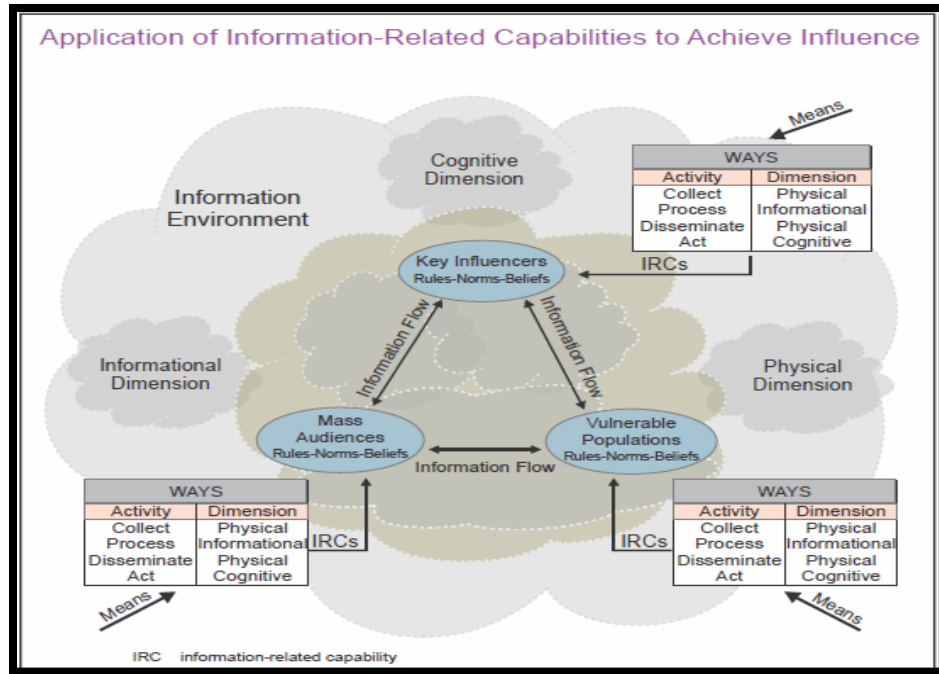


Figure 2. Information Related Capabilities

Source: CJCS 2012, I-7.

Information Warfare (IW). IO is conducted during the time of crisis or conflict to achieve or promote specific objectives over a specific adversary, or adversaries and it is also called IW. IW is any action to deny, exploit, corrupt or destroy the enemy's information and its functions; protecting ourselves against those actions and exploiting our military information functions.

Conflict between two or more states in information space with the aim of causing damage to information systems, processes and resources, critically essential and other structures, subverting the political, economic, and social systems, mass psychological work on the population to destabilize society and the state, and coercing the government to take decisions in the interests of the opposing side (Giles 2012). (From Section 1,

Fundamental Terms and Definitions of “Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space,” a document presented at an information security conference in Berlin on 14 December 2011 and released in text form on 22 December 2011)

Influence. The act or power to produce a desired outcome or end on a target audience (CJCS 2012, I-3).

Influence Operations. Operations focused on affecting the perceptions and behaviors of leaders, groups, or entire populations. Influence operations employ capabilities to affect behaviors, protect operations, communicate the commander’s intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary’s decision cycle, which aligns with the commander’s objectives. The military capabilities of influence operations are psychological operations, military deception, operations security, counterintelligence operations, counterpropaganda operations, and public affairs operations. Public affairs, while a component of influence operations, is predicated on its ability to project truthful information to a variety of audiences (HQDA 1996, 1-13)

Difference between Information Warfare and IO. Many military theorists contend that IW is what the military does when IO fails. That is one difference, but there are also subtleties between these two warfare areas as well. The difference between these two terms is that IW contains six elements and is mostly involved with the conduct of operations during actual combat, while IO, on the other hand, includes these six capabilities and two sometimes integrated or related activities. IO is broader than IW and is intended to be conducted as a strategic campaign throughout the full spectrum of

conflict from peace to war and back to peace. Therefore, IO is much more comprehensive than IW, and it is in IO that the full integration across government agencies and with private industry must occur (Armistead 2004, 12). Figure 3 explains the IO relationship over time

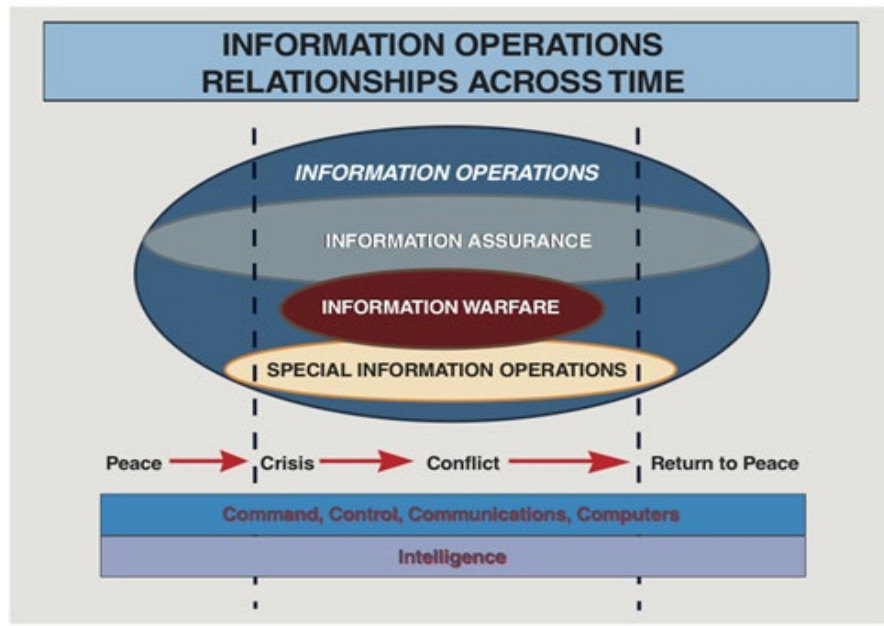


Figure 3. IO Relationship over Time

Source: IT Law Wiki 2019.

Electronic Warfare (EW). EW is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (CJCS 2012, 1). EW consists of three divisions: Electronic Counter Measure or Electronic Attack (ECM/EA), Electronic Counter Counter-measure or Electronic

Protection (ECCM/EP), and Electronic Support Measure (ESM/ES). Figure 4 explains the method of EW in integrated IO.

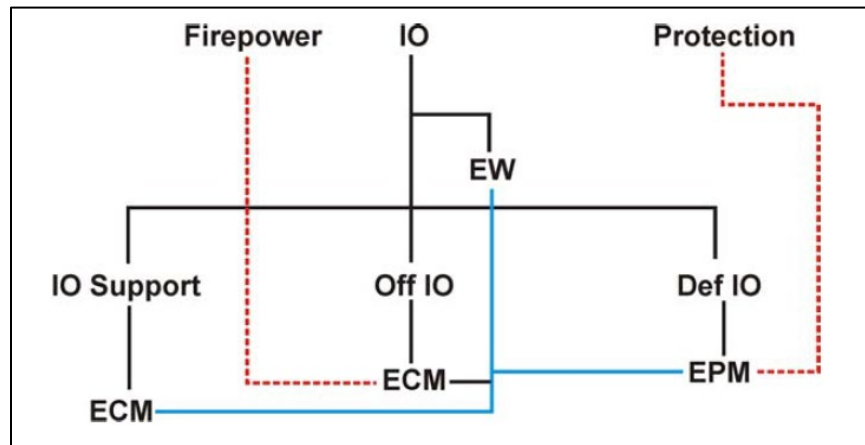


Figure 4. EW in Integrated IO

Source: Canada DND 2018, 11.

Message. A narrowly focused communication directed at a specific audience to support a specific theme (CJCS 2012)

Operations Security (OPSEC). OPSEC is a process that identifies critical information to determine if adversary intelligence systems can observe friendly actions, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information (CJCS 2012, II-12).

Psychological Operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and

individuals in a manner favorable to the originator's objectives. Psychological Operations is also called Military Information Support Operations (CJCS 2006b).

Recruitment. To seek out, evaluate, obtain a commitment from, place, and orient new employees to fill positions required for the successful conduct of the work of an organization (Andrews 1988).

Signal Intelligence (SIGINT). The generic term SIGINT is used to describe communications intelligence (COMINT) and electronic intelligence (ELINT) when there is no requirement to differentiate between these two types of intelligence. Technical and intelligence information derived from EM non-communications transmission (e.g., radar, navigational aids, jamming transmissions) by other than intended recipients are known as ELINT. Technical and intelligence information derived from EM communications and communications systems (e.g., Morse, voice, teleprinter, facsimile) by other than intended recipients are known as COMINT (Canada DND 2018, 18).

Scope

This study will be limited to the scope of establishing the correlation between the different well-established doctrines of few of the armies. The assessment of future battlefield by other nations or armies in the domain of IO and the development need of respective nations' armies will be out of the purview of this research.

No efforts were made to collect data physically from outside CGSC and CARL except some interview over the telephone. The data collection efforts were limited to web-based documents, and documents received from CGSOC. The author also did not conduct any survey involved with the IO of different armies. The research committee gave explicit guidance in directing the research in the desired path.

Limitations

This study will be limited to the scope of IO relating to organization and doctrine, leaving aside the training, material, leader development, and education, Personnel, facilities, and policy. Besides, this research is limited in that only English language sources will be examined. No translation of primary source material is available for the production of this thesis. Also, any study or physical interview outside Fort Leavenworth will not be possible to include in the research. Financial implications and IO technical architectures are kept beyond the purview of this research.

Delimitations

Many of the U.S. Department of Defense's IO existing tactics, techniques, and procedures are classified at the SECRET level or above. The majority of the detailed analysis of the technical aspects of adversary influence techniques is also currently classified. This thesis will only address that information which is readily available in the open source arenas and not currently classified by the United States Government. This will be the same for gathering information from the other armies as well. Recommendations as to potential future tactics, techniques, and procedures will be generalized and not go into such detail, as they could constitute an operational plan.

Author's Qualifications and Justification

The researcher was commissioned as an infantry officer and had abundant opportunity to be deployed in the operational environment of Bangladesh. Right after his commission, he was posted the Chittagong Hill Tracts for three years (2007-2009), the area where predominantly the Bangladesh Army has fought Counter Insurgency

Operation (CIO) for many decades. There the author had the opportunity to conduct operations and closely work in the information environment of the operational area. He served as an Intelligence Officer, Adjutant, Quartermaster, and Company Commander in different camps where the military invariably conducted operation related different fields of IO to influence the local population who were working against the Bangladeshi Government.

Later in 2010, the author had the opportunity to serve in an Infantry Division Headquarter (HQ) as a grade three staff Officer-Intelligence in the counter Insurgency branch. There he had the opportunity to closely work with other departments (Psychological operation branch, the media branch, and operation branch). In fact, working in the Division HQ gave great exposure to the information environment and IRC of Bangladesh Army. After his Junior Command and Staff College (JCSC), he had the opportunity to perform as an instructor in the School of Infantry and tactics. As an instructor, he had to study a lot about the IRC of the Bangladesh Army to impart knowledge to students. He was also closely associated with the development of the new sniper and mechanized infantry doctrine for the Army.

The researcher's last posting was in the Bangladesh Military Academy (BMA) as an Instructor of the cadets. During his stay, BMA undertook a paradigm shift in the conduct of training for the cadets. BMA adopted the model of the United States Military Academy (USMA) and extended its training duration from two years to four years. His close association with the restructuring and remodeling of the training system of the academy gave a significant exposure to the aspects of organizational restructure and reform.

Last year he finished his staff college from Defence Services Command and Staff College (DSCSC) in Bangladesh. In the curriculum of Staff College, there were significant study modules related to IO (Media package, psychological operations, civil-military relationship, cyber operation by British staff college team, Counter Insurgency operation by Srilankan Army team). Apart from his professional experience, he has also participated in Junior Command and Staff College in Aldershot Canada. There he had the opportunity to learn about different aspects of information and influence operation from North Atlantic Treaty Organization (NATO) perspective.

Summary

In this chapter, the author explained the purposes of the thesis clearly. In accordance with the purpose, the author listed primary and secondary research questions, which were answered during the process of this research. Side by side, few assumptions, limitations, and delimitations are also incorporated into the later part of this chapter. A critical portion of this chapter is that the author standardized the definitions, which will help the reader to understand the overall context of this thesis. The next chapter highlights essential findings from different literature concerning the institutionalizing IO.

Conclusions

The IO is the new magical instrument, which enables a military force to win a war or avoid a confrontation through information superiority and without physical fighting on the ground. According to the famous historian and military theorist, Captain Sir Basil Liddell Hart in his book, 'Thoughts on War', "The real target in war is the mind of the enemy commander, not the bodies of his troops." With the proliferation of IT, the IO is

regarded today as an integral part of warfare. The media and the cyber is conceived as a weapon. The idea is conceived not just theoretically but in every conflicting situation. Most of the armies are now establishing a separate body to deal with media, cyber as a whole IO.

The importance of IO cannot be overstated. The IO does not confine to the boundary of a nation, or with only its adversaries; instead, it spans over the entirety of the global affairs. Now there are ideas like 'Facebook War Room.' that indicates the spectrum of IO is much more than what can be imagined. IO has evaporated the thin line between the combatants and non-combatants. The information environment is ever changing. The art of information confrontation must be practiced continuously, refined over time, and tailored to specific audiences. Therefore, the Bangladesh Army should institutionalize the IO as soon as possible.

CHAPTER 2

LITERATURE REVIEW

Chapter Introduction

There is a vast reservoir of primary and secondary sources on IO. IO has been a prevalent topic among the military think tanks in the last couple of decades. Since future warfare is going to be in the realm of the information domain, much research is carried out on IO in the recent past. However, progress in the militaries of the Southeast Asia region is not very noteworthy. There are also many unofficial documents. Non-Civilian scholars also carry out many write-ups in journals and research. Documents from outside the military are likely to provide a different perspective on the subject matter and lead to a more suitable solution. Moreover, those documents also provide a very in-depth analysis of the subject matter. Access to the U.S. Army doctrines was readily available. However, many of the army doctrines were classified. Therefore, there was limited access availability. Another significant source of the documents was the internet or the Fort Leavenworth Combined Arms Research Library, where there was a considerable amount of related sources.

While reviewing the literature, the resources are categorized into a different segment. Those are international military doctrinal publications on IO, Bangladesh army publications, Bangladesh army research works, international publications, journal articles, books, and international research papers. In the following paragraph, all accessible literature will be reviewed as per those categories. There was no research found on the establishment of IO architecture of the Bangladesh Army. However, there

are many articles, which describe different fields of IO. The following literature was found on IO from different sources.

International Military Doctrines Published on IO

U.S. Army. There is sufficient amount of publications in the U.S. Army. The Department of Defense (DOD), the Chairman of the Joint Chiefs of Staff and the Department of the Army publishes those. Those departments publish manuals, articles, regulations, and others for the conduct of IO.

As per most of the U.S. publications, while IO is applied during both peacetime and conflict, IW tends to be applied during conflict or crisis. This is because the techniques of IW are assumed to be the employment of coercive force and will usually be perceived as a hostile act. Since the borderline between IO and IW was not well defined, IW was deleted from the 2006 version of JP 3-13. The three-interconnected-dimensional framework was for Cyber Operations, U.S. Army Communications-Electronics Research, Development propagated EW, and IO, and Engineering Center, Intelligence and Information Warfare Directorate (CERDEC I2WD). Which states, “We conclude that this will come about if the cyber-warfare and EW elements are consolidated because their technologies, infrastructure, operational use, and personnel training are merging and they will benefit from common doctrines.” (Porche et al. 2013, 46). EW is thereby considered as an element within cyber-attack as Cyber-war and EW are both means of using Electro-Magnetic System (EMS) technology to attack and defend against the enemy. Increasingly their means are digitally enabled.

Field Manual 3-0, Operations. FM-3.0 is the Army’s most recent publication published in October 2017. This manual is published to prepare the U.S. military for

large-scale combat operations in highly contested, lethal environments where enemies employ potent long-range fires and other capabilities. The manual is a capstone doctrine which addresses the conduct of all major operation. This manual addresses the conduct of IO, and its integration in all kinds of major operation. There is very detailed information on the plans, preparation, and execution of IO. The manual identifies some related activities, such as public affairs and civil-military operations for units to synchronize with IO. According to the pamphlet, the Army conducts operations across multiple domains and the information environment. Currently, all Army operations are multi-domain operations, and all battles are multi-domain battles. In multi-domain operation, the information domain is integrated as an essential and inseparable part, and it includes IO as an integral part.

According to the FM 3.0, the key considerations for operating in multiple domains include mission command, reconnaissance in depth, mobility, cross-domain fires, tempo and convergence of effects, protection, sustainment, and IO. Chapter 2 describes the theatre IO group. It describes that the Army provides IO support to the theater army through elements dedicated to helping theater organizations analyze and operate within an increasingly complex information environment. Chapter 2 also discusses the importance of information in any OE. In this chapter, there is a detailed guideline for the conduct of IO. It provides guidance on IO for both offensive and defensive actions. Several other chapters also contain details guidelines regarding the conduct of IO.

Field Manual 3-13, Information Operations. This manual is the prime doctrine, which delineates the guideline about all the tactics, techniques, and procedures for the

conduct of IO. The pamphlet was published in the year 2013. In the Preface, the manual states provide doctrinal guidance and directions for conducting IIA and discusses the importance of information in operational environments. It also guides the staff to conduct IIA to achieve the desired effects that support the commander's intent and objectives. It states that the principal audience for FM 3-13 is commanders and staffs at all echelons of command, Army civilians, and government contractors. As it is very evident from the name of the book that the book is much more detailed for the conduct of IO than FM 3.0.

There are a total of eight chapters in this pamphlet. Those are: construct of inform and influence activities, aspects of inform and influence activities, capabilities of inform and influence activities, roles, responsibilities, and organizations of inform and influence activities, inform and influence activities integration, targeting and inform and influence activities, assessment of inform and influence activities, and soldier and leader engagement of inform and influence activities.

The first chapter in the pamphlet defines inform and influence activities. It also discusses each action in the definition and considerations of IIA. Chapter two discusses the aspects of IIA. Then it discusses the information environment as commanders use IIA to accomplish their mission objectives. The next chapter describes the designated information-related capabilities and organic capabilities integrated throughout inform and influence activities. Chapter four discusses the role of different staffs related to IO and describes the ways to integrate information-related activities into the military decision-making process (MDMP).

Worth mentioning, the pamphlet dedicates one chapter to providing guidelines for the staffs to integrate IO in the MDMP. The fifth chapter discusses the MDMP from an

IIA perspective. It describes the action of the IO staff in every step of the MDMP. It describes the Running Estimate and the Military Decision making Process through different matrix and chart. Chapter 6 mentions that for Targeting and IIA use the same targeting process and formats as FM 3-60. In this chapter, the pamphlet describes the measure of performance development. Chapter 8 has the most significance from the perspective of the Bangladesh Army since it describes the soldier and leader engagement, which is very closely associated with the framework for IO.

The pamphlet FM 3-13, Information Operations, published in November 2013 is designed for the conduct of IO in large-scale combat operation environment, which is most applicable for the division and corps-level staff planners and commanders. However, it might function at the tactical level, but the manual is not designed for the tactical commander and staffs below brigade.

Joint Publication 3-13, Joint Doctrine for Information Operations. The manual published in November 2012 provides joint doctrine for the planning, preparation, execution, and assessment of IO across the range of military operations. This is a similar doctrine as FM 3-13; however, it describes everything from a joint force perspective. From this doctrine, the Army has derived its portion of IO procedures and guidelines. It is a comprehensive doctrine from the perspective of the joint concepts of IO and providing IO concepts for influencing the target audience. It endorses the significance of incorporating IO in all kind of joint operations. This doctrine has five chapters. This pamphlet describes the procedure for conducting multinational IO as well. It is applicable for IO at echelons above corps or working in the joint environment.

Joint Publication 3-13.1 Electronic Warfare. This is another joint doctrine, which is closely associated with the IO and discusses EW planning, preparation, execution, and assessment in support of joint operations across the range of military operations. Being the first U.S. Army EW doctrinal publication, the pamphlet is as timely as it is essential. It explains the U.S. Army's EW current strategy into cyberspace and electromagnetic (EM) environment. This manual particularly provides insight and guidance to the army commanders and their staffs on how the EM spectrum can impact their operations. The different facets of EW are described in functional point of view in support of full-spectrum operations and provides a baseline for common understanding. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and prescribes joint doctrine for operations and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans.

UK and NATO Doctrines. The UK terms the IO as Influence Operation. The UK definition is very much in line with the C2W tradition, targeting only adversaries or potential adversaries: 'Coordinated actions are undertaken to influence an adversary through affecting his information, information-based processes, and systems while protecting one's decision-makers and decision-making processes' (UK MOD 2002).

Joint Warfare Publication 3-80, Information operation. This pamphlet was published in June 2002 for the British Army. This publication provides understanding, information, and guidance to all involved in the planning and execution of IO on joint and single Service operation. However, the doctrine is primarily for the Joint Task Force Commander (JTFC) and those of his staffs with IO responsibilities. This pamphlet

addresses the planning and conduct of IO primarily at the operational level. The context in the doctrine is a higher-level information campaign, ways to achieve coherence between IO and Information campaign. It also discusses the IO in detail, which describes its aim, and explains how to integrate IO with the campaign plan. It has a few chapters, which provide a deliberate guideline on the planning and conduct of IO in coordination with JTFHQ.

Allied Joint Doctrine for Information Operations, AJP-3.10. NATO military IO doctrine is intended primarily for use by NATO forces and provides a useful framework for operations conducted by a coalition of NATO partners, non-NATO nations and other organizations. This doctrine, therefore, provides a common baseline for achieving IO interoperability, rather than trying to encompass each nation's Info Ops approach. This pamphlet acknowledges the primacy of civil/political direction on information issues and that the policy and subordinate doctrine applies to the military lever of power only. The joint doctrine is primarily focused on the operational level. The content of the book includes: principles of IO, and highlights those particular IO considerations relevant to the conduct of operations, such as the sensitivity to political factors, and the role of non-military entities and emerging technological capabilities in the information environment, both within and external to NATO.

Canadian Army Doctrines. There is a good number of Canadian doctrines, which talk about IO. There are significant alignment and similarity between the Canadian doctrines and the U.S. doctrines. However, the most prominent doctrine dealing with the IO was reviewed for the research. Some of those doctrines are described below.

Canadian Forces Joint Publication 03.10–Information Operations. It is the doctrine, which is intended for the Canadian forces to conduct IO. Canadian doctrine, dated though extant, defines IO as actions taken in support of political and military objectives, which influence decision makers by affecting other's information while exploiting and protecting one's information (Canada DND 1998). The Canadian Army doctrine of EW is although comprehensive and rich in functionality, is instead tends to be biased towards U.S. doctrine, and hence provides limited scopes for a different point of view. In the Canadian Army's Land Operations IO are defined as "coordinated actions to create desired effects on the will, understanding and capability of adversaries, potential adversaries and other approved parties in support of overall objectives by affecting their information, information-based processes, and systems while exploiting and protecting one's own

Land Forces Information Operations B-GL-300-005. This doctrine manual describes a multidimensional concept used by the Army to achieve success across the continuum of operations. This doctrine is designed for the Canadian land forces to perform IO. The Canadian Army has accepted IO as one of the essential combat function. Therefore, it is essential to integrate this combat function with all others to maximize combat power. The pamphlet describes that the elements of IO are not new; some have been present in warfare for thousands of years. However, with the invention of new technology, its importance has become more significant than ever before. The aim of IO is information superiority gained by the optimum exploitation of information and by denying the same capability to any adversary.

Australian Doctrine. Information Activities-ADFP 3.13.1-Information Operations Procedures is the pamphlet which is designed for the Australian Army to conduct IO. Australian Defence Doctrine Publications (ADDP)-3.13, Information Activities is designed for the joint forces to operate in Information Environment. The prime aim of this pamphlet is to guide the planning and conduct of Information Activities in the joint and multinational environments for the Australian Army. According to the doctrine Information activities are defined as the integration, synchronization, and coordination of two or more IRC that generate and sustain a targeted information advantage. Defense conducts information activities at all levels in a whole-of-government context consistent with Australian Government guidance. The Australian Army, however, seems to be moving away from traditional IO constructs: ‘Actions conducted to influence target audiences in order to achieve understanding, acceptance, and support of our actions and aims, and to diminish the quality and speed of the adversary’s decision making, while maintaining our own, to achieve decision superiority’ (Nicholas 2008).

Land Warfare Doctrine 2-0, Intelligence. This doctrine was published in 2018. This is a very recent doctrine, which also has many guidelines regarding the IO of the Australian Army. The pamphlet states that: to ensure that the Army remains a dominant land force, a focused intelligence enterprise that facilitates situational understanding and supports the commander in decision-making is required. Land Warfare Doctrine LWD 3-8-6, Civil-Military Cooperation also describes the IO for the Australian Army.

Russian Doctrine. Access to Russian doctrine was challenging due to the language barrier. However, there were many articles, which mentioned many aspects of the Russian doctrine and talks about the structure of the Russian IO. Worth mentioning one

article was “Russia’s Improved IO: From Georgia to Crimea.” The article, “Russia’s Improved IO: From Georgia to Crimea” describes Russian series of military reforms in the IO model resulting from the 2008 conflict with Georgia. After a successful evolution, later Russia used IO more effectively in Crimea. Russia’s continued refinement of its IO may keep it ahead of the United States. According to the article, (Igor Panarin, an influential scholar and a well-regarded Russian IW expert) outlined the basic instruments involved in the larger information struggle including propaganda (black, gray, and white); intelligence (specifically information collection); analysis (media monitoring and situation analysis); organization (coordinating and steering channels and influencing media to shape the opinion of politicians and mass media); and other combined channels (Darczewska 2014). In the article, the writer described the implication of the Russian IO model involved in Georgia, Ukraine, and Crimea. The model involves information-technical and information psychological operations. Russia failing to win IO campaign against Georgia evolved and applied their corrected doctrine against Ukraine where they were overwhelmingly successful. This is a useful article to understand the Russian way of conducting IO.

Bangladesh Army Publications

Operations of War. The warfighting function is termed as Battlefield Operating System’ (BOS) in the Bangladesh Army doctrine. Out of eleven BOS in the army land doctrine ‘Operations of War,’ three are information based: EW, intelligence, and deception. Those three directly links with the conduct of the IO. The pamphlet underlines the importance of EW stated, as “EW is an essential element of combat power.” All these three elements consist of an essential element to protect C3. Intelligence delineates, “By

knowing the enemy and forecasting what he is likely to do, intelligence not only saves lives but also enables the best use to be made of the forces available.” The pamphlet, while underlying the importance of deception, suggests, “The deception story is false information provided to the enemy to lead him to an incorrect appreciation of friendly forces and plans.” Those all those BOS essentially ensures the IO in the OE.

Intelligence and Electronic Warfare. This is another pamphlet, which delineates the instructions for the Bangladesh Army to deal with “Intelligence and EW.” The doctrinal pamphlet elaborately dealing with ‘Intelligence and EW’ duly notes: “In a world of sovereign nations, information is a prime element of national power. Intelligence, which is best defined as evaluated information, is the vital and often pivotal foundation for national decisions.” In one of the chapters of the pamphlet elaborately addresses intelligence aspects in regards to EW, IO, psychological operation, deception, and denial operation.

Domestic Research Work and Journal Articles

Intellectual discourses on C2W, IW, EW, and Cyberwar/ Net-Centric war, or currently termed as IO, are a handful. In his thesis ‘The Information Age: Imperatives for Bangladesh Armed Forces’, Group Captain Moueenuddin Ahmed, ndc, psc stressed to find the need and type of restructuring of the organization and a doctrinal guideline commensuration with the information age. The research titled “Information Warfare - its relevance and viability in Bangladesh” by Brigadier General Akbar, ndc, psc, identifies some challenges in the issue of IW. The challenges included scopes for better understanding, developing a strategy for deterring digital information attacks, developing

a means of providing a warning for attacks and ways of successfully defending against attacks that do occur. Few of the other documents related to IO was also reviewed:

Dilara Zahid (2007) “Impact of Cultural Globalization on the Upper-Class Youth in Dhaka City” has mentioned the effect of cultural globalization. She argues that due to the introduction of cable TV and internet the younger generation of the country has become reckless. The research was conducted only on the upper-class youths particularly in Gulsan, Baridhara and Mirpur area as the ICT did not spread to the other strata of the society till then.

Sagarmay Deb (2014) of Central Queensland University, in his article, “Information Technology, Its Impact on Society and Its Future” argues that the benefits from IT far outweigh the negative aspects of it. He, however, mentioned a few negative sides like loss of privacy, unauthorized access data, hacking, etc.

Lieutenant Colonel Md Shahidul Islam (2013) in, “A View of Command, Control, Communications, Computer and Intelligence (C4I) Architecture in Bangladesh Army” presents the requirement of establishing an ideal C4I Centre in Bangladesh Army with the existing resources taking examples from a world perspective. This presentation suggested a roadmap towards establishing C4I architecture in Bangladesh Army along with the implementation plan. This paper also highlighted the lacunas and shortfall of the implementation plan.

Major Shafiul Azam Parvez (2013) in, “Future Battle Field Trends and a View of Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR) Architecture for Bangladesh Army” visualizes the future battlefield trends and explains some of the examples. The benefits of C4ISR architecture

from the world perspective are also highlighted. It describes ICT enhancement initiative and integration of that for Bangladesh Army. The paper did not portrait any feasible C4ISR architecture for the Bangladesh Army.

Lieutenant Colonel Abu Sayeed Mohammad Ali (2010) wrote the “Trends of Future Warfare and Options Available.” The author highlighted that technological inventions are making the present standing obsolete and tomorrow becoming a reality. The paper also visualized future warfare scenario with recent changes and inventions.

International Publications, Journal Articles, and Books works

The 21st Century Army – Strategies for Future by Lt Gen Gautam Banerjee, Manas Publications, New Delhi, India (2012). The author in his book captured most of the contemporary and emerging trends of warfare of the 21st century. He covered leadership, IW, combined arms operations, insurgency and economics of defense in his book from the perspective of India. In Chapter 2, the topic of IW was discussed in four parts: background of IW, concept, conduct, and status of IW capabilities in other countries origin. In the end, the author focused on military IW in India. The book, although rich in theory, precludes the application part of defensive IW. The IW threat patterns can be deduced in broad terms leaving enough scopes for further delving on the subject matter through the lens of Bangladesh.

Information Warfare - Separating Hype from Reality by Edwin Leigh Armistead, Manas Publications, New Delhi, India (2010). The author, in his book, opined that the potential and magnitude of IO is going to be more powerful and significant in the coming future. The author deliberated that leaders focus on technology must expand to include IO’s physical interconnectivity, content and cognitive dimensions, especially perception

management. Lastly, the author reiterated that the success of any information campaign would largely hinge upon collective inter-agency structure and interconnectivity of information nodes at the strategic level. The military-strategic and operational level doctrine, employment, functional details covering threats and vulnerabilities are left aside within the purview of the discourse.

Information Operations Planning by Patrick D. Allen, Artech House, Norwood MA, USA (2007). Dr. Allen has categorized the whole write up into three significant part: IO and its role in security and conflict, the IO planning process and tools, and lastly describe the future of IO planning. The author, while elaborating new campaign planning methods provides a comprehensive overview of the planning process that integrates traditional planning methods and advanced concepts. He underlined the increasing importance of IO in military operations and dwelled on detail characteristics of IO planning. While doing so, Allen defines the first principles of planning, describes techniques to represent and simulate plans explicitly, and illustrates the methods with screenshots of actual planning tools.

Information Warfare: Corporate Attack and Defence in a Digital World by Hutchinson and Warren, Butterworth-Heinemann, Oxford, UK (2002). The book is a methodical compilation of ‘Computer Weekly Professional Series’ which illustrated the uses and abuses of information and its power in the civilian paradigm of IW keeping aside conventional military and national security issues. The book is written mainly from the information attacker’s point of view, initially dealing with fundamental principles of IW followed by intelligence function, attack techniques, and security-oriented defense systems and proposes viable risk analysis model for managerial implications. Although

military aspects of IW is precluded, it offers a different outlook of IW in the academic and technical perspective altogether.

Information Warfare Principles and Operations by Edward Waltz, Artech House, Norwood MA, USA (1998). Waltz describes the basis for information-based warfare (IBW), beginning with the information sciences that define information, and technologies to create knowledge from data. He also explains the means to apply these technologies to achieve dominant battle-space awareness and knowledge, the goal of IBW. Part II of his book, at first, describes IW policy, strategy, and tactics; then it deals with IO that attacks opponents' information systems and defends a nation's systems. An overview of the core, enabling, and emerging technologies in this area are provided in conclusion.

Information Warfare as the Hobbesian Concept of Modern Times. The Principles, Techniques, and Tools of Russian IO in the Donbass by Holger Mölder & Vladimir Sazonov published in 2018 is a paper, which explains the methods of Russian IO in Ukraine. The analysis of the case study is built on narrative inquiry, which is based on interviews with Ukrainian experts and available open access sources. The paper explains the Hobbesian concept of warfare and relates it to Russian IO method. Russia has been among the pioneers of contemporary IW and actively started to use different forms of information campaigns in pursuit of its political goals. The paper states that Russia's information tools for convincing an audience are rich and varied and include historical myths, narratives, and symbols. Russia effectively uses the 'data deluge method' 80 to influence people with sometimes controversial information. The purpose is to convince or disorientate the target audience. The paper is beneficial to understand the mechanism of Russian IO in Ukraine.

International Research Papers

There are several research carried out at the CGSC previously by many U.S. students over IO. However, most related four research papers were reviewed for this thesis. Those research works were very closely associated with the research topic.

How to organize the headquarters for IO at the brigade and division, by Maj Mark E. Brock, U.S. Army. This research carried out in 1996 was in the scenario when the U.S. army was getting involved in the counter-insurgency operation in Iraq and Afghanistan. The Army was transforming into a modular force, and the issue of IO became the business of the leaders at all levels. Then U.S. Army doctrine for the IO was not very well organized and units were experimenting with various methods of incorporating staff officers and noncommissioned officers into the planning process for IO. Therefore, this research was an endeavor to address the issue. According to the researcher, some units are approaching the problem of integrating IO into operations with the use of an Effects Coordination Cell. Other units have Information. Considerations of available resources, the commander's intent and numerous other factors lead to the conclusion that the Effects Coordination Cell is the best way for these HQs to organize.

Influencing tomorrow: a study of emerging influence techniques and their relevance to United States information operations by Maj John M. Boehnert, U.S. ARMY. This research was carried out in the year 2015. The researcher mentions that the rapidly changing information environment and media landscape present both challenges and opportunities for United States IO professionals. The thesis conducts a case study from a timeline of 2001-2015. It mentions different international terrorist organizations using IO to disrupt global harmony. It also talks about Russia and its use of IO to support

its offensive strategy. The researcher mentioned that the U.S. military could extract a great deal of knowledge from those instances.

Overcoming IO legal limitations in support of domestic operations by Major Peter L. Elstad, USA. In this thesis, the researcher talks about the legal aspects of IO and the challenges from the perspective of the domestic operation. The author mentions that the current U.S. Title 10 restrictions limit the use of certain assets (e.g. Psychological Operations PSYOP assets) against the U.S. domestic population during times of crisis. However, according to the new FM 3-0, information is an element of combat power. This thesis attempts to answer the question, —can army information tasks be legally and doctrinally applied in domestic operations. The study of this article unleashed another new dimension for the research.

Preparing the American soldier in a brigade combat team to conduct IO in the contemporary operational environment by Maj Brian Thomas Beckno, USA. This research paper addresses the issue of the preparation of the tactical level leaders and soldiers for conduction IO in a modular framework. The research explains the IO from the perspective of operations in Iraq, Afghanistan, from a counterinsurgency operation point of view. The author talks about the requirements for conducting IO for U.S. Army leaders and soldiers in a BCT framework. The researcher mentions many skills; these skills are intercultural communication, language, negotiation, and media awareness. The applications are laws of war, rules of engagement, ethics, and morality, and commander's intent. The researcher's work also mentions the institutional training for the members of BCT for operating on a tactical level.

Summary

There are many sources, which describe the technique and procedures to conduct IO and describes the architecture for it. Most of the western doctrines have similarities with the U.S. doctrines in basic principles and theory. However, the terminology is different for different armies such as Influence Operation (UK), Information Activities (Australia). There are doctrines published for different level, mostly tactical and operational. Those documents vary from a wide range of joint publication to instructions of recent operations at the tactical level. The U.S. Army FM provides the most comprehensive and detailed guideline and structure for the conduct of IO. It provides the commander and his staff with planning considerations and ways of execution for the organization at a different level. The entire pamphlet in common describes that conduct of IO is a complicated affair and needs proper integration at the appropriate level. Therefore, synchronization is a complicated affair.

Other non-military publications also provided a good insight into the subject matter from its application point of view in different operation. Publications related to the conduct of IO from the Russian perspective added a great value since Russia has been successfully using IO for its military operations. The concept of IO has evolved and got matured in the last two decades from a way of attacking an enemy's command, control, and communications systems to the current concept of integrated tools a commander may employ to inform or influence local and regional friendly neutral, and adversarial audiences in favor of military operations (Elstad 1988) . The purpose of this chapter is to provide an analysis of available literature to determine an architecture for the Bangladesh Army. The study was mostly confined to the research of different army doctrine.

Therefore, through compare and contrast pick up the best architecture for the Bangladesh Army, which is now performing many global responsibilities through United Nations (UN) mission.

CHAPTER 3

RESEARCH METHODOLOGY

Chapter Introduction

The Government of Bangladesh (GoB) has formulated the “Vision-2021” and the concept of ‘Digital Bangladesh’ in 2007 as a stepping stone to lead the nation to a middle-income country by the year 2021 (GoB 2007). The country is already on the verge of reaching the landmark goal. In confirmation of the concept, the Armed Forces concurrently developed ‘Forces Goal-2030’ to address the long felt need for modernization and growth (Which remains classified). Appropriate defensive measures against cyber-attacks in computer network systems and electronic-attacks against radio communication in the electromagnetic spectrum (EMS) are some requirement that needs to be incorporated for all the armies. Therefore, Bangladesh Army army raised IT Support Organizations. To enhance it further, Bangladesh Army needs a viable IO architecture.

The primary question of the thesis is- What should be the appropriate architecture of IO for the Bangladesh Army to conform to the future battlespace trends related to information environment? The research will provide a basis for recommendations to solve the problem. The purpose of this study is to find out a viable architecture for the Bangladesh Army to conduct the IO to protect its information environment from the adversary. A qualitative research methodology is used for this research to answer this study’s primary and secondary research questions. The research project will adopt a qualitative method. The study will be carried out based on both primary and secondary sources. Qualitative content analysis of the existing literature will be carried out,

particularly on IO in general and information security affecting Bangladesh Army in particular. The researcher will not conduct any survey since it will be challenging to access significant expert group present in the Bangladesh Army.

Research Methodology

The purpose of this section is to describe the research methodology used for this thesis. First, the scope of the thesis required reduction. The field of study IO deals with is very vast and wide. The IO lines of effort typically include but are not limited to, public affairs operations, military information support operations (MISO), combat camera, soldier and leader engagement, civil affairs operations, civil and cultural considerations, operations security (OPSEC), and military deception (HQDA 2013, 1-1). Moreover, other capabilities the commander may allocate components of cyber electromagnetic activities, special technical operations, presence, posture and profile, physical attack, and physical security, capabilities not solely designed to inform or influence, but may help in achieving effects and mission objectives. Each of these core competencies has its own set of doctrines. Except for PSYOPS, the others are governed by regulation. However, the law regulates the PSYOPS. These capabilities have separate proponents for doctrinal development and regulation. In this thesis, the researcher will not describe in details how each of the fields will be organized for the Bangladesh Army. Instead, it will suggest an organization for IO to function with the existing institution that deals with information and intelligence.

The research project adopted a descriptive method. The study carried out is based on both primary and secondary sources. The research was carried out through qualitative content analysis of the existing literature, research papers, peer-reviewed articles and

particularly, the unclassified doctrinal publication of U.S., U.K., Canada, Australian, and Russia related to IO. The method is a combination of analysis of other related research papers, doctrinal publications, and document review. The gathered information and data are critically evaluated, cross-checked, and rigorously synthesized. The thesis will draw a conclusion and recommendation for the Bangladesh Army depending on the analysis of a wide range of information, detailed analysis of the doctrines of different countries. The analysis of the doctrines will be the prime field of concern, and only a few developed countries, as mentioned in the previous chapter will be used for this analysis.

This thesis is not going to analyze any of the core capabilities related to IRC; instead, the research is going to focus on the doctrines and organizations of the different armies. The structure through which all the modern armies are operating will be analyzed. This thesis attempts to determine a suitable structure for the Bangladesh Army based on the analysis of the well-established doctrine of US, UK, Canada, and the Russian Army. The primary and secondary questions are likely to provide the path, and an answer to the problem, how Bangladesh Army should establish a well-structured IO architecture? Since this research is focused on establishing an IO model, the research will use the publication and doctrines of the Armies mentioned above. The character of the problem demands qualitative research. It is researched similar to a case study, and the study was based on both primary and secondary sources. The gathered information will be critically evaluated, cross-checked, and rigorously synthesized. The research will deal with two kinds of data, which are:

Primary Data

As a primary source, information was gathered from the personal experiences of the officers of Bangladesh Armed Forces who are exposed to IT matter through their research works. Senior officers of Bangladesh Armed Forces were also consulted for their expert opinion on the operational aspect of IO. Discussion between the author and the officers of Army Headquarters (AHQ), Division and Brigades HQ were the primary source of information for this research.

Secondary Data

Secondary data of the related issues were collected from various published papers and presentations. The researcher used relevant content analysis to critically, and objectively review published and printed facts, opinions, and observations. Various papers and publications had been collected from the internet. This helped to formulate an idea regarding the answers to the questions under study. Figure 5 shows the operationalization diagram:

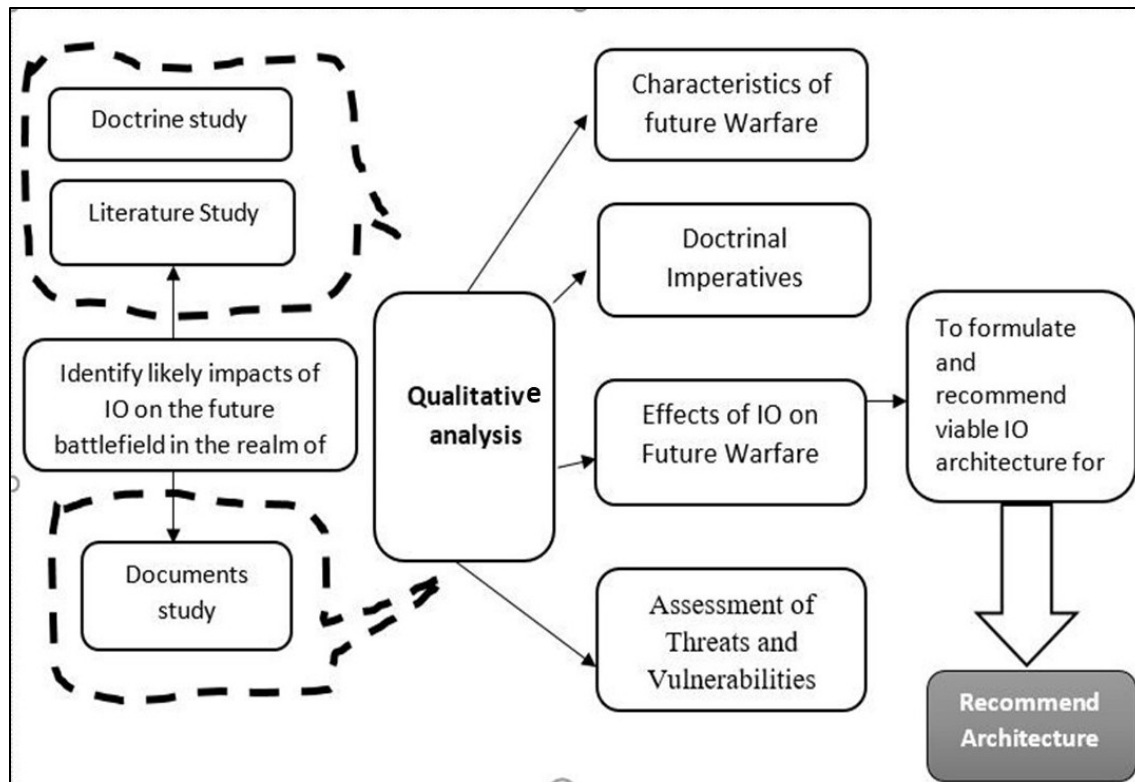


Figure 5. Operationalization Diagram

Source: Created by author.

Scope and Limitations

This paper first analyzes the future battlespace trends and preparation of the Bangladesh Army. The researcher analyzed the IO architecture of advanced and regional countries. The researcher will discuss the appropriate IO architecture of the Bangladesh Army, including challenges. However, future development on IO was out of the preview of the thesis. IO architecture of other countries was consulted mostly from the doctrines and some from the open sources. As such, the authenticity of the open source information may not be confirmed. The study was mostly based on secondary sources.

Definitions and Terminologies

A review of the related definition and terminologies is essential to provide a common understanding of the research paper. Since the U.S. Army has a well-developed set of doctrines related to IO, the Bangladesh Army follows many doctrinal terms of the U.S. Army, therefore, for this thesis, most of the definitions, and terminologies were drawn from the U.S. military doctrine. However, several other definitions and terminologies were considered from the Bangladesh Army doctrine. The IO is also called Influence Operation in other doctrines; therefore, this doctrinal definition is accepted in the thesis to avoid confusion.

The thesis used the definition of IO located in FM 3-13 and JP 3-13. The doctrine defines 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 (HQDA 2013). This specific definition eliminates confusion in defining IO. However, the study of literature is done on a wide span of the timeline. As a matter of fact, in a different timeline, the IO was defined differently. Therefore, this thesis considered that the present definition after the necessary evolution is currently the standard one. Alongside many other definitions were also documented in the research, which all are related to IO. The researcher has outlined all the related definitions in the first chapter to eliminate all confusion.

With this definition streamlined, the next step will be to analyze all the doctrines of different armies. Here the concept of the future battlefield trends will also be analyzed. Through the discovery of the challenges, the paper will conclude with some

recommendations. To answer the primary research question, the thesis will compare and contrast different IO organizations followed in different armies. The criteria used for this comparison is mostly taken from the latest FM 3-0, which outlines the details of IO. The thesis will make this a keystone doctrine since FM 3.0 is very recent and addresses the full details of IO. For solving the problem, the research will take into account the U.S. Army DOTMLPFP (Doctrine, Organization, Training, Materials, Leadership and Education, Personnel, Facility, and Policy) construct. However, due to the paucity of time and the scope of the research, this thesis will only consider the doctrine and organization. However, this paper will address the challenges associated with other fields as well. The conceptual framework is described in Figure 6.

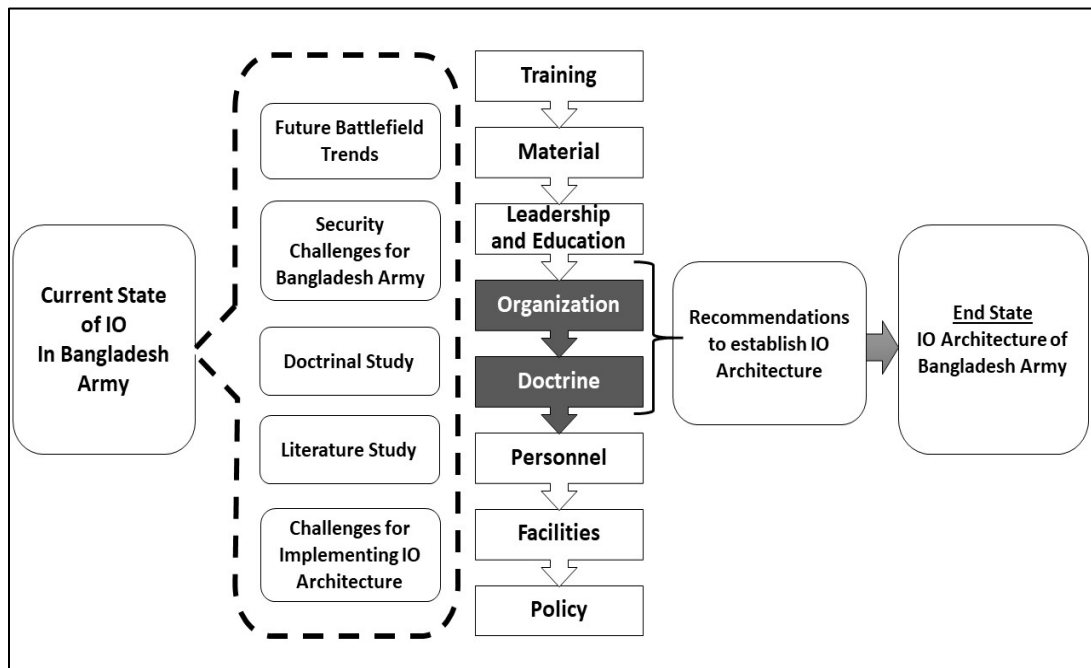


Figure 6. Operational Approach

Source: Created by author.

Chapter Summary

This chapter outlines the method that will be followed to discover the answer to the primary question. This research methodology should provide recommendations for secondary questions. In fact, the answer to the entire secondary question will lead to the answer to the primary question. The researcher uses the DOTMLPFP of U.S. Army force management model to determine the esteemed solution. However, not all the aspects of the concept were taken into consideration. The thesis attempts to compare and contrast among the different organizations of IO used by different armies and then suggest the best suitable model for the Bangladesh Army. This thesis will compare and contrast the different models for IO staff organization and evaluate those models using established principles to find a suitable structure for the planning, preparing, and organization of the Bangladesh Army. The next chapter will analyze all the established doctrines.

CHAPTER 4

FUTURE BATTLEFIELD TRENDS, THREAT PERCEPTION, AND EVOLVING DOCTRINAL CONCEPTS AND INTERNATIONAL EVOLUTION OF IO ORGANIZATION

Chapter Introduction

Like most other military concepts, IO is also a continually evolving affair with its historical origin dates back to the time of antiquity. As ancient as 500 B.C., in the time of Sun Tzu. In the 'Art of War,' Sun Tzu professed, "If you know the enemy and know yourself you need not fear the results of a hundred battles . . . all warfare is based on deception. There is no place, where espionage is not used. Offer the enemy bait to lure him . . . the supreme art of war is to subdue the enemy without fighting (Giles 2000)."

According to Carl von Clausewitz, "War always changes its color as per its environment" (Clausewitz 1989). Warfare has changed its character since the beginning of time. However, in recent time, the rapid proliferation of technology had a more significant and indelible impact over the conduct of warfare and concepts. The technology was always a determining factor to shape the outcome or result of warfare. It is well estimated that the next significant change that will affect the technology is the AI; it will change the way of warfighting. Today's soldiers will have to perform as a soldier, a technocrat, a cyber-warrior, a media manager, and many other roles. The concepts of modern-day warfighting are changing, and will undergo changes in the future that are more dramatic.

For military planners, the dominance in the information domain is critical to military success; command, control, communications, and intelligence nodes are of vital importance for this. As per the statement of Captain Sir Basil Liddell Hart (Thoughts on

War, 1944), “the real target in war is the mind of the enemy commander, not the bodies of his troops.” IO in the form of EW has been practiced ever since the electromagnetic (EM) field was discovered in 1819 and EM waves in 1865. New techniques were often primitive; it was only from World War II onwards that the element of sophistication was introduced in this field. The operation Desert Storm in 2003, the world saw the vivid demonstration of all-encompassing IO by the U.S.-led coalition forces. However, a comparison of the more than 20 existing IO doctrines of various NATO states shows that the concept is handled in various ways. Only a few states have the political determination or capabilities to apply the entire range of instruments. Besides, the majority of countries attribute greater importance to defensive measures than to possible offensive operations (CSS Analyses in Security Policy 2008, 2).

The constant threats in the information domain are witnessing multipronged developments and challenges. They commit criminal activities through phishing, hacking, and stealing of sensitive organizational and personal data. Thus, governmental institutions and companies come under security threat for their secret data that can hamper the daily life of the entire populations in the country. The Bangladesh Bank heist illustrates the need for organizations to move from reactive to proactive security by focusing on three specific strategies, prevention and protection, early detection and speedy mitigation. In the Bangladesh Army, there is a dire need of a core group of professionals consistently working on cyber threat intelligence, data protection, and encryption.

Considering the previous definitions, in this chapter, the researcher will discuss the future battlefield trends/ characteristics, the threat perception for Bangladesh Army,

the present state of the Army in terms of infrastructure to conduct IO. Then the doctrinal and organizational comparison will be drawn among all the models of different Armies. This chapter will delineate the evolution and different concepts of IO existing in different armies (U.S., Russia, UK, Canada, and Australia). By drawing a compare and contrast among all the existing models, the researcher will suggest the most suitable approach for the Bangladesh Army to incorporate institutionally. Before understanding the evolution of different doctrine, it is imperative to understand the characteristics of future operations.

Characteristics of Future Operations

The future battlefields are likely to be chaotic, intense and highly destructive (CJCS 2006b). From the fighting method of the non-state actors and terrorist organization (i.e., the Islamic State) to the conduct of the Russian hybrid warfare with the experiments of combining massive fires with drones and broad-spectrum IW in Ukraine, there are signs the future of warfare is very vivid. One easy finding from the facts above is the technological advantage is going to have the most significant role in determining the terms of the future war for sure. With the initiation of Information and Communication Technology (ICT), a new conceptual dimension to warfare popularly termed as Network Centric Warfare (NCW) including Command and Control Warfare (C2W), Cyber Warfare, and others previously introduced. In the series of all previous Revolution in Military Affairs (RMA), the new addition is the technology entangled with the vast web of information.

The dimension of Future Warfare. Martin Van Creveld, in his ‘On Future War,’ stated, “in the future, war will not be waged by armies but by groups whom we today call

terrorists, guerrilla, bandits, and robbers.” They are likely to be organized on charismatic lines and motivated by fanatical, ideologically based loyalties. In the future, conventional war is likely to be replaced by this and make increased use of prohibited weapons (Van Creveld 1991). As the information age matures, a determined adversary will be able to sabotage, disrupt, or contaminate the information highway. General Gordon R Sullivan and Colonel James of Dubik suggested five trends of future warfare (Ali 2010):

1. Increased lethality and dispersion
2. Increased volume and precision fires.
3. Increased integration of technologies.
4. Achievement of greater mass and effect.
5. Reinforcements in invisibility and delectability.

The battlespace will be global in both geographic and virtual space and highly congested. A combat situation will replace the typical linear battlefield with a 360-degree threat, potential for new high tech weapons, use of chemicals, and biological and use of non-traditional forces and terrorism. With the gradual urbanization of the world’s population, future battles will inevitably be fought within city limits. As such, in addition to the threat from opposing force, the field commander will face structural damage, local industrial hazards, and loss of mobility and degradation of communication links. The essential characteristics of future battlefields and their combined effects are discussed in the subsequent paragraphs:

High Lethality. Advanced armies will employ extremely lethal, precise, and destructive weapon systems. Technological advancements in the present and the future will support this development in lethality and destructiveness. Armies will fight the

highly lethal war against non-state actors and hybrid threat in a complex environment. Implications of wars against hybrid threats include the likelihood that they will be extremely lethal and protracted and the prospect that since they will often take place in congested urban zones (“feral cities”), they will be manpower intensive (Norton 2003).

Expanded Battlefield. The Battle Area is going to be expanded to a greater limit with superior IT. Nations, non-state actors, and even individuals will be able to target military forces and civilian infrastructure at increasing, often over intercontinental, ranges using a host of conventional and unconventional means (TRADOC 2018). The vulnerability of every individual soldier will increase largely in the combat zone when deployed. Nonmilitary installation and the civilian population are likely to be included in the targeting list of the adversaries. The adversary will be equipped with increasingly sophisticated, nuanced, and destructive capabilities, including weapons of mass destruction, conventional hypersonic weapons, and perhaps most critically, cyber weapons and IW.

Wider Dispersion and Use of WMD. The threat of mass destruction will force a wider dispersion of combat groups. Units may have to be deployed widely dispersed initially, with the preparation of quick concentration using greater mobility in times of need. With the broader proliferation of WMD in the battlefield, there will further increase in uncertainty. The WMD might be used in the form of nuclear, conventional, or weapon in cyberspace. WMD will not be the only threat capable of directly targeting and even destroying society, as cyber and information can directly target infrastructure, banking, food supplies, power, and general ways of life (TRADOC 2018). The proliferation of WMD, amongst states and non-state actors, will be a central, enduring cause of conflict.

The risk of Chemical, Biological, Radiological, and Nuclear (CBRN) use will endure; indeed, increase, over the long term (UK MOD 2015).

Dominated by Technological Developments. From now, up to 2050 will be termed as the Era of Contested Equality; the period is marked by significant breakthroughs in technology and convergences in terms of capabilities, which lead to significant changes in the character of warfare. During this period, traditional aspects of warfare undergo dramatic, almost revolutionary change (TRADOC 2018). The technological gap between the conventional armies and their adversaries such as different nonstate actors will diminish. The technological proliferation will force all the armies to contest for technological advantage. Non-lethal, cyber, and space technologies will become mainstream for most of the military. Robotics will be incorporated in the way of military warfighting. Already many countries, develop military robots with some level of autonomy. Many counties will depend on artificial intelligence (AI) for target recognition and destruction by the autonomous weapon system.

Hybrid Adversaries and Threats and Unconventional Warfare. Hybrid threats and nonlinear engagements will dominate the future battle space. Deep reconnaissance, long-range fires, mobility, and unconventional forces will blur the distinction between front and rear. Operation throughout the length and breadth of enemy columns will be a standard feature. Both attack and defense will have to be conducted simultaneously as each combat group will try to mass and maneuver against his opponent. In future conflict, smart adversaries will present regular armies with hybrid threats (combining conventional, irregular and high-end asymmetric threats) at the same time and space. Engagements will undoubtedly involve a range of trans-national, state, group, and

individual participants who will concentrate and operate both globally and locally (UK MOD 2015). Hybrid threats will produce terrorism, insurgency, inter-communal violence, criminality, and widespread disorder. Most of the war of the 21st century is unconventional one – the war against terror, for example, wars in Afghanistan and Iraq, the Israel-Hezbollah conflict and more.

Network Centric Warfare (NCW). The concept of NCW entails a flatter organizational hierarchy through the widespread networking of sensors, decision makers, and shooters. Here sensor gathers analyses and selects targets, commanders take decisions, and shooter engages it, nearly netted in one integrated system (Ali 2010). The system is highly dependent on modern communication technology. This networking combined with changes in technology, organization, processes, and people may allow new forms of organizational behavior. Potential Game Changers through 2050 Revolutionary technologies that, when developed and fielded, will provide a decisive edge over adversaries not similarly equipped (TRADOC 2018). Some of them are described below:

1. Laser and Radio Frequency Weapons – Scalable lethal and non-lethal directed energy weapons can counter Aircraft, UAS, Missiles, Projectiles, Sensors, and Swarms.
2. Swarms – Leverage autonomy, robotics, and artificial intelligence to generate “global behavior with local rules” for multiple entities – either homogeneous or heterogeneous teams.

3. Rail Guns and Enhanced Directed Kinetic Energy Weapons (EDKEW) – Non-explosive electromagnetic projectile launchers provide high velocity/high energy weapons.
4. Energetics – Provides increased accuracy and muzzle energy.
5. Synthetic Biology – Engineering and modification of biological entities have potential weaponization.
6. Internet of Things – Linked internet “things” create opportunity and vulnerability. Great potential benefits already found in developing U.S. systems also create a vulnerability.
7. Power – Future effectiveness depends on renewable sources and reduced consumption. Small

IW and its concept of NCW have reshaped warfare. A networked battlespace integrates all elements and synergizes their firepower and information flow. Battlespace Management System (BMS) comprises of computer integrated to link each soldier, fire and supporting elements, logistics, and other elements, which are part of the electronic network. Here, every element has access to information and can call each other. It enables widely dispersed elements to converge when information of a threat is received. Those elements can synergize their capabilities to destroy the enemy.

Space and Precision. Now, space warfare is assuming greater importance. Its range is global having the best precision-guided weapon, can deliver munitions in minutes, and above all, its intelligence is spectacularly good. Space is emerging as the center of gravity of modern warfare. One of the most critical developments in the history of twentieth-century warfare has been the emergence of the precision weapon. This

weapon can aim against a single target, relying on external guidance or its guidance system. Countries like China are perusing even counter space program. Recent improvements in China's strategic capabilities have ramifications far beyond the Asia Pacific region. China has enhanced its strategic strike capabilities and pursued a robust counter space program, punctuated by the January 2007 successful test of a direct-ascent, antisatellite weapon (Owens 2008).

Joint Operations with Greater Mobility. The nature of the modern battle and the broad geographical range (land, sea, and airspace) of areas of operations makes it imperative that land forces fight as joint teams with the navy and air forces as well as with appropriate civilian authorities. Tomorrow's battlefield is likely to be characterized by highly mobile mechanized forces, using more lethal, more accurate and long-range weapons. Large troops carrying aircraft, high capacity helicopter and improved tracked vehicles will facilitate the armies to move, and maneuver faster than previous battles.

Electronic Warfare with Psychological Effect. The electronic spectrum, its control, and use will affect the planning, and execution of operations in future wars. It has already emerged as a vital component of modern warfare, and its vitality will increase in days to come. Gulf war accentuates the dynamic and revolutionary nature of electronic combat as well as its impact. In future wars, EW equipment will be an effective warfighting tool.

Comments on Future Warfare. Any future war is likely to be fought in multi-dimensions. IW will be the focal point in any such conflict, and its requirement will be of utmost importance. Before the war is being launched, there will be likely effects of a series of warfare through intelligence-based warfare, psychological warfare, economic

IW, cyber warfare, media warfare and so on. Future conflict is going to be a demonstration of modern technology to an extent beyond the limit of our expectations with minimum collateral damages but with maximum effectiveness. Conventional and IW warfare will be complementary to each other.

According to the 2018 U.S. National Defense Strategy (NDS), the future warfare will be ever more lethal and will take place in a disruptive battlefield, combined across domains, and conducted at increasing speed and reach. The battlefield will vary from close combat, throughout overseas theaters, and reaching to even homeland. Some competitors and adversaries seek to optimize their targeting of our battle networks and operational concepts, while also using other areas of competition short of open warfare to achieve their ends (e.g., IW, ambiguous or denied proxy operations, and subversion). These trends, if unaddressed, will challenge the ability of military forces to deter aggression (SecDef 2018).

Effects of IO in Future Warfare

After taking all the characteristics of future warfare, it is imperative to find out its relation to IO. IO is going to influence the conduct of future warfare significantly. Warfare has changed more in this era of IT than it has in all the preceding ones. Technology has always been the major determinant of warfare and always shaped its concepts. No denying fact that technology has changed the way of warfare forever. The changes are going to be more rapid and profound in the future. Today the warfare is based on the dominance of information where there is the participation of state and non-state actors.

The scholars view IO through other angles. According to Robert Leonhard, “It is about making the friendly force move faster, shoot better and protect itself more economically. It is about slowing the enemy, disrupting his operations demoralizing him. (Leonard 1998, 232).” Another writer, Patrick D. Allen in his book, “Information Operations Planning,” puts up his argument that the ultimate objective for IO is to change the behavior of the enemy commander because of the conducted IO (Allen 2007, 44).

Information Warfare (IW). IW is one effect of the effect of IO. The Internet of things (IOT) is the new era in IT, which has substantially changed people’s way of life. Though the IO is significantly different from IW, however, IO can be turned to IW during any hostility. IW aims to deny, exploit, corrupt, or destroy an adversary’s information, information-based processes, information systems, and computer-based networks while protecting one’s own. Future warfare is predominantly going to be in the realm of the information domain, and IW is used to destroy the enemy’s will to fight through degrading its operation in the information environment. Therefore, it is envisaged that IW will be one of the major effects of future warfare in regards to IO.

Cyber Warfare. The citizens of different countries are increasingly getting dependent on the internet. The Internet has become much cheaper and accessible to mass people. Therefore, globally the number of internet users has increased drastically. Many recent incidents portray that many countries have used cyberspace to interfere in the internal affairs of other countries. Most of the countries are now taking preparation for protecting their cyber domain and conduct the battle in the fifth space (Cyberspace). Cyber component of future warfare is going to have a significant impact on IO. Many modern armies like the U.S. Army, UK Army, and other western armies have established

cyberwarfare component. Cyberwar is waged insidiously and covertly during the peacetime. It does not rely on the physical destruction of the adversary; somewhat it corrupts and disables enemy networks. The effect of such cyber activity can be even more significant than physical destruction.

Assessment of Threats and Vulnerabilities: Bangladesh Army Perspective

According to the Bangladesh Telecommunication Regulatory Commission (BTRC), the number of internet users almost doubled in the last two years. It shot up from 30.48 million in 2013 to 58.31 million in February 2016 (The Daily Star, 03 May 2016). Also, from 2016, the total number of Internet Subscribers has reached 80.829 million at the end of January 2018 (BTRC 2018). Which signifies how much the nation is increasingly getting dependent on the internet and IT. Therefore, it is becoming a concern for national security and military. Globally, there were many incidents taking place in recent years. The North Korean attack of 2014 on Sony Corporation, U.S. was one of the most destructive cyber-attacks in U.S. history until date. In 2007, Estonia endured the world's first nation-scale cyber-attack against critical infrastructure, while this 23 December 2016 parts of Ukraine temporarily lost its national power grid in a coordinated cyber-attack (Reuters 2016). In February 2016, stealing incident of 81 million dollars from Bangladesh Bank accounts by hacking its Society for Worldwide Interbank Financial Telecommunication (SWIFT) code system is a glaring example of the prevalent looming threats that surround us. Therefore, it can easily be deduced that organizations including Bangladesh Army can no longer rely on the same trusted techniques to adequately protect against new threats because the state and non-state actors are now capable of creating complex attacks which are neither easy to detect nor contain.

Potential IO Threat Scenario of Bangladesh: Regional Context

All the military of the south East Asia region faces a tremendous threat from the non-state actors. Alongside from non-state actors, Bangladesh's immediate neighbors are reportedly enhancing their IO capabilities. The main problem with Bangladeshi information domain is Bangladeshi people uses around 90% of software which is pirated (Bleyder 2012). Using pirated software have become so mainstream that people think it to be very reasonable. However, people do not know about how that pirated software without any security involved is putting our cyber domain at risk. More importantly, terrorist organizations conduct their financial and information transactions through the internet. In the past, the non-state actors conducted many terrorist attacks globally through the cyber domain. The trends of developments in the fields of IO are discussed in the succeeding paragraphs.

The neighbouring armies of Bangladesh are spending a lot on Intelligence, surveillance, and reconnaissance (ISR) systems (Jha 2014). Thereby, the perceived threat to Bangladesh may not be in the form of direct military intervention; rather it may be in the domain of information and technology. Neighbouring armies of Bangladesh has also grown in terms of space technology. Their indigenous capability in the field of space technology and the successful launch of Satellite and Remote Sensing Satellite (IRS) have led them to grow space power. Many of those armies in the region has also developed a secure cryptosystem for defense computer networks.

Bangladeshi cybersecurity specialist Dr. Touhid Bhuiyan was saying, "Bangladeshi government websites are severely vulnerable to cyber-attacks. The host domains are also not secure, leaving many loopholes for hackers to breach

our system. The websites should be frequently tested for vulnerabilities to prevent further attacks (Rabbi 2017).” Another neighbor of Bangladesh has established a surveillance post in Coco Island long ago (Pike 2016). Intelligence sources also revealed that they has already acquired EW equipment. It has intercepting, monitoring and surveillance capabilities. The maritime reconnaissance and electronic intelligence station on Great Coco Island in the Bay of Bengal is the most important SIGINT.

The vulnerability of the Military. The secrecy and security are the main two primary issues that concern the military of any country. Most of the leading nations in the domain of military power including our potential adversaries have developed enormously in IO sector in the recent past. Moreover, many countries have acquired the capability to incapacitate the C2 nodes of their adversaries. Undoubtedly the future warfare is primarily going to be in the domain of information. That means the Bangladesh Army will have to fight a war for which it needs more preparation like most other armies. Therefore, globally military Installations/Databases/ Communication Systems are becoming incrisingly vulnerable.

Backbone Telecommunications’ Vulnerability. BTCL has the biggest communication network consisting of microwave, fiber optics, and copper wire links. BTCL’s microwave towers can be the primary target of the potential adversary. However, the underground cables and fiber optics network will have a degree of immunity from air strikes. Potential terrorists or saboteurs can gain access to these systems and can change the system configuration. Thus re-routing numbers to different lines, setting up monitoring stations, disconnecting specific numbers and even disrupting routing for entire exchanges, can bring chaos and confusion.

Susceptibility of Submarine Cable. The entire submarine cable has been anchored above the seabed. This has increased daily international calls and providing faster data transmission than the existing satellite circuits. Internet speed became faster and cheaper. It is expected that a substantial development would take place in the IT sector due to the submarine cable. It has connected Bangladesh at Cox's Bazar. It is noteworthy that out of three preceding landing stations; two are at Mumbai and Chennai. Planned Electronic disruption at those nodes can force Bangladesh to switch over to satellite communication or disruption from the rest of the world. The mobile threats are portrayed in the Figure-7 (Sunil 2014).

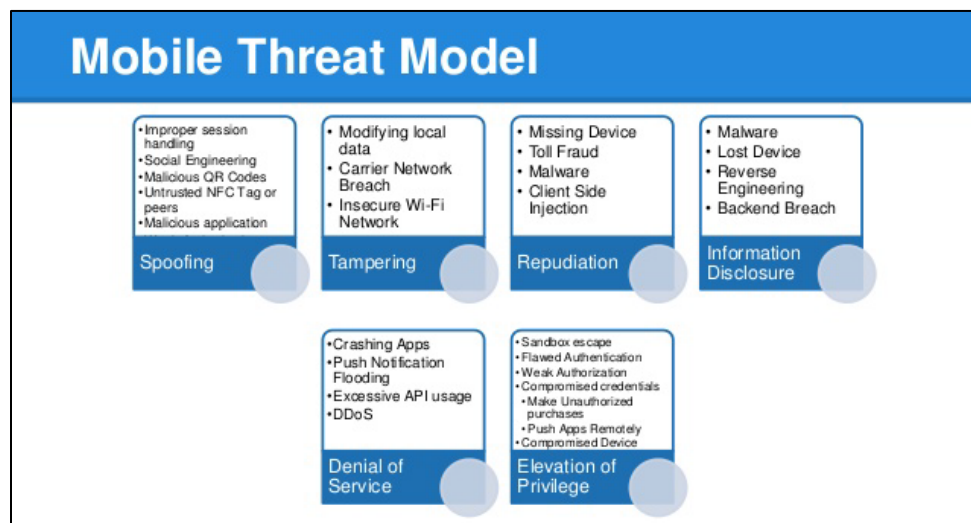


Figure 7. Comprehensive Mobile Threat Model

Source: Sunil 2014.

Force Management Aspects

The U.S. Army has a very well structured force management model. The U.S. doctrine defines force management as the purposeful preparation of individual members of the Armed Forces (and the units that they comprise) to present a force capable of executing assigned missions. According to the model, the first phase focuses on generating capabilities from DOTMLPFP (doctrine, organizations, training, materiel, leader development, and education, personnel, facilities, and policy) construct. The DOTMLPFP is a practical construct, which can guide for methodical force development. DOTMLPFP is a problem-solving construct for assessing current and future capabilities while managing change. However, for this research, from this construct, only doctrine and organization will be deliberately analyzed. The DOTMLPFP construct is shown in Figure 8.

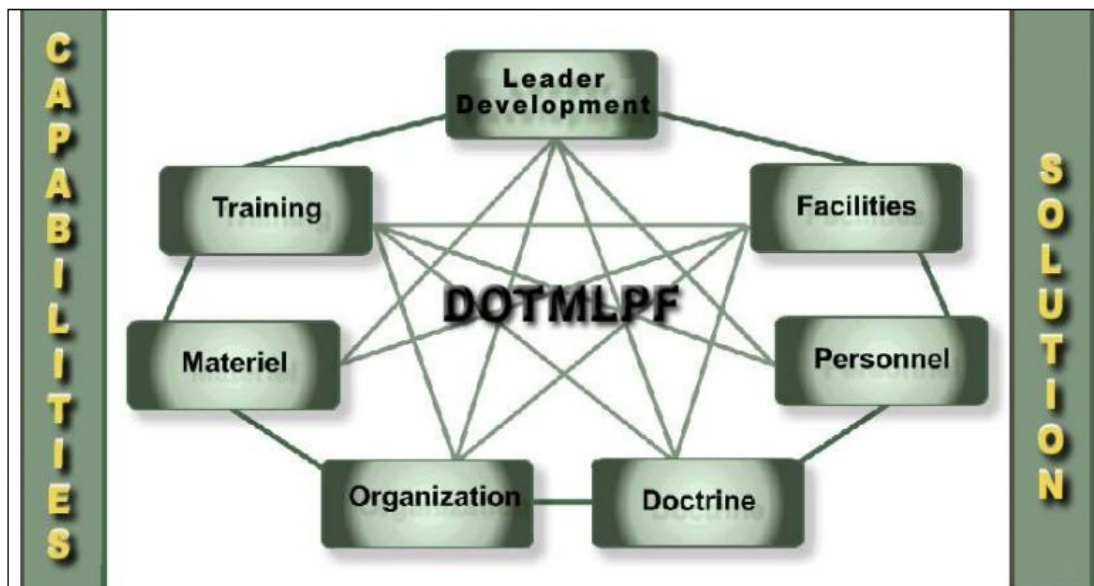


Figure 8. Problem-solving Construct Widely Used by U.S. Military

Source: HQDA 2016, 11.

Advantages for the Bangladesh Army for Incorporating IO

Modern warfare takes place through the exercise of soft power in the information domain at first. As the world moves toward conflicts in which, as Gerasimov describes, “Wars are not declared but have already begun.” It is evident that, whether referred to as IW, information confrontation, IO, or information struggle-no state is guaranteed victory based solely on the abundance of resources or capabilities (Darczewska 2014). The mastery of IO must be continuously nourished, the approach must be corrected over time and must be tailored according to specific audiences. In the modern battlefield, all facets of military operations rely primarily on the information domain. For every military, the first engagement takes place in the information domain. Presently, most of the modern war-fighting gadgets are associated with technology and electronics. For the successful conduct of any military operation, gaining information superiority is the essential aspect of warfighting. US-led coalition forces in the ‘Operation Desert Storm’ in the year 2003 demonstrated the most stunning use of IO. Through a structure for conducting IO readiness state of the Bangladesh Army will be very high.

IO will be an asymmetric warfare tool for the Bangladesh Army to make power balance. IO is denoted as the new asymmetric weapon, and the incidents by Russia with Georgia and Crimea certainly support this categorization (McGrath 2016). Incidents show that small nations with a well-organized IO structure can fight strong adversaries using the new asymmetric weapon. Testimony to this argument is the Russian failed IO against Georgia. Russia, generally perceived as one of the leading powers in IW, lost its information struggle against resilient Georgia, the smaller country with less military capability and military history (Cordesman 2014). Therefore, it is evident that a small

country like Bangladesh and its military can also defend its operational environment from powerful adversaries using this new generation asymmetric weapon. The following Diagram 9 shows how an actor can weaponize the cyberspace:

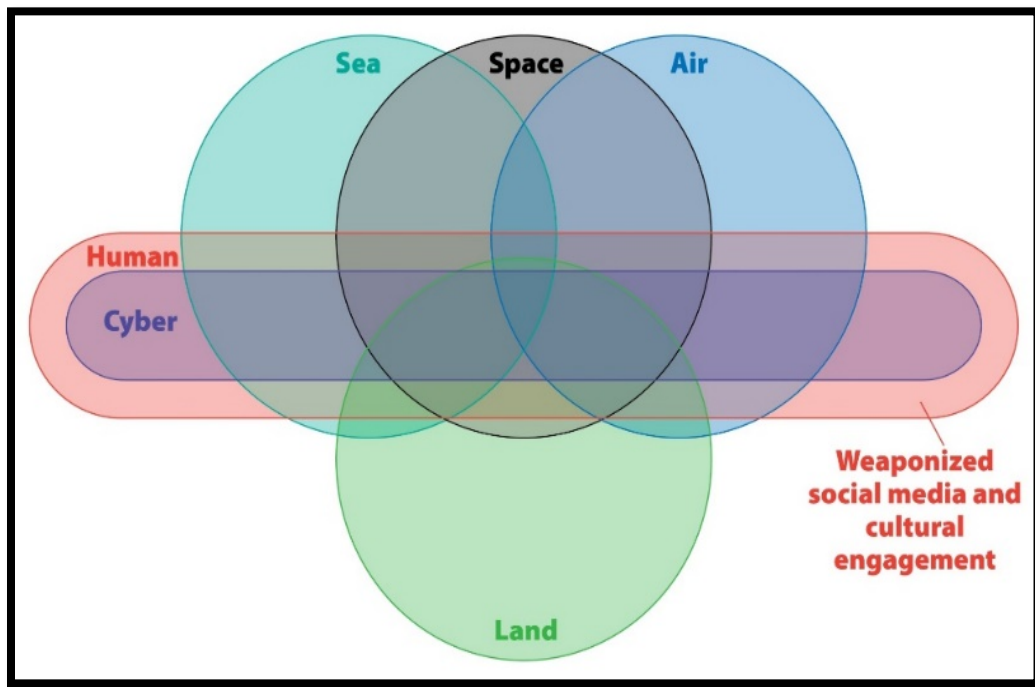


Figure 9. Multi-Domain Extended Battlefield.

Source: HQDA 2013.

Since state and non-state actors have an equal share in information, therefore, IO provides more information security. State and non-state actors worldwide have identified the information environment as the new battleground to be dominated and have already taken measures to wand these ends (Mannion 2018, 1). Globally, non-state actors have been already making impacts. The threat from terrorism will expand in the coming decades as the growing prominence of small groups, and individuals use new

technologies, ideas, and relationships to their advantage. The so-called Islamic States killed many people, globally in the recent past. The recruiting of the members, and finally the attack is usually coordinated through the cyberspace.

IO planning will ensure the protection of critical Bangladesh Army infrastructure. Starting from state governance, utility services, commerce and control of critical national infrastructure, everything is operated through the cyber and IT. The world community has witnessed massive cyber-attacks by an unknown host in a different part of the world. On many occasions, such an attack could successfully paralyze many critical utility services. In the recent past, the first organized cyber-attack took place at the national level against Estonia in 2007. Ukraine was the first victim to temporarily lose its national power grid in the context of a coordinated cyber-attack (Brantly, Cal, and Winkelstein 2017).

Arguably, the latest meddling of the national election of U.S. by Russia was one of the most significant examples. It signified how the IO could change the security environment of the world. At home, in February 2016, stealing incident of 81 million dollars from Bangladesh Bank accounts by hacking its SWIFT (Society for Worldwide Interbank Financial Telecommunication) code system is a glaring example of the common looming threats that surround us. The growing number of warnings voiced in the first half of the 1990s over the potential threat to national security from (asymmetric) cyber-attacks against power plants, banks, or air traffic control gave rise to the debate over protecting critical infrastructures (CSS Analyses in Security Policy 2008, 2).

The IO will ensure additional protection in the cyber domain. According to a report of the Bangladesh Telecommunication Regulatory Commission, “The number of internet users almost doubled in the last two years. It shot up from 30.48 million in 2013

to 58.31 million in February 2016” (The Daily Star 03 May 2016). At this milieu, it is very evident that the threat forces have more access to the information environment to impact national security and military. Therefore, any threat force either a state or a nonstate actor can now gather information and launch a cyber-attack against the military through planting malware. Several attack vectors are phishing attacks, unsecured wireless networks, removable media, mobile devices, malicious web components, viruses, and malware (Kostadinov 2011). The following Diagram 10 shows how the cyber-attack enters the rings of protection:

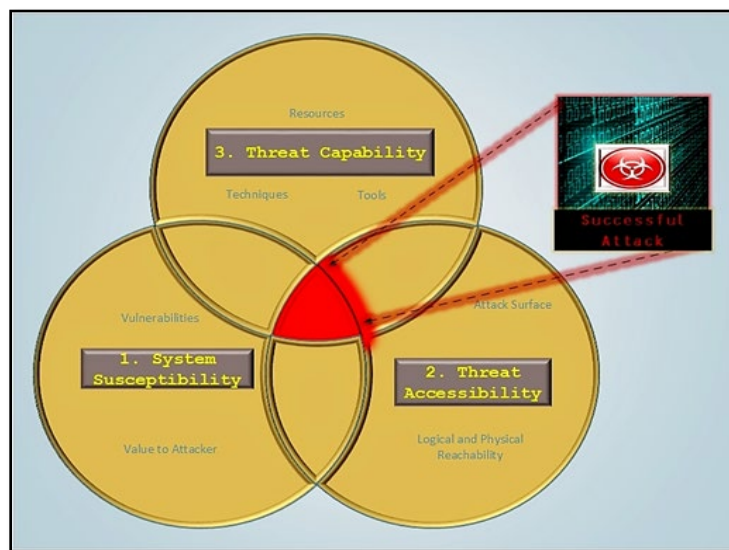


Figure 10. When a Cyber Attack Encircles the Rings of Protection

Source: Kostadinov 2011.

In the recent past, the strategy, techniques, and means invested in attacking and defending cyber-space have seen tremendous growth both in the military and civilian domain. The example of Cambridge analytical scandal, Wiki Leaks, and Panama Paper’s

discloser are crude examples that show how fragile the information domain is to the aspects of personal and national security.

IO at tactical level shall enhance the efficiency of every unit for the Bangladesh Army. Doctrinally, IO is operational and strategic level operations conducted to support tactical level commanders and their operations. However, for all kinds of operations including counter-terrorism, tactical level commanders must emphasize their planning on the use of IO. Now every member of the organization is equally essential due to the concept of 'Strategic Corporal.' The concept illustrates, even the action of a very insignificant member of the military can affect the performance and image of the organization. That means the low-level unit leaders can take independent action and make major decisions. So even at the tactical level, all soldiers need to understand the importance of IO. Since the Bangladesh Army is operating globally in the United Nations peacekeeping operation, therefore it is essential to integrate IO even at the tactical level. It will empower the junior leadership and every single individual of the organization.

Organizational Comparison and Contrast between All Doctrines

The European countries including the UK follow a similar kind of doctrine and organization for their unified operation in NATO. However, there are differences in the US, Australia, and Russian doctrines in the conduct of IO. In the subsequent paragraph, the paper shall put the analysis of the organizational aspects of all the Armies (US, NATO, UK, Canada, Australia, and Russia) from their doctrinal perspective. The organizational analysis will center on the different levels of war: strategic, operational, and tactical. The paper shall also endeavor to discuss the staff organization of the Armies. From this analysis, the researcher will draw a comparison among all the organization and

suggest a model for the Bangladesh Army. The U.S. Army is globally one of the leading armies in the IO domain.

The U.S. Army Doctrine

The U.S. Army has separate manuals for the conduct of IO at the joint, operational, and tactical level. Field Manual 3-0, Operations (FM-3.0) is the Army's most recent publication, which delineates details instruction about the conduct of IO in the LSCO. FM 3-13, Information Operations is the prime manual, which delineates the guideline about all the tactics, techniques, and procedures for the conduct of IO at the tactical and operational level. Joint Publication 3-13 (JP 3-13) is the Joint Doctrine for the conduct of IO in the U.S. military. The manual published in November 2012 provides joint doctrine for the planning, preparation, execution, and assessment of IO across the range of military operations at the strategic level. According to U.S. Army doctrine FM 3-13 on IO, the components of IO are the following:

1. Military deception (MILDEC).
2. Military Information Support Operations (MISO).
3. Soldier and leader engagement, including police engagement.
4. Civil Affairs (CA) operations.
5. Combat camera.
6. Operational Security (OPSEC).
7. Public affairs.
8. Cyberspace Operations.
9. EW.
10. Space operations.

11. Special technical operations.

The formations that deals with the information domain for the U.S. Army as part of the Army Cyber Command are Network Enterprise Technology Command (NETCOM), 1st IO Command, Cyber Protection Brigade, and 780th Military Intelligence Brigade. Within the next three years, the U.S. Army will convert the U.S. Army Cybercommand to IO Warfare Command. At the operational and tactical service levels, each military branch uniquely contributes to an integrated IO effort synchronized by the joint force or joint task force headquarters J-39 division (HQDA 2013). The following paragraph will describe in details about the organizational aspect of all these formations at a different level. The dynamic continuum of IO at a different level is shown in Figure 11.

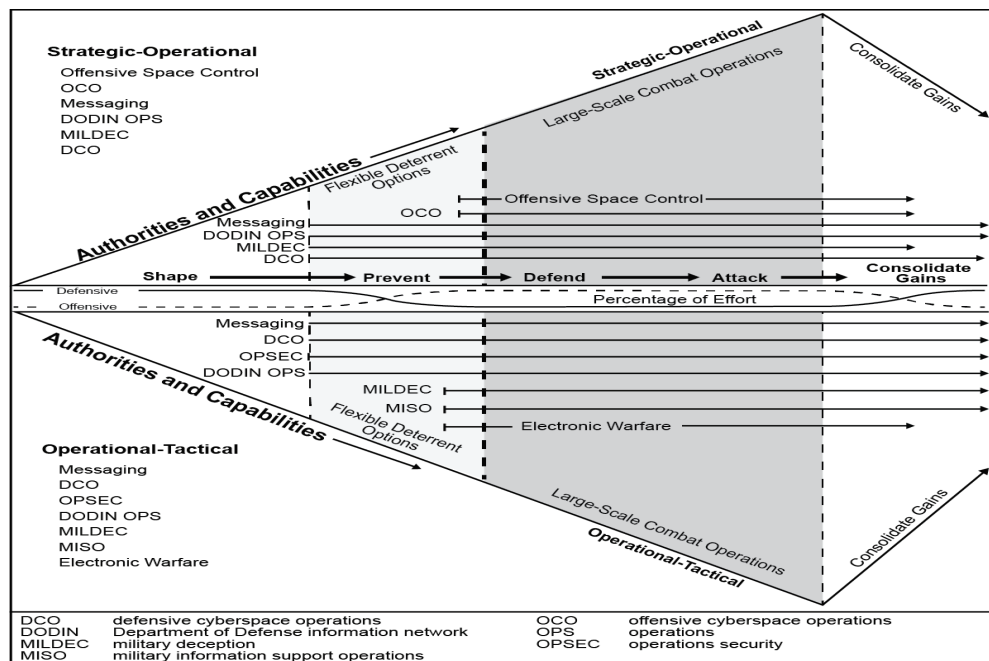


Figure 11. Dynamic Continuum of Information Operations

Source: HQDA 2013, 2-27.

Architecture at the Strategic Level. The authority to employ IRCs is rooted foremost in Title 10, United States Code (USC). While Title 10, USC, does not specify IO separately, however, it gives authority to provide authoritative direction over all aspects of military operations. The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3210.01, Joint IO Policy, provides joint policy regarding the use of IRCs, professional qualifications for the joint IO force, as well as joint IO education and training requirements (CJCS 2012). While all unit operations, activities, and actions affect the information environment, IRC requiring synchronization and coordination as part of IO.

At the joint operation level, the IO cell chief makes sure that the IO experts are adequately grouped with the Joint Planning Group (JPG) to ensure that IRCs are integrated within all planning. Joint IO planners should be integrated with the joint force planning, directing, monitoring, and assessing the process. Overall, the Under Secretary of Defense for Intelligence (USD[I]) is responsible for planning all kind of intelligence support for the conduct of IO. At the joint level, the Joint IO Warfare Center (JIOWC) is established. CJCS controls the JIOWC and it supports the joint staff to integrate the IRC and conduct IO to meet the expectation of the Combatant Commander (CJCS 2006a). Figure 12 depicts the Details of the national IO cell. The formations, which deals with IO at the strategic level, will be discussed in the subsequent paragraphs.

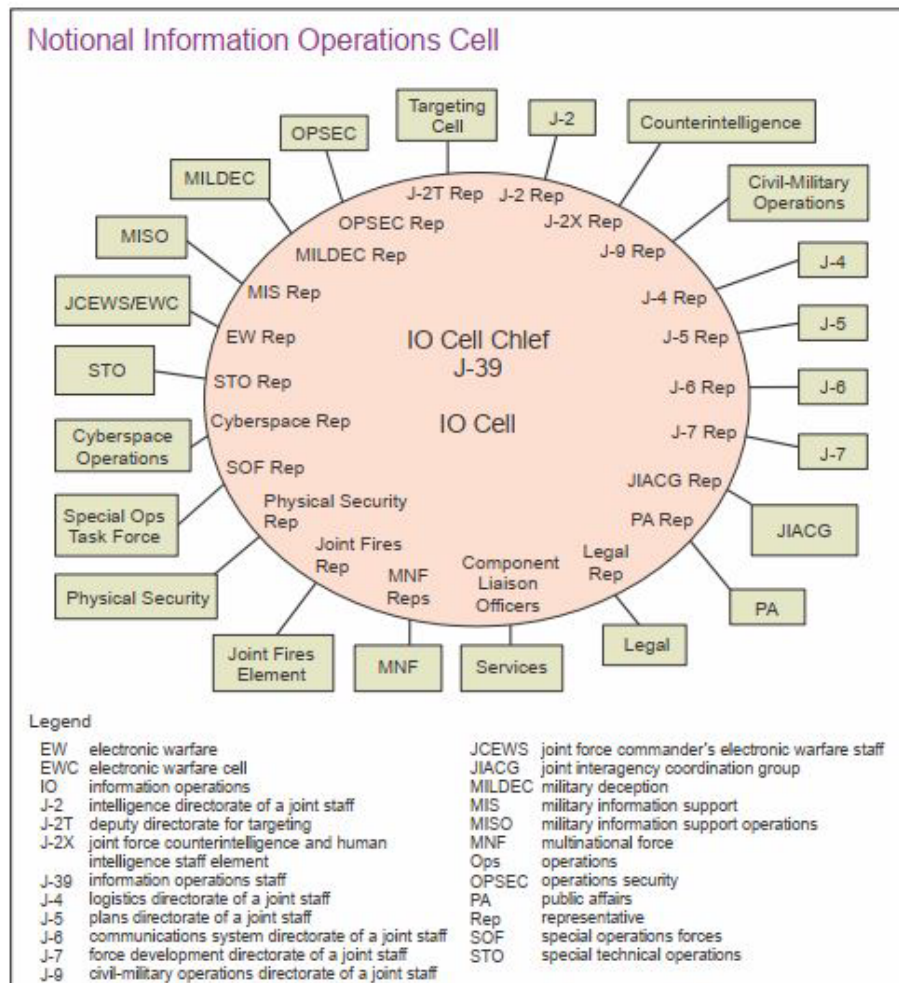


Figure 12. National Information Operation Cell

Source: CJCS 2012, II-6.

The 1st Information Operations Command (Land). This formation was formerly the Land Information Warfare Activity Information Dominance Center (LIWA/IDC), is an IO command of the U.S. Army Cyber Command (ARCYBER). The Army Cyberspace Operations and Integration Center is an operational element ARCYBER is responsible for supporting joint IO missions through operational control of the 1st IO Command (Land). The 1st IO Command is the U.S. Army's only Active Component IO

organization. A multi-component, brigade-level organization, it consists of a HQ and HQ Detachment (HHD) and two battalions (CYBERCOM 2019). Figure 13 shows the location of the different units under the U.S. ARCYBER.



Figure 13. U.S. Army Cyber Command Deployment

Source: CYBERCOM 2019.

1st IO Command's mission is to provide IO and Cyberspace Operations support to the Army and other Military Forces through deployable teams, reach back planning and analysis, and specialized training. The 1st IO Battalion is responsible for the training and global deployment of multiple expeditionary IO teams from the Active Duty and Reserve Component to synchronize information related capabilities in support of the Army, Joint Task Forces, and Combatant Commands. Using publicly available information, 1st Battalion provides social media analysis to enable force protection and operational security in support of deployed forces. The 2nd IO Battalion deploys multi-

functional IO teams worldwide while maintaining close and remote network access to employ a full range of IO capabilities that improve the readiness and ability of U.S. military forces to operate decisively in a contested Information Environment. (1st IO Command 2019). The organization is shown in Figure 14.

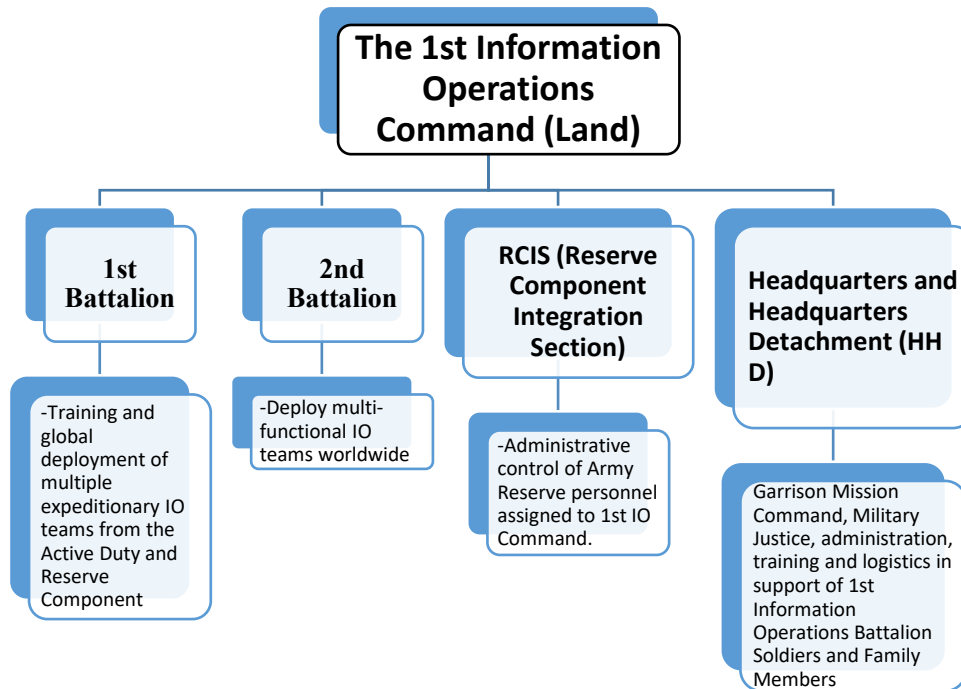


Figure 14. The 1st IO Command (Land) Organization

Source: 1st IO Command 2019.

Architecture at the Operational Level. Theater IO Groups. This group provides IO support to the theatre Army. These units augment theater forces with deployable, mission-tailored, support teams and continental U.S. based operational planning support, intelligence analysis, and technical assistance (HQDA 2013). The Army is responsible for providing the support for the theater forces, which includes organizations, include the

1st IO Command (Land) from the Regular Army and theater IO groups from the Reserve Component. Theater IO group commanders deploy scalable theater IO group elements with varying capability packages to support IO and IIA mission requirements for Army Service component command through BCTs.

Architecture at the Tactical Level. At the tactical level in every division and brigade HQ, there are IO cell and tactical field support team. In the framework of the BCTs, the tactical field support teams provide IO and IIA support. The IO cell at the tactical level operates with the principals of mission command. At the tactical level, very often the resources are limited to organic personnel, weapons, and munitions or assets. However, those can be attached, borrowed, or improvised to perform the given mission. At the operational and tactical levels, the Army uses IIA, in coordination with cyber electromagnetic activities, to support strategic communication and IO-focused objectives and to execute joint directed tasks (HQDA 2013).

IO Headquarters Staff Structure. Commanders often organize their staff structure depending on the mission, requirements, strengths, and weaknesses. When operating in a joint or multinational environment, commanders may reorganize its staff to better align with higher HQ. Besides, commanders designate resources (IRC) to employ to support IIA. At the joint level Under Secretary of Defense for Intelligence-USD (I) is responsible for planning all kind of intelligence support for the conduct of IO. At the operational level, the responsibility lies with the division and brigade commanders.

Doctrinal Guideline for Composition of Staff. To find out an appropriate structure for the staff or any cell, the first is to examine who all are likely to be involved in this affair. Doctrinally, members of both lethal and non lethal system are involved in the

planning. Along with these representatives, other potential participants are members of the legal team, operations officer, chief of staff, civil-military, psychological operations, liaison officers, and deception planners (Brock 2005, 23). Figure 15 illustrates the details of the staff required for any HQ.



Figure 15. IO Cell

Source: CJCS 2012.

Role of the Commander in conducting IO. The commander leads IIA, and he is advised by the G-7 (S-7) and supported by the entire staff for conducting IO. The commander addresses the global audience and audiences in each area of operations through mission command and IIA, while acknowledging the social aspects and dynamics of the information environment in an area of operations. The G-7 (S-7)

coordinates and synchronizes the commander's themes and messages with the higher HQ to maintain the synergy and to ensure they do not conflict (HQDA 2013).

G-7 assistant chief of staff, IIA. The G-7 (S-7) acts as the commander's coordinating staff officer for the planning, integration, and synchronization of designated IRC. G-7 (S-7) is the key appointment who advises the commander on IO affairs when operational activity and its direct or indirect message or perception could influence the information environment. The IIA section led by the G-7 (S-7) in the MDMP contributes to the overall intelligence preparation of the battlefield (IPB) by developing IIA input and products. This section works with the G-2 (S-2) to develop products that portray the information infrastructure of the area of operations and aspects of the information environment that can affect operations (HQDA 2013). An effective G-7 (S-7) understands how to use all components of the mission command system to successfully integrate, coordinate, and synchronize the use of information-related capabilities into the supported unit's operations. The G-7 (S-7) uses various available network-enabled systems to leverage existing and emerging technologies to help transfer knowledge horizontally and vertically (HQDA 2013).

Integration of IO in the Running Estimate and the Military Decision-making Process. In the process of MDMP, in every step, there is the deliberate integration of IIA. While doing the mission analysis, the G-7 (S-7) writes the paragraphs one (mission) and two (situation and considerations) for the IIA running estimate (HQDA 2013). These paragraphs form the basis of all the subsequent planning throughout the MDMP. At the end of mission analysis, the IIA running estimate includes all the necessary guideline for the conduct of IO throughout the operation. However, this is not finished at the end of the

mission analysis, rather this is a continuous process and updated as and when necessary. In fact, paragraph two of the IIA running estimate becomes the IIA input to the mission analysis briefing.

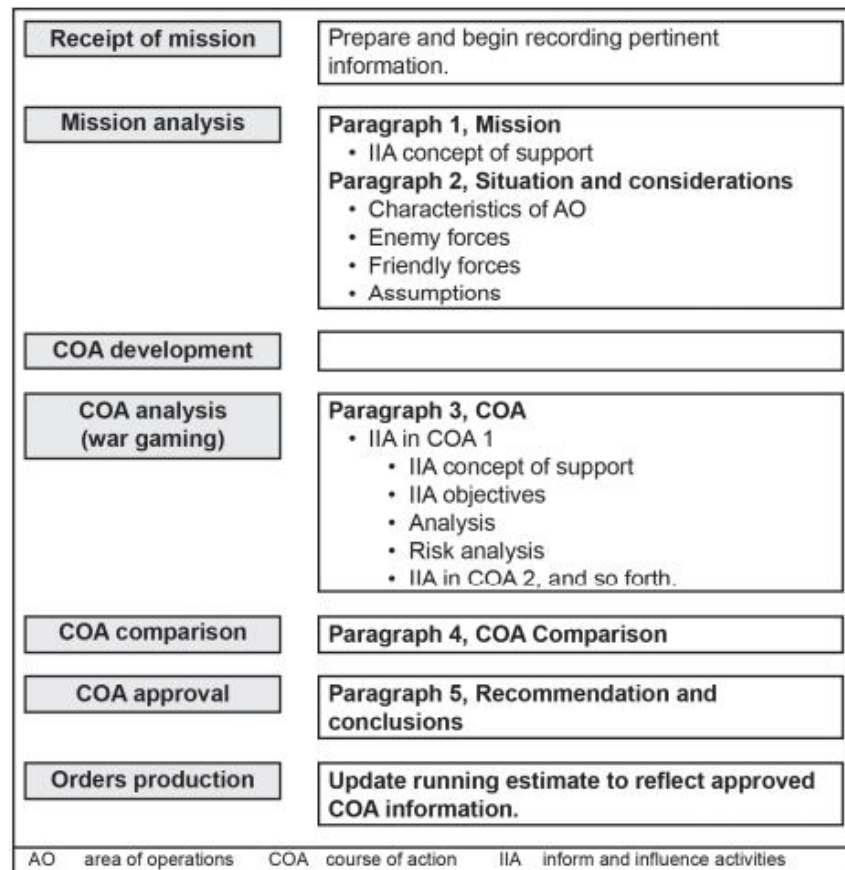


Figure 16. IIA Running Estimate and the MDMP

Source: HQDA 2013, 5-22.

The NATO

There are many similarities in the doctrine and operation procedure of all the NATO countries. The NATO doctrine is outlined in a manner that all the NATO countries can operate in harmony. AJP 3.10, (2014) is the operational level NATO publication to provide direction and guidance for planning, conducting and assessing IO integration into operations. The doctrine is designed to provide combined, joint IO interoperability. Since the end of the Cold war, most of the NATO countries under the leadership and alliance of the US, have reorganized their militaries to fight counter-terrorism (CT) and counterinsurgency (COIN) operations.

Countries like Russia, China, and Iran, have continued to develop their information and political warfare capabilities. As a result, significant information knowledge and capability gap now exist between NATO their potential adversaries (Lauder 2007). In particular, Russia has used extensive political warfare capabilities and theory. Therefore, the NATO countries have vigorously updated all their doctrines, and they have developed the NATO doctrine. The information environment is defined by AJP 3.10 as “an environment comprising the information itself, the individuals, organizations and systems that receive, process and convey information, and the cognitive, virtual and physical space in which this occurs” (NATO 2009).

The British Army Doctrine

Presently, the British Army is a well-organized military outfit to conduct IO. British use of IO led to the change in British domestic public opinion and international (especially U.S. public opinion). Examples include the atrocities in Belgium, such as the burning of towns (Leuven), labeling the Germans as the Huns, the sinking of the

Lusitania, and the Zimmerman Telegrams. Those incidents led to increased recruiting, including volunteers from neutral countries. The leading two organizations that conduct the information is the 77th Brigade and the 1st Intelligence Surveillance and Reconnaissance Brigade (1st ISR). In the British Army, the IO is termed as Information activities and outreach (IO&A), and the IO includes Information activities and outreach (IO&A).

The 77th Brigade was established in the year 2015. A year before that, a memo flashed across the British Army, which stated, “Warfare in the Information Age, we are now in the foothills of the Information Age.” It stated that the British Army needed to fight a new kind of war, one that “will have information at its core.” That paved the way to establish this unique brigade. The Army needed to be out on social media, on the internet, and in the press, engaged, as the memo put it, “in the reciprocal, real-time business of being first with the truth, countering the narratives of others, and if necessary manipulating the opinion of thousands concurrently in support of combat operations” (Miller 2018). In the subsequent paragraph, the researcher will explain the organization of the British Army related to IO&A.

First Intelligence, Surveillance and Reconnaissance Brigade. The first ISR Brigade of the British Army has created as part of the Army 2020 reforms (Jones 2015). The brigade became operational on 1 September 2014 and had responsibility for all British Army ISR capabilities. The Brigade is composed of 19 units; 10 regular and nine reserve units (UK MOD 2013) which includes weapon locating radar and other technical surveillance equipment; surveillance and target acquisition patrols; and the unmanned

aerial systems (UAS). It is intended to be able to deploy tailored ISR groups to support deployments (UK MOD 2014). Figure 17 shows the dispositions of the brigade.

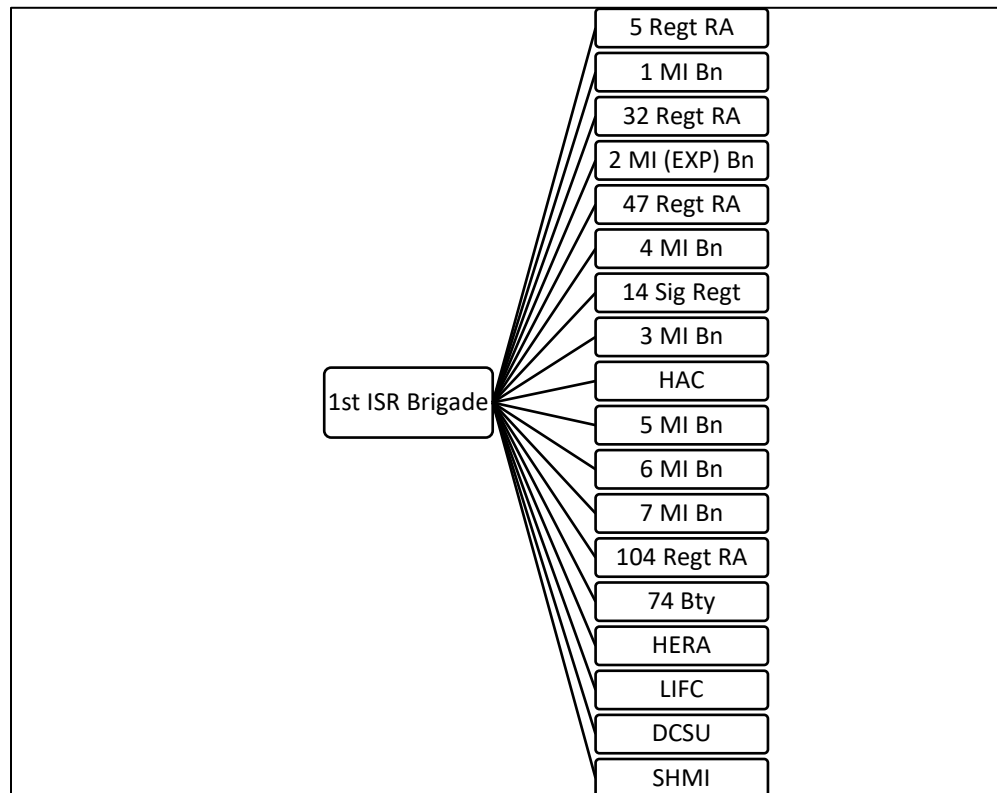


Figure 17. Organization of 1st ISR Brigade, UK

Source: UK MOD 2014.

The 77th Brigade. It is a combined Regular and Army Reserve unit, which was established in January 15. It was raised under the Army 2020 concept of the British Army (Jones 2015). The brigade aims to challenge the difficulties of modern warfare using non-lethal engagement and legitimate non-military levers as a means to adopt behaviors of the opposing forces and adversaries (UK MOD 2019). The brigade delivers information

activities and outreach (IA&O) in order to influence the perceptions, will, and cohesion of target audiences. The brigade is the part of the Force Troops Command and structured to execute its operational outputs. Its organization shown in Figure 18 (UK MOD 2019).

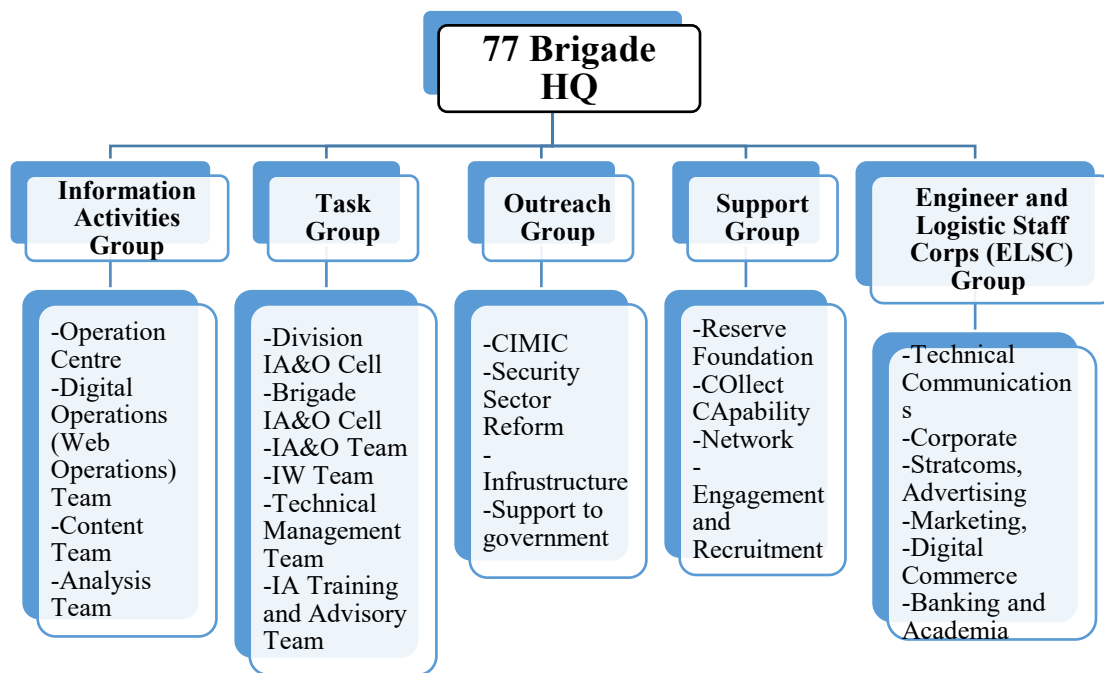


Figure 18. The Structure of British 77th Brigade

Source: UK MOD 2019.

Their activities include audience actor and adversary analysis, information activity and outreach, counter-adversarial information activity, support to partners across government, collecting media content, disseminating media, monitoring the information environment, evaluating the information environment (UK MOD 2019). The unit operates globally to serve the interest of the U.K. Government. Provide support to other government departments in the aim to achieve stability overseas; lead on special

influence methods; build military capacity in all stages of conflict (UK Parliament 2015).



Source: UK MOD 2019.

The Brigade and Unit IO cell. At the brigade level, there is another IO cell, which is a small team and acts as a bridge between the division IO cell and the subunit level teams. This cell supports manoeuvre brigades planning and execution. The 77 Brigade

send representatives for establishing those IO cells. The brigade IO cell will have several IO teams which will be allocated to the under command units. The IO teams assigned by the brigade operate at the battlegroup/ unit level. However, they are also capable of operating independently. They will be apportioned as necessary to achieve the supported commander's desired effects. The structure is given below in Figure 20.

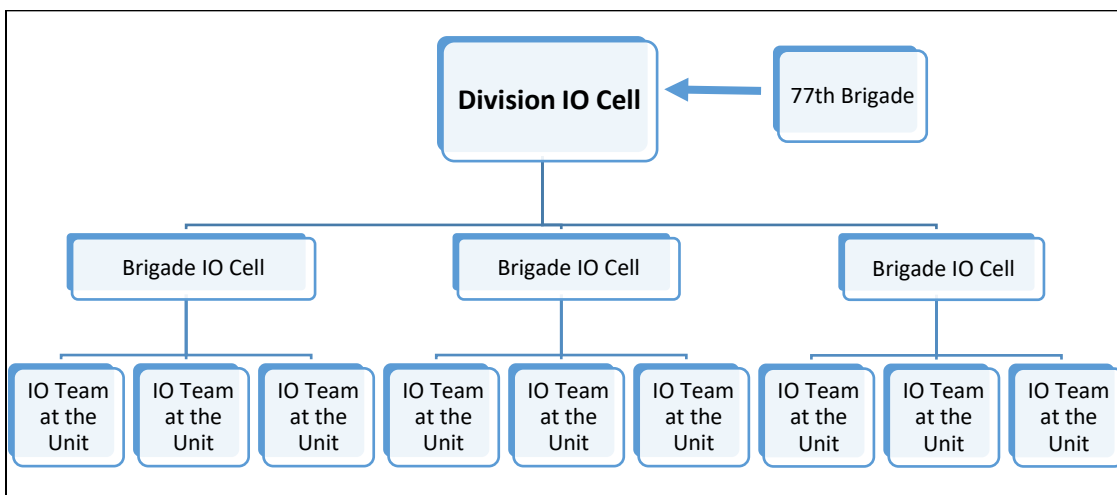


Figure 20. IO Structure Division and Below

Source: UK MOD 2019.

Canadian Doctrine

Canadian Army has the IO doctrine, which has a lot of similarity with other NATO countries. All the doctrines outlines that must be fully integrated and coordinated with all other Joint Force actions to achieve success and meet the commander's objectives (Canada DND 2015). The Canadian Army has separate doctrines for the IO at a different level. The Canadian Forces Joint Publication (CFJP) outlines the lore of the

Canadian Armed forces at the strategic level. Land forces IO (B-GL-300-005/FP-001) is the doctrine, which outlines the role of the land forces at the operational and tactical level. In January 2018, the doctrine was published and updated. Land force doctrinal note 003/06: the conduct of IO in the contemporary operating environment also provides some additional guidance. In the doctrine, the distinction between the levels is clear. However, the effects of political, strategic, operational, and tactical levels of joint operations will not remain isolated to one level.

According to Canadian Doctrine Communication Information System (CIS) are essential to the effective application of military power. The Canadian Army Command and Information architecture have three complementary components focused on operational, system and technical issues. The operational architecture view of the overall command and information architecture establishes the required connectivity among processes, functions, information, and organizations to provide our command, control and information system (CCIS). The system architecture view of the overall command and information architecture seeks to identify relationships among Command and Control Information System (C2IS) components and create physical connectivity within the information system. The technical architecture view of the overall command and information architecture establishes a set of rules governing the arrangement, interaction, and interdependence of all the parts and elements that together constitute our CIS (Canada DND 2018). The architecture is shown in Figure 21.

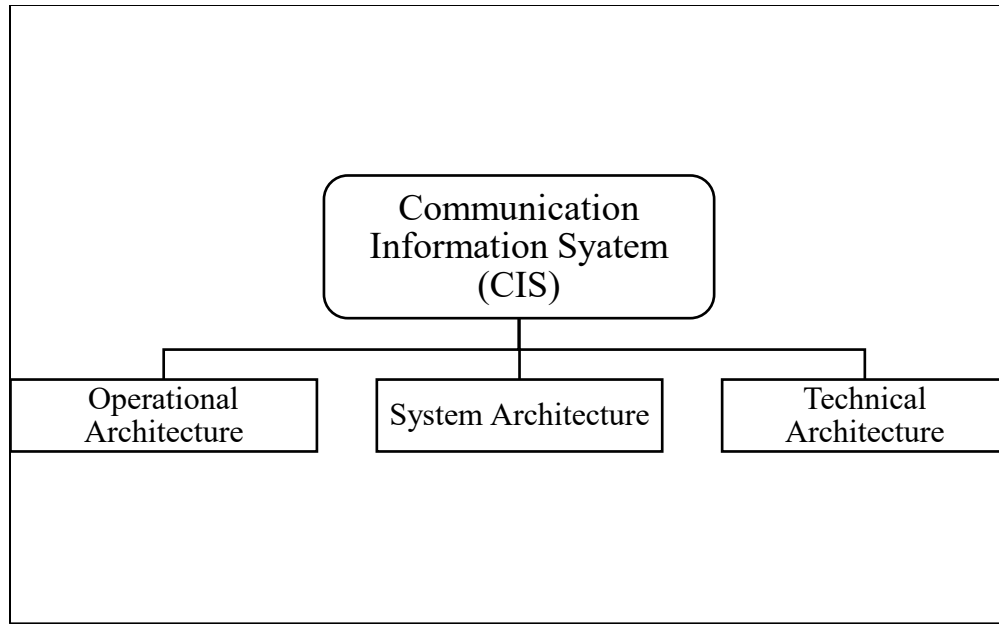


Figure 21. Components of IO Structure

Source: Canada DND 2018.

Architecture at the Strategic Level. Canadian Armed Forces (CAF) joint doctrine defines IO as “actions taken in support of political and military objectives which influence decision makers by affecting other’s information while exploiting (fully utilizing) and protecting one’s information” (Canada DND 2015). At this level, the CAF is used within an overarching entirety of government framework and in a synchronized fashion. Operations by CAF are directed, planned and conducted at three levels of command; direction and guidance are obtained from the Chief of Defence Staff (CDS) via the Strategic Joint Staff (SJS), while planning and execution are primarily achieved at the operational and tactical levels (Canada DND 2015). The integration of IO at the strategic level is shown in Figure 22.

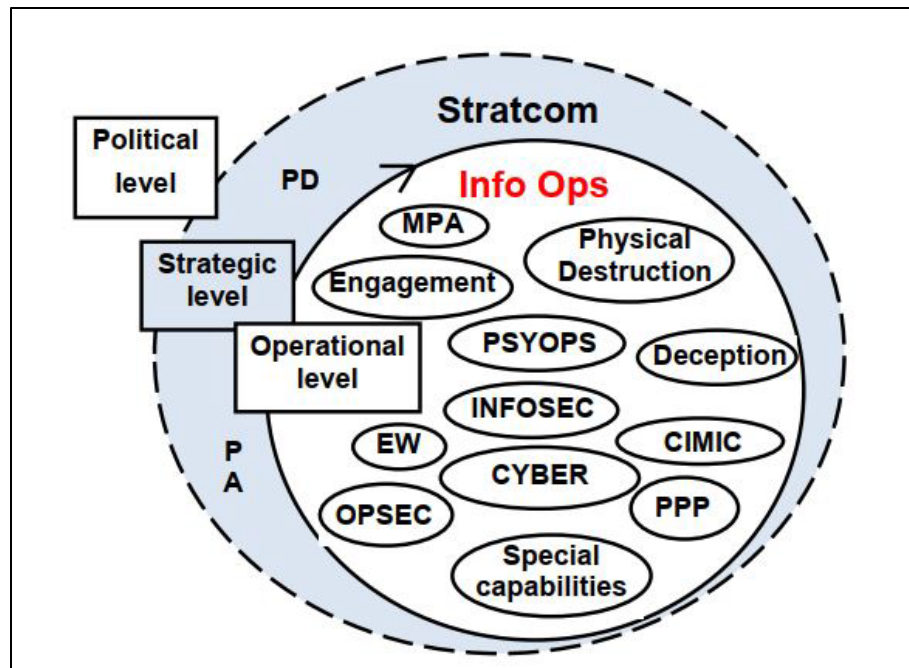


Figure 22. Integration of IO within the Strategic Communication Framework

Source: Canada DND 2015.

Available political guidance, strategic goals, directives, and limitations make up strategic guidance. The strategic framework includes typically a narrative in regards to the threat. The Strategic Joint Staff (SJS) considers the contribution that IO, can make to the achievement of Government of Canada (GC) strategic objectives and provides military advice to the GC in forming IO advice (as outlined in CAF Policy on IO). After the initial coordination process has been established and strategic planning guidance has been issued, the SJS contribute to further refinement of the OPLAN, contingency plan (CONPLAN) or Standing Defence Plan (SDP), taking into account issues from the strategic guidance (Canada DND 2018).

Architecture at the Operational Level. At the operational level, for the CAF, the architecture of the Land Force Command and Control Information System (LFC2IS) supports the Land Force Command and Control System (LFCCS) (Canada DND 2018). This architecture is a three-tiered interoperable system. The system is illustrated in Figure 23. The top tier consists of the specialized and functional applications to enable the Common User Core (CUC) to become functional. The middle tier consists of the CUC. The CUC provides common applications and services such as, command and control tools, digital geospatial services, database management, planning, orders preparation and messaging, which can be tailored to the user requirement. The bottom tier can be thought of like the foundation that supports the rest of the strategy, comprising the digital information distribution backbone and position determination and navigation capability (Canada DND 2018).

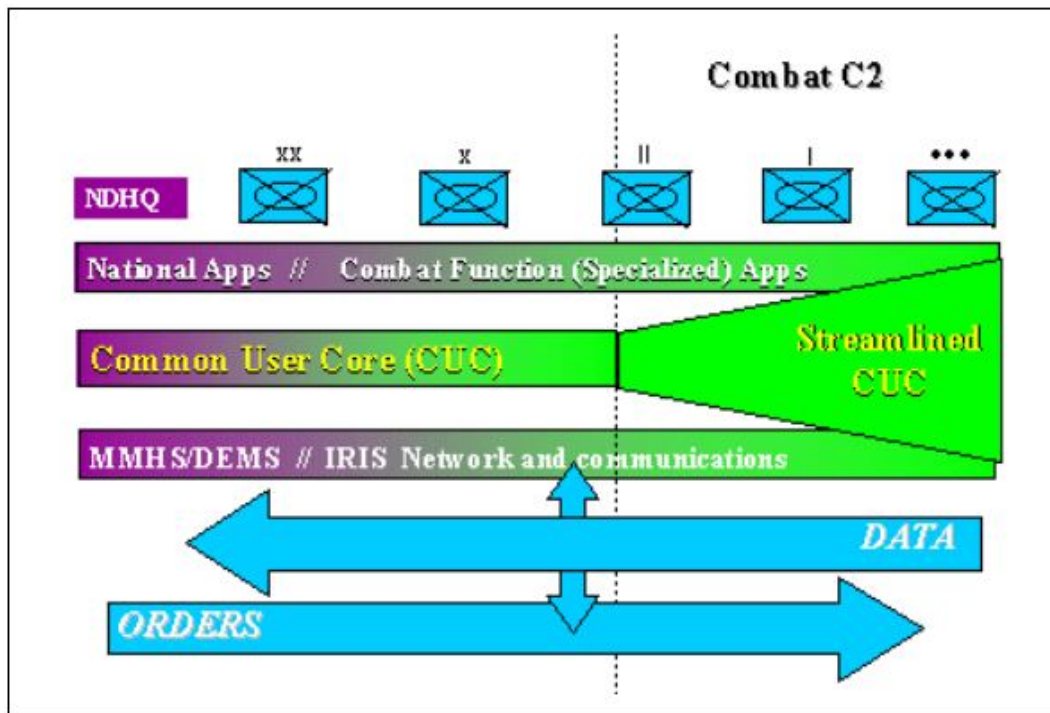


Figure 23. Architecture at the Operational Level

Source: Canada DND 2018.

Architecture at the Tactical Level. At this level for the CAF the IO on creating the desired effect on approved target audiences, key local decision-makers and groups by affecting their will, capabilities, and understanding (including decision-making processes). IO is also conducted to protect own information and information systems. The division and units below operate at the tactical level.

IO Headquarters Staff Structure. The IO Staff is comprised of a Chief IO and sufficient supporting staff relative to the HQ size and function. The command level and assigned mission will determine the focus and responsibilities of the IO staff. For the IO staffs to operate at the Operation level and above the HQ need a comprehensive setup to

perform analysis, planning, operations, intelligence support and specialists to conduct targeting and operation assessment. In the Canadian Army, several models for the staff structure exists; however, the concept of centralized IO brigade under the COS with a Chief Info Ops is considered the most effective one. The IO representatives should be integrated into the J2, J5 and J3 areas (Canada DND 2018). The Canadian doctrines consider the IO component as shown in Figure 24.

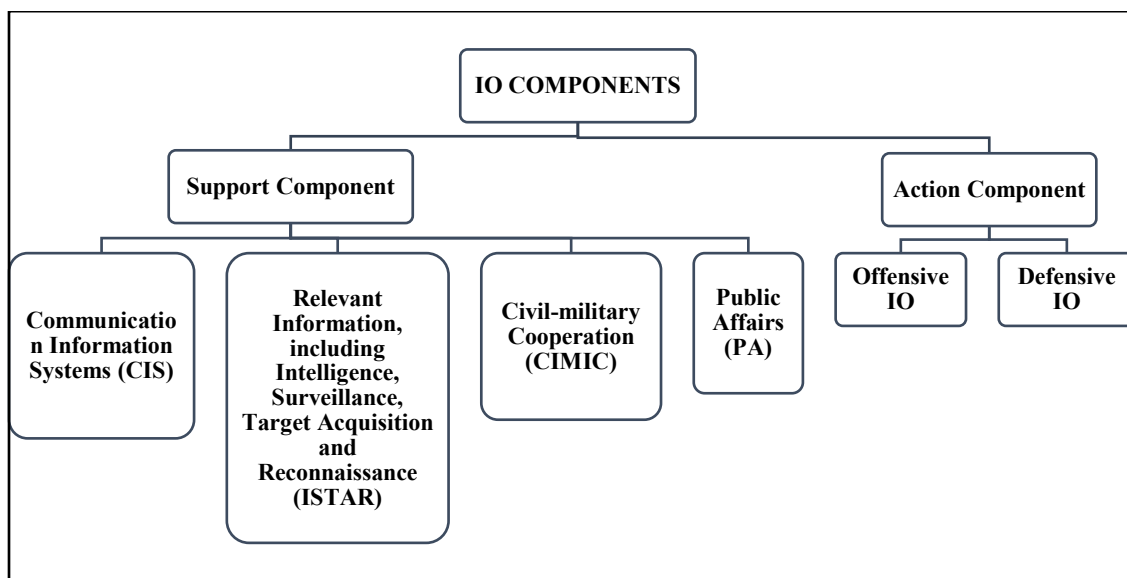


Figure 24. Components of IO in Canadian Doctrine

Source: Canada DND 2018.

Australian Doctrine

Australia, keen to embrace the concept, relied almost solely on U.S. doctrine for the formalization of the function (Logue 2010). According to Australian doctrine, the information domain is composed of all information and related infrastructure that may

influence operations. The information domain interacts with the physical and human domains as shown in Figure 25.

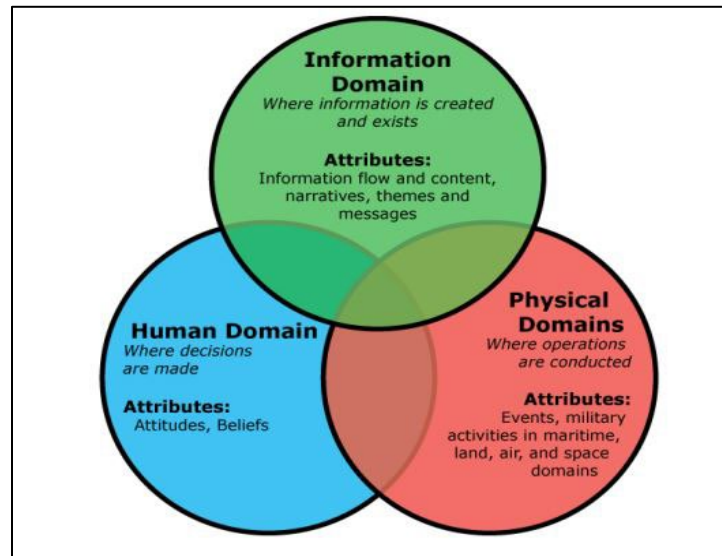


Figure 25. Relationship between Domains

Source: Australian DOD 2013.

Architecture at the Strategic Level. In the Australian Army at the strategic level, the Chief of the Defence Force (CDF) and Secretary are responsible for the overall direction of Info Activities within Defence. They act as the bridge by coordinating Defense's input into the National Security Committee of Cabinet¹ and promulgating CDF planning guidance to Defence. The CDF focuses on Strategic Command Groups planning and execution of shaping and influencing. Military Strategic Commitments Division. This coordination contributes to the communication at the strategic level and drives the structure for IO. Figure 19 outlines the coordination of IO at the strategic level

within Defence (Australian DOD 2013). Headquarters Joint Operations Command (HQJOC) is responsible for the planning and execution of IO (Figure 26).

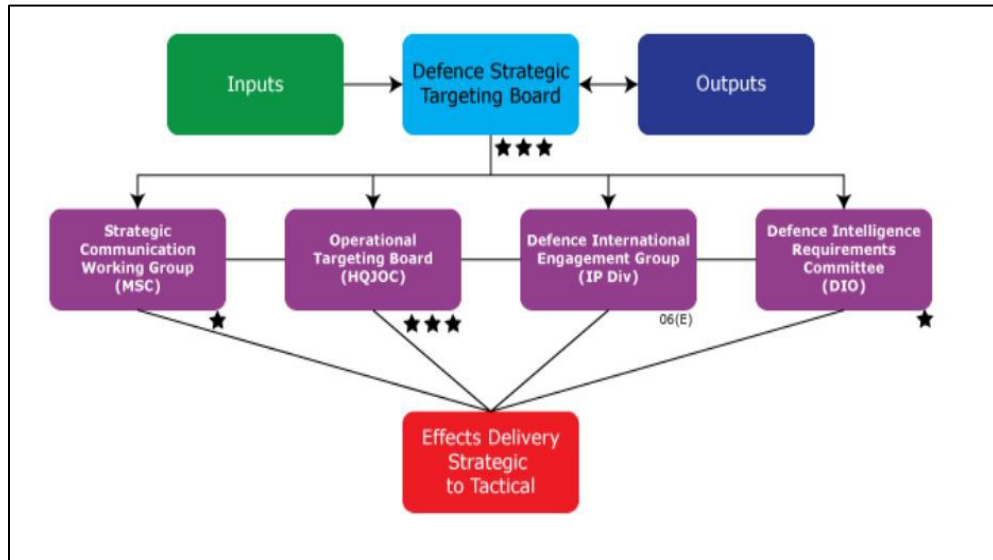


Figure 26. Coordination of Information Activities

Source: Australian DOD 2013.

The Intelligence and Security Group is headed by the Director Australian Signals. He is responsible for coordinating, as the national authority on information security; the development of information security policy; the provision of general advice and assistance on broader network security issues, as well as high grade and other forms of cryptography; and the formulation of guidelines for best practice architectures and monitoring regimes. Deputy Secretary Intelligence and Security is responsible for intelligence support to information activities.

Architecture at the Operational and Tactical Level. The Service Chiefs are responsible for the generation and sustainment of physical information-related capabilities. At the tactical level, the Australian Army follows a similar approach like other NATO armies. There are IO staff integrated at every level of HQ. The IO staffs are responsible to suggest the commander at different level to provide advice related to IO. According to the Australian doctrine the IO are the operational level, planning and execution of information activities and operate on the will, understanding and capability of an intended audience (Australian DOD 2013). Just like all other NATO doctrine the central idea of Australian IO doctrine is that IO includes both influencing the decision making of actors while protecting our own information and decision making. The IO activities includes:

1. Shaping and influencing (at the strategic level);
2. IO (at the operational level); and
3. Inform and influence actions (at the tactical level).

Therefore, it is evident that the Australian doctrine advocates that the execution of the IO be at the operational level. According to the doctrine, the provision of intelligence support to IO planning, including:

1. Nodal analysis products as required.
2. Psychological activities.
3. EW.
4. Physical Destruction.
5. Deception.
6. Operations Security.

7. Advice and warnings on security threats to materiel and personnel.

Russian Doctrine

The Russians are one of the successful practitioners of the IO concept in the present time. In fact, The Russians have integrated this approach for centuries in their military and political concepts. Historians had traced the strategy as far back as 1380 when Prince Dmitry Donskoy and 50,000 Russian soldiers defeated the so-called Golden Horde of 150,000 Mongolian warriors in the Battle of Kulikovo. Donskoy's men claimed victory thanks to a surprise attack by a regimen of soldiers hidden in a nearby forest (Elliott 2018). Russia spends approximately \$400–\$500 million per year on foreign information efforts, while the U.S. spends USD 20 million on Russian language services. From these statistics, it is easy to understand that Russia is more focused on IO (Koshkin 2015). Russia's information tools for convincing an audience are rich and varied and include historical myths, narratives, and symbols. The purpose of which is to convince or disorientate the target audience.

The Russians have developed it under a doctrine called "Maskirovka." The meaning of the word "maskirovka." means masking, and it is a fitting name for a tactic, that depends entirely on misrepresentation and disinformation. Maskirovka has persisted as a strategy from the Russian Imperial Army days, to the era of the Soviet Union, and up to today under Vladimir Putin. However, the three elements involved remain the same: distract your opponent, disguise what the military is really doing and spread disinformation to sow confusion and delay a response. A present study reveals the components of Maskirovka are surprise, camouflage (Kamufliazh), a maneuver intended to deceive (Demonstrativnye manevry), concealment (Skrytie), the use of decoys and

military dummies (Imitatsia), disinformation, a knowing attempt to deceive (Dezinformatsia) (Ash 2015).

In recent conflicts, Russia has proven itself adept at using disinformation and misinformation, as well as combining the technical and psychological aspects of IO, to advance their political aims. The competing superpower like Russia and China to balance their asymmetry with the US, have been conducting a series of attacks against Governmental computer systems. The Russians have conducted cyber-attack on Estonia, and the Chinese have attacked the U.S. and Japanese economic system (Black 2013). Over the time since the cold war Russia have proven themselves adept at both the technical and the psychological aspects of IO integrating the platforms on social media.

The Russian understanding of IO relates to the application of soft power as a tool of political warfare and foreign policy. The Russian foreign policy concept notes the ‘illegal’ use of soft power and human rights concepts to put pressure on sovereign states, intervene in their internal affairs, and destabilize them by manipulating public opinion (Monaghan 2012, 6). As part of the IO Russia Conducts political warfare, which consists of three components: foment, seize and consolidate. Therefore, the Russian doctrine considers the exercise of IO campaign as a part of their foreign policy. According to Russian doctrine, cyber effects must pursue the same strategic, operational, and tactical purpose as the maneuver campaign they support. Unsurprisingly, Russian writing on information confrontation continues to evolve, a testament to the strategy being dynamic and fluid much like the domain in which it is applied (Iasiello 2017).

Chapter Summary

The present-day battlefield will be unleashed through the exercise of soft power in the information domain at first. Arguably, the IO is the most effective tool to achieve informational dominance and superiority over the adversary, which often helps to win the war without fighting on the ground. Over time, the theme of IO has evolved significantly from C2W, IEW, and IW to IO. However, central understanding remained mostly unaltered. According to most of the doctrine, the information dimension is inherently composed of Physical, Informational, and Cognitive dimension (HQDA 2013).

Embracing the cognitive dimension, the horizon of IO got even larger. Down the intelligence channel, Counter-deception, counter-propaganda, counter-intelligence are also essential tools. The IO therefore, always supported by intelligence and tailored to multi-source IW. Major deductions that can be drawn from the preceding international doctrinal discourse are listed below:

1. The broad IO concept revolves around the physical, informational and cognitive dimension.(Figure 27)
2. The physical dimension is related to physical equipment, systems, and processes such as the Commander/Leader, C2 System, Computer System, etc.
3. The cognitive dimension shapes the perception of the target audience/ organization/ leadership to influence the mind of the decision maker and create the desired effects. The tools are PSYOP, MILDEC, C2W, and predominantly intelligence-led operations.

4. The informational dimension of IO (the focus of the research) affects the content and flow of information. The tools of IO (peace and war) in general and IW (wartime only) in particular, are EW and Cyber Operations or CNO.

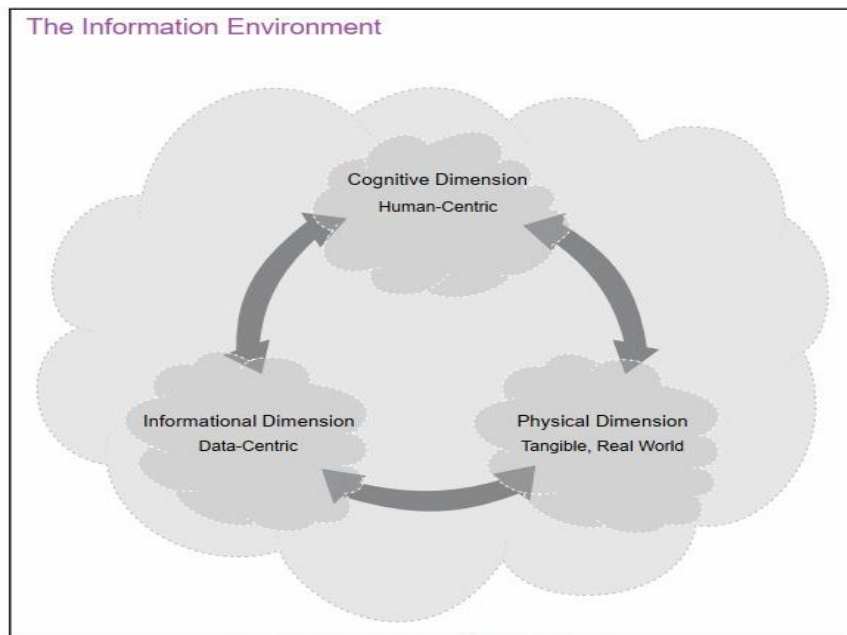


Figure 27. The Information Environment

Source: CJCS 2012, I-2.

From the analysis of all the doctrines and organizations of different armies, it is evident that all of them have highly focused on establishing a good architecture. To establish a functional framework for the conduct of IO for the Bangladesh Army, it is imperative to incorporate good methods and practices. The following paragraphs will suggest a few recommendations for the Bangladesh Army to start with an IO architecture. Some of the recommendations will be related to technical aspects, and some of the recommendations will be related to organizational aspects.

Recommendations to Establish an IO Architecture for Bangladesh Army

Integration at the National Level

First, IO is not to be conceptualized in isolation as purely military tasks, but as part of an integrated task shared by the military and civilian state and non-state actors. In the context of a comprehensive information strategy, the integration at the national level will be the first requirement, and the military should operate under the umbrella of the national institution. Like many other countries, Bangladesh needs to establish a National Center for information strategy. This organization will maintain cross-government civilian and military representation and directly advise the Prime Minister. The Bangladesh Army has a wide range of deployment all over the world for the UN mission. This organization will also collect and analyze information of those countries and provide to the military for their preparation before deployment. Within the military, the IO should not be considered as a task of the Army Signal Corps alone; instead, it should be considered a task for all the arms and services. Every layer of the organization should be responsible for coordinating all military agencies with national intelligence agencies. Figure 28 shows how all the systems are interlinked for the IO.

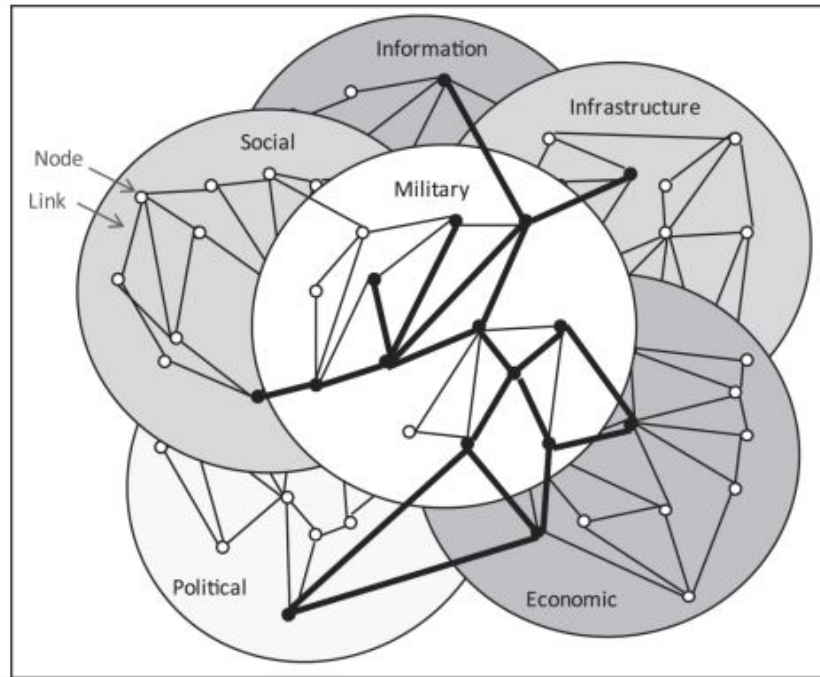


Figure 28. Linkage between System

Source: HQDA 2013, 5-24.

Integrating IO Architecture Organizationally

According to Forces Goal 2030, the Bangladesh Army will enhance its capability for dealing with the information domain. There is a need for a separate IO cell working from Division down to AHQ and AFD level to adequately addressing the intelligence, operations, and technical needs. Integrating IO by establishing an IO-specific battalion would include companies focused on specific information-related capabilities (i.e. Civil Affair Company, Public Affair Company, Cyber Company, and Psychological Warfare Company). Such a battalion would be a single focal point for capabilities and resources for the incorporation of IO in every corps. Alongside, each division headquarter can also

have an IO branch with specialists. Such established structure will allow developing the Army to retain and improve institutional knowledge, refine, improve training availability to IO practitioners, and solidify the place of IO institutionally. A suggested diagram is shown in Figure 29.

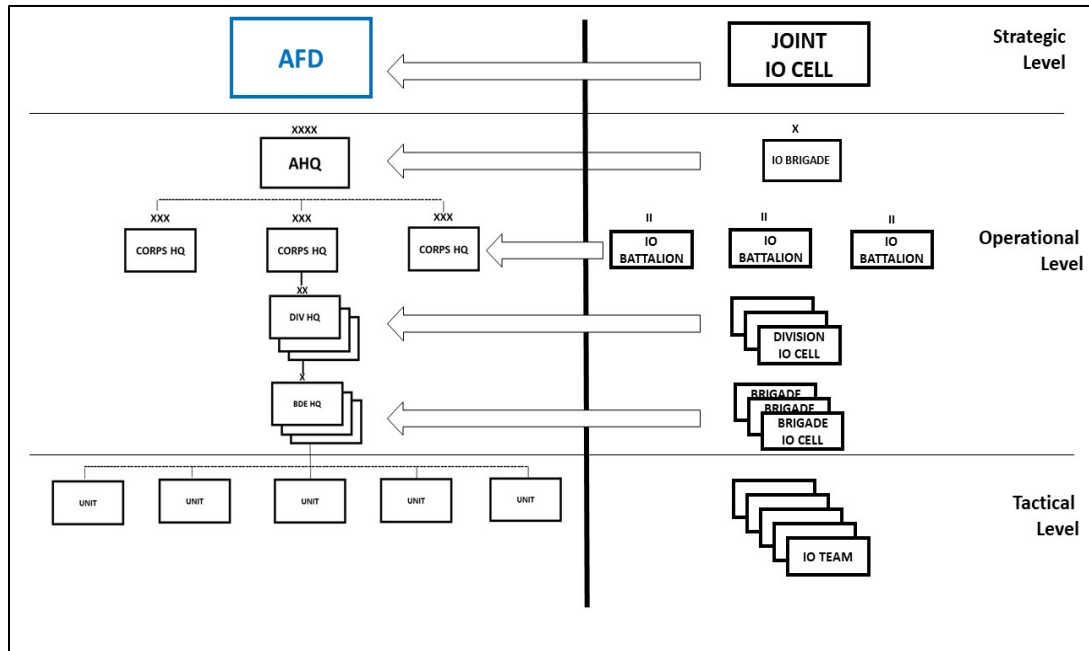


Figure 29. Proposed IO Architecture for Bangladesh Army

Source: Created by author.

Establishing an IO Brigade under the Army Headquarters

In most of the armies, there is a designated formation for dealing with the IO. As an example, the British 77th Brigade and the 1st Intelligence Surveillance and Reconnaissance Brigade (1st ISR), and the U.S. the 1st Information Operations Command (Land). From the analysis of the rest of the armies, it was revealed that there is

a dedicated organization to deal with IO affairs. Bangladesh Army needs to establish a similar brigade which will directly operate under the AHQ and provide IIA capabilities to all the under command units. This unit can be named as the IO Brigade (IOB) This formation will work in coordination with the AFD and will be responsible for establishing IO body at division, brigade, and unit level.

Formulation a Viable Command and Staff Network

From the AFD down to the unit level at every layer, there should be proper integration of staff structure. These IO experts will provide advice to the commanders in regards to the IO affairs. There should be a joint IO cell at the AFD (which is the HQ responsible for the Joint Operation in Bangladesh). This cell should provide advice to the Principal Staff Office (PSO) in AFD. They should also be responsible to coordinate affairs related to IO down to operational and tactical level. At the AHQ, the IO Brigade should provide the necessary staff to advise the Chief of Army Staff (CAS). At the operational and tactical level in each corps, division, and brigade, this IO Brigade should establish necessary cell to perform all IO related affairs. A suggested structure for the staff organization is illustrated at Figure 30.

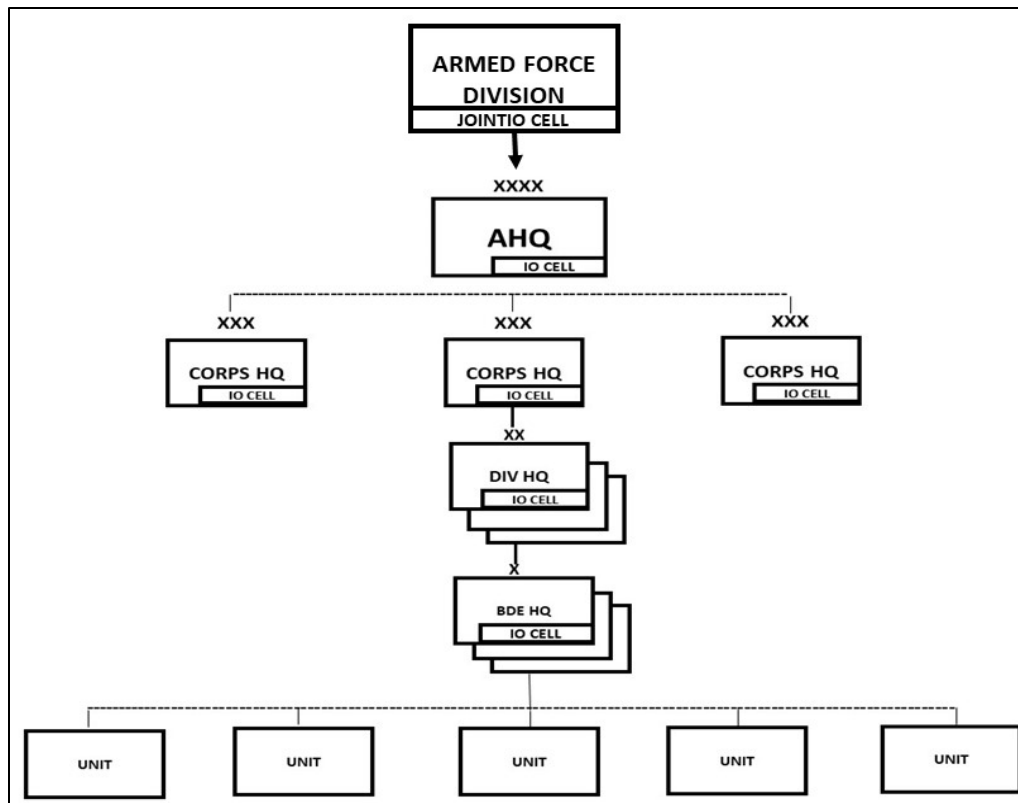


Figure 30. IO Command and Staff Structure

Source: Created by author.

Introducing the IO as a Career Field for the Officers

The U.S. Army has different functional areas assigned to the officers, which enables them to be proficient in that particular field of operation. Individual officer in the army can choose his career path in that field. In the U.S. Army, the IO is a functional area for the officers. The Army IO officers (functional area 30 through the command's IIA section) serve as the integration specialist for the U.S. Army (HQDA 2013). The Bangladesh Army officially does not categorize such functional area. However, Military Secretary Branch (MS Br) plans officers in the different carried field. In the Bangladesh

Army, all the officers are trained, and posted according to their specialization. The IO officer can be also included in the specialization category for the Bangladesh Army. Therefore, an officer will be trained and prepared in the field of IO throughout his career and generate the best output while discharging his duties.

Conversion of Soldiers to Information Operations (IO) Trade

One of the major findings of the research is in most of the modern armies; the IO was established as a separate trade. At present, the Bangladesh Army, Signal Corps is solely responsible for dealing with the communication and ICT related affairs. However, the army needs to establish IO/ ICT as a separate trade where the soldiers can be enrolled and can be retained for the entire duration of their service. The soldiers can be absorbed in IO as a conversion trade after attaining certain qualifications defined by IT Directorate. AHQ will centrally maintain the database of these qualified soldiers. A model is described in Figure 31 as a suggestion.

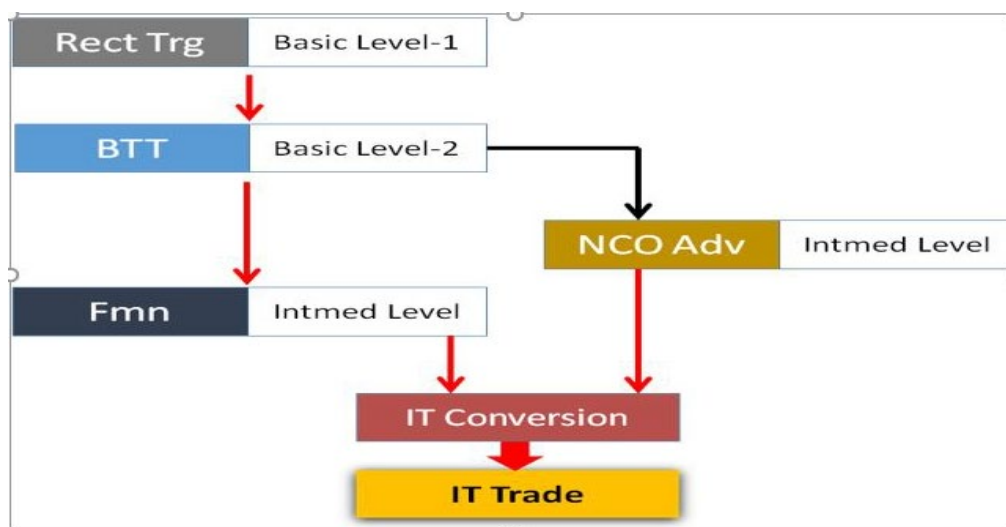


Figure 31. The Procedure of Conversion to IO Trade

Source: Created by author.

Developing an Information Operation Doctrine

For most of the armies, IO doctrine has been developed very recently. A comparison of the more than 20 extant IO doctrines of various NATO states shows that there are different approaches to deal with the concept. Only a few countries have the political determination or capabilities to apply the entire range of instruments. Most importantly, it requires extensive economic backup. In addition, the majority of countries attribute greater importance to defensive measures than to possible offensive operations (CSS Analyses in Security Policy 2008, 2) Therefore, Bangladesh Army should primarily focus on developing an IO doctrine giving priority to defensive IO (cyber defense, operational security, and media affairs). Figure 32 explains the doctrinal IO Architecture of U.S. military:

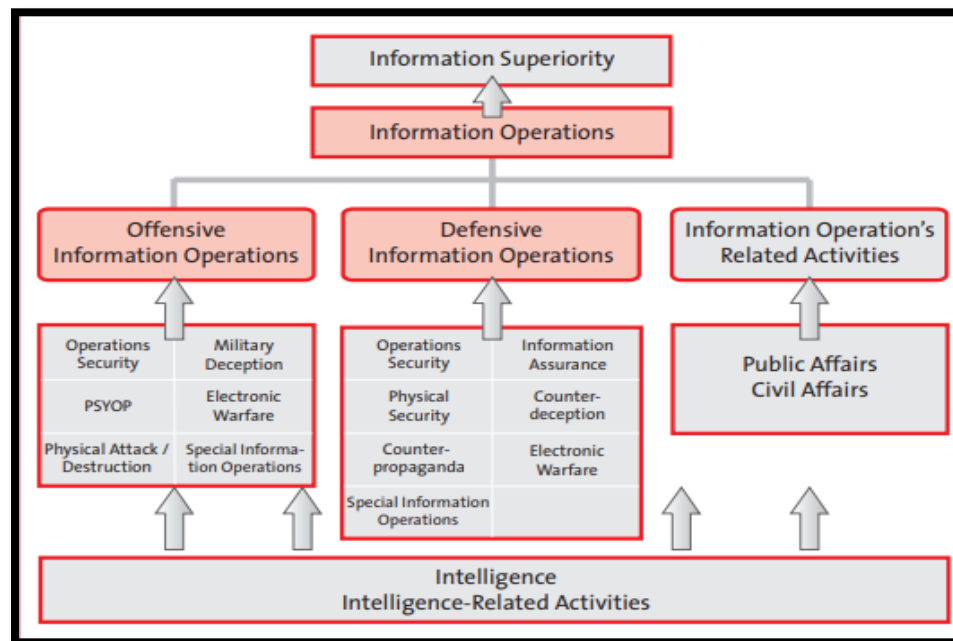


Figure 32. Information Operation according to U.S. Doctrine

Source: HQDA 2013.

Establishing a Training Facility for Imparting Institutional Training

Sophisticated and cutting-edge technologies dominate the information domain. The evolution of technology is happening every moment. Therefore, such a delicate task cannot be understood, and handled by a group of unprofessional. The very nature of the IO demands the establishment of a dedicated organization and a core group of professionals, who will be consistently working on the information domain. For the soldier and leader development, there should be a dedicated training institution to educate the IO community operating for the Bangladesh Army. Like military intelligence (MI) and military police (MP), the IO can also be introduced as a career field. The Bangladesh army can establish a training facility for IO in the School of Military Intelligence or even in the School of Infantry and Tactics.

Material Acquisition for Information Operation

The establishment and operation of IO architecture demand incorporation of many high-end latest electronic gadgets and equipment. Point to note that the IO includes cyber and space. Therefore, it is likely to be extremely costly. Therefore, the military should allocate a substantial amount of money from its annual budget for the establishment of the standing IO capacity. The army can also enhance its ability by integrating the capabilities of the Bangabandhu-1 satellite. The initial setup will be costly; however, gradually to cost will come down. Keeping that priority in mind, the Bangladesh Army should allocate budget for its force development accordingly.

Policy Development

There should be a well-formulated policy, which will help the army to operate safely in the information environment. Policy related to every information related capability needs to be formulated. There should be strict protection from fake news and cyber propaganda against the country. Alongside, there should also be strict vigilance to monitor, regulate, and enforce the related policies. However, existing policies may be amended to provide better integration among all the information related capabilities.

Develop a Defensive IO Architecture

The Bangladesh Army should develop a defensive IO architecture. For the Bangladesh Army, the defensive IO will integrate and coordinate all policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive IO is conducted through information assurance, OPSEC, physical security, counter-deception, counter-propaganda, counter-intelligence, EP/ECCM with limited/ focused EA. Defensive IO is supported by intelligence and tailored, multi-source IW. Defensive IO ensures timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their purposes. Offensive IO also can support defensive IO. Defensive IO ensures the necessary protection and defense of information and information systems upon which forces depend to conduct operations and achieve the objective.

Four interrelated processes support defensive IO: information environment protection, attack detection, capability restoration, and attack response. Since they are so interrelated, full integration of the offensive and defensive components of IO is essential.

IO can be depicted as attempting to influence, disrupt, corrupt, or usurp adversarial human or automated decision-making while protecting friendly decision cycle. The assurance includes the following component properties and capabilities: Availability, Integrity, and Authentication based on controls: (1) authorization (granting and revoking access rights), (2) delegation (extending a portion of one entity's rights to another), and (3) user authentication (reliable corroboration of a user, and data origin). Typically, objectives of CND or Cyber Defence is achieved in layered secured network architecture (Figure 33).

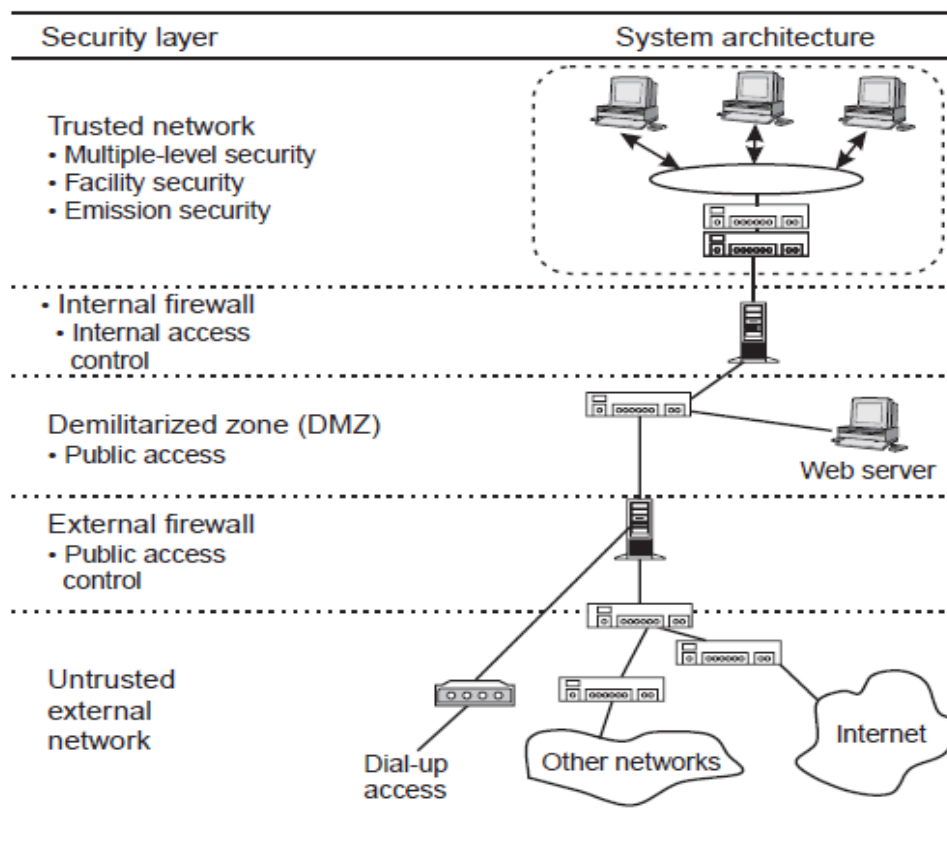


Figure 33. Typical Commercial Multiple-Layer Network Security Architecture

Source: Created by author.

Establishing Active Directory

The first thing the Bangladesh Army needs to do is separate its military network from the daily common user network. Preparation of Active Directory by the Bangladesh Army is now in the process, which will improve the authentication and enable access control to the Bangladesh Army network. Common access of the unsecured computers to the Army Network should be prohibited. This will facilitate centralized logging and monitoring to the network and centrally update. There should be a restriction on the use of removable devices and on installing or uninstalling of unsafe software. Considering the internet as a security threat for the Bangladesh Army network, new projects should be undertaken to develop an independent wireless network for daily office works, which will be separated from the military network and physically separate internet from the Bangladesh Army network.

Chapter Conclusion

In order to achieve the dominance in battlespace awareness, today's fragmented command, control, decision making actions, and all activities related to warfare should be more focused, efficient, and effective to ascertain the common goal. Most modern militaries in the present world are increasingly becoming dependent on information dominance as the key to victory. A Harvard paper published in 2017 estimated that the Chinese government employs two million people to write 448 million social media posts a year. Their primary purpose is to keep online discussion away from sensitive political topics (Miller 2018). This signifies how much importance some of the armies give for the conduct of IO. Disinformation and deception have been a part of warfare for thousands of years, but across the world, something new is starting to

happen. Therefore, it is very important for the Bangladesh Army to establish an architecture for IO.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Chapter Introduction

Information Operations is increasing in importance across all domains in military, political, industrial, and social environments. The nature of warfare is changing. It is no longer just about who has the larger military, but is also about who has the best information regarding the battlefield; to include all actors be they state or non-state, combatant or non-combatant, military or civilian (Arquilla and Ronfeldt 1997). The information domain and information conflict have blurred the boundaries between peace, conflict, and war (Ehrhart 2017). In today's battlefield, all facets of military operations rely primarily on the use of electronics primarily engaged in the information domain. Since operations are intricately and increasingly associated with modern gadgets, warfare is becoming more dependent on IO than any other elements of military power. It is, therefore, that every army be able to operate freely in the highly saturated informational domain. Hence, it is imperative for any military organization to understand the prevailing information environment to identify specific sectors that are vulnerable to information breach, manipulation, and exploitation.

Gerasimov describes that, the world moves toward conflicts in which "Wars are not declared but have already begun," (Darczewska 2014). Disinformation and deception have been a part of warfare for thousands of years. Therefore, the concept of IO is not something new. However, with the new technological developments across the world, a new method of warfare is going on. Information is one of the elements of national power, and different nations have long been using it to support combat operations, but now the

conflict is taking place primarily, sometimes exclusively, through it. In the past, the information was used as a tool of warfare, which has now become a domain of warfare. It is not only confined to the developed countries like U.S., Russia, or China but also it is used by most of the underdeveloped nations as well. Scholars opine that a global informational struggle has broken out. Dozens of countries are already doing it. We only come to know about the use of IO through the campaigns that are conducted by those countries (Miller 2018).

Conclusion

Bangladesh is one of the rapidly developing Countries of the world, and it is moving fast towards the digitization of society with the vision of ‘Digital Bangladesh’ (Islam 2018). At present, Bangladesh is not on the list of highly vulnerable countries concerning information domain. The banking, telecommunication, education, air communication and business sectors of Bangladesh are increasingly adopting technological advantage. It is observed that within the last few years, Bangladesh made most of the service sectors computerized. The more a nation gets digitized and automated, the more vulnerable it becomes to information attacks. Thus, the future networked society would increase the vulnerabilities to this type of warfare in the years to come. Vital national economic interest, information infrastructures, and national psyche now assume more significance in the context of overall national security perspective.

To achieve the national objective the information remains as one of the most important and vulnerable assets. These objectives may be economical, diplomatic, or even military. In the present globalized world, economic objectives are the prime focus of every nation, which depends on uninterrupted and timely access to correct information.

Hence, all the diplomatic or military efforts are diverted to obtain information and at the same time, protect their own information from any attack. In fact, this tendency has led to the warfare of information in this digital age. This is likely to be even more noticeable in future conflicts, in which IO will play a more significant role. The emergence of the concept of IO may be traced primarily to the information revolution that has affected most of the military across the globe. IO is 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 (HQDA 2013).

It is challenging to anticipate the future field of warfare. The rapid and vast development of technology vis-à-vis weaponry system made the future battlefield critical and confusing. Thereby it is predicted that in the future, IO will destroy the enemy's will to fight, primarily dealing with command control communication and information (C3I) with vast technological advancement. It is evident that in the future, information is likely to appear as a weapon rather than a tool that is supporting traditional kinetic weapons through information data. Thereby someone may imagine that the trends in future wars likely to be violent military and non-violent wars. These will have similar types of combat, but of greater magnitude.

The rapid development of technology has changed the method and made an enduring impact on every war-fighting concepts. The most significant changes that IO has brought in the process of warfighting is the development of NCW. The future battle is likely to be more chaotic, intense, and highly destructive and will be of high intensity. The characteristics of the future battlespace are likely to be highly lethal,

expanded battlefield, wide dispersion, use of WMD, hybrid adversaries and threats, and unconventional warfare, NCW, Space and Precision, Joint Operations with Greater Mobility, EW with Psychological Effect and dominated by technological development. Battle will be fought in greater depth due to the increase in strategic reconnaissance and surveillance. Space will be emerging as the center of gravity of modern warfare.

While assessing the threats and vulnerabilities of the Bangladesh Army, EW capability of neighbors was studied. The neighboring countries significantly use IO for the conduct of their military operation. Those Armies have evolved doctrine for integrating various components of IO with an IW doctrine. Most of them have capabilities of assisting the commander in commanding its troops and controlling its weapons. At the west, the U.S.'s individual command, services, and agencies in DoD traditionally developed their IO architectures. There are many similarities in the IO doctrines of the NATO countries. Among the NATO countries, the UK Army is right now very efficiently organized to conduct IO. Other NATO countries expert in IO are Canada, Germany, and France. However, one thing common, to the study of all the doctrine of all those armies is they all highly value the IO.

The neighboring countries significantly use IO for the conduct of their military operation. Those armies has evolved doctrine for integrating various components of IO with an IW doctrine. They have capabilities of assisting the commander in commanding its troops and controlling its weapons. At the west, the U.S.'s individual command, services, and agencies in DoD traditionally developed their IO architectures. There are many similarities in the IO doctrines of the NATO countries. Among the NATO countries, the UK Army is right now very efficiently organized to conduct IO. Other

NATO countries expert in IO are Canada, Germany, and France. However, one thing common, to the study of all the doctrine of all those armies is they all highly value the IO.

On the other hand, the operating procedure for IO for Russian and Chinese Army differ from western methods. IO concept for Russia focus on acquiring information on the opponent and the conditions of the conflict, collection, and processing of information and intelligent C2 systems to organize and conduct combat actions. A

Harvard paper published in 2017, estimated the Chinese government employs two million people to write 448 million social media posts a year. Their primary purpose is to keep online discussion away from sensitive political topics (Miller 2018). Countries such as Russia, China, and to a lesser extent Iran, are using IO as a way to gain an asymmetric advantage over the much larger U.S. military. Information activities have become an ingrained feature of modern warfare, not just for cyber-empowered militaries such as that of the US, China, and Russia, but for low-tech forces. Therefore, it is imperative for the Bangladesh Army to adopt and integrate the IO to gain an asymmetric advantage over its potential powerful adversaries.

With the increased dependency on information, spectrum forces across the world are gearing up for the battle of the fifth dimension, i.e. cyberspace. IO based future warfare will have dominating maneuver over adversaries in terms of finding out accurate positioning of forces and will ensure getting logistic support to the right place at the right moment. The Bangladesh Army has started its preparation to conform to the future warfighting trends and adopt a Forces Goal 2030 to transform it into a modern, efficient and time-befitting force. Bangladesh Army has acquired quite significant technological

advancement in the field of ICT. The recent launch of a Bangabandhu satellite has also increased the capability of the country in the information domain (Times of India 2018).

In pursuit of professional excellence and growth, Bangladesh Armed Forces also developed “Forces’ Goal-2030” the Bangladesh Army kept the GoB’s concept of ‘Digital Bangladesh’ in the peripheral vision while developing the army’s forces goal.

Accordingly, the Bangladesh Army raised few IO related organizations in 2012, but threadbare threat analysis, risk, and vulnerability assessment followed by operational IO doctrine is not formulated yet. The intricate integration of intelligence, operations, and technology (ICT) makes IO complicated especially in terms of the complex C2 arrangement. It becomes complicated not only within the army, but also in the joint service level and national level as well. Hence, it is necessary to empirically examine whether the absence of a viable IO structure in the army poses a threat to information security or not. If it does possess security threat, then the Army should try to identify cardinal facets of IO structure for consideration of the Bangladesh Army.

Bangladesh Army has little experiences of dealing with organized IO in the information environment. Probable IO architecture of the Bangladesh Army demands integration of various elements to the system (Operational architecture, system architecture, and technical architecture). To establish an architecture, it also demand the integration of different elements into the system of IO, such as military deception (MILDEC), Military Information Support Operations (MISO), soldier and leader engagement, including police engagement, Civil Affairs (CA) operations, Combat camera, Operational Security (OPSEC), Public affairs, Cyberspace Operations, EW. All of these elements should be integrated into the newly established IO architecture for

Bangladesh Army. The information environment consists of three interrelated dimensions, known as physical, informational, and cognitive. Actions in the information dimension affect the content and flow of information by denial, manipulation, corruption, and exploitation. As the system will expand with the advancement of modernization. Hence certain standards on the platform should be made a benchmark for future integration. National fiber augmented by microwave backbone can be used as a core backbone to support adequate bandwidth in the field for integrated voice, data, and video.

From the analysis of the doctrinal sources, major findings were beneficial to suggest an architecture for the Bangladesh Army. The study showed that the broad IO concept revolves around three dimensions, those are the physical, informational, and cognitive dimension. From the analysis of all the doctrines and organization of different armies, it is definite that all of them established a good structure to support the IO. As a beginning point to start IO, the Bangladesh Army needs to establish a functional framework. To meet that goal, it is imperative to incorporate the good methods and practices. The U.S. Army and the British Army has dedicated formations to deal with IO. The IO organizations are nested from the national down to the tactical level for achieving a synergic effect. The following doctrinal publications were analyzed for the research:

1. The U.S. Army doctrines.
2. The British Army doctrines.
3. The Canadian Army doctrines.
4. The NATO doctrines.
5. The Australian Army doctrines.

The findings of the research show that the implementation process of IO architecture will take a long time, modern equipment and huge amount of budget. Therefore, many challenges are likely to be faced during the implementation phase for establishing the operational architecture, system architecture and technical architecture. However, the technical aspects were kept out of the preview of the research. Some of the challenges are the mind set up of soldiers and officers, standardization of training, the involvement of huge budget and longtime planning, ensuring the security of the system and network, dependency on networking, hardware, and software, and others. For smooth implementation of the system all, those hurdles are to be addressed appropriately. Therefore, the goals should be set as immediate, intermediate, and in the long term.

There is a provision of establishing Brigade size IO organization in the Forces Goal-2030. One of the battalions will look after the aspects of combat intelligence and counter-intelligence. Whereas PSYOP, Deception, and Information/Cyber Warfare will be dealt with by some another Battalion of that brigade. There is a need for a separate IO cell working from Division down to AHQ and AFD level to effectively address the intelligence, operations and technical needs. With some basic equipment, some pilot project should be planned to test to-be-procured IO gadgets along a single Brigade-Division-AHQ axis. While the need for formulation of IO doctrine was unanimously endorsed, the majority of the respondents opted for the development of defensive doctrine at first, giving due priority to OPSEC, Cyber defense, and EP/ECCM, ESM. Majority of the experts opine that, a mix of wheeled and man-portable EW system should be procured for the army and think that concurrent development of IO doctrine, IO training, and procurement should be a way forward for Bangladesh Army.

Information awareness and perceptions gained from analysis of collected information and personal observations have long been an integral part of human existence; those with a superior ability to gather, understand, control and use information have gained a substantial advantage (NATO 2009). The ability to manage and employ information underpins activities across all elements of national power. From the strategic to the tactical level and across the range of military operations, information plays a vital role in the manner in which decisions are made. Applying IW theories in today's geopolitical climate remains a work in progress. An around-the-clock news cycle and the various ways of disseminating and consuming information worldwide makes implementing information-based operations and tailoring messaging against competing narratives' challenges. As observed in Georgia, smaller nations can competitively control information and influence target audiences to at least mitigate the efforts of, if not defeat, larger nations.

An integrated national policy along with short and long-term programs may reduce the IO threats and vulnerabilities substantially. The effective and coordinated effort of civil, military, private and media will increase the advantages, and opportunities of Bangladesh in this technological arena. However, defense against the threats related to the information domain is a continuous process. The military should, however, give policy guidance and set up IO committee for defense against IO. For future security and military strategy formulation, the government must take two active considerations of the fact of IW. The Armed Forces, on the other hand, should prepare for future war by initiating its education and training program on the subject.

Recommendation

1. Bangladesh Army should recommend to Ministry of Defense (MOD) to establish a National counter information strategy and center. The organization will be maintaining cross-government civilian and military representation and will be responsible for directly advising the Director of National Intelligence. Furthermore, this center needs to collaborate with national security stakeholders to develop unique strategies for each state and nonstarter actor.
2. In the context of a comprehensive information strategy, IO should be properly integrated at the national level, and the military should operate under the umbrella of the national institution.
3. A policy should be formulated for protecting the information domain against fake news.
4. The MOD should implement a strategy for educating the public as well as identifying and reporting fake news.
5. A cell under the Military Intelligence School should be established for an initial period and later there may a separate school established to provide institutional training on IO.
6. The Bangladesh Army Training and Doctrine Command (ARTDOC) may carry out an analysis to formulate a policy so that officers and other ranks of different arms and services can be prepared and posted to perform in different IO fields. IO should be introduced as a career field for the officers.
7. A separate Directorate in the AHQ may be established for IO under the General Staff branch.

8. ARTDOC may carry out detail study of different doctrines and formulate doctrine related to IO for Bangladesh Army.
9. Separate IO branch may be integrated from Division down to AHQ and AFD level. (The proposed architecture is shown in Figure 22 in Chapter 4)
10. Commanders should have the flexibility to organize their staff structure for IO depending on the mission, requirements, strengths, and weaknesses. When operating in a joint or multinational environment, commanders may reorganize its staff to better align with higher HQ.
11. The Bangladesh Army may establish an IO Brigade under the AHQ to provide the specialist related to IO for all the corps and divisions in future.

Recommendations for Future Research

This research was limited by comparing and contrasting between different doctrines, which were available as open sources. There was no survey conducted for the research due to time and resource constraint. Any study or physical interview outside Fort Leavenworth was not conducted for the research. Hence, the research was qualitative in nature. This thesis did not examine the entire spectrum of the DOTMLPF-P characteristics for more effective integration of IO. Additionally, the research only carried out an in-depth study regarding the doctrinal and organizational aspects of different armies. However, the technical aspects, budget, policy formulation, training, the material acquisition was kept out of the preview of the research. This research was also limited to only English language sources. Last but not the least, the financial implications and IO technical architectures were also kept beyond the purview of this research.

Following are the recommendation for future research:

1. Policy development for the integration IO in the Bangladesh Army.
2. Material Acquisition for the integration of IO for the Bangladesh Army.
3. How to integrate a doctrine for the IO of Bangladesh Army.
4. Methods on how to establish IO education and training institution for the Bangladesh Army.
5. Financial management for the integration of IO organizations for the Bangladesh Army.
6. IO conducted by China and lessons for Bangladesh Army.
7. Further classified research can be carried out covering the classified doctrines of different armies.

Closing Thoughts

IO is the new magical instrument, which enables a military force to win a war or avoid a confrontation through information superiority and without physical fighting on the ground. According to the famous historian and military theorist, Captain Sir Basil Liddell Hart in his book 'Thoughts on War,' "The real target in war is the mind of the enemy commander, not the bodies of his troops." With the proliferation of IT, the IO is regarded today as an integral part of warfare. At present, the media and the cyber is used and conceived as a weapon not just theoretically, but in every conflicting situation. Most of the armies are now establishing a separate body to deal with media, cyber as a whole IO.

The importance of IO cannot be overstated. The IO does not confine itself to the boundary of a nation, or with only its adversaries; instead, it spans over the entirety of the global affairs. Now there are ideas like 'Facebook War Room,' that indicates the

spectrum of IO is much more than what can be imagined. IO has evaporated the thin line between the combatants and non-combatants. The information environment is ever changing. The art of information confrontation must be practiced and refined over time, and tailored to specific audiences. Therefore, the Bangladesh Army should institutionalize the IO as soon as possible.

GLOSSARY

Electronic Warfare (EW). EW is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (US JP 3-13.1). EW consists of three divisions: Electronic Counter Measure or Electronic Attack (ECM/ EA), Electronic Counter Counter-measure or Electronic Protection (ECCM/ EP), and Electronic Support Measure (ESM/ ES). Figure 4 explains the method of EW in integrated IO (CJCS 2006b, 11).

Information Environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. Conceptually, the information environment encompasses both tangible (physical) elements and intangible elements (such as human ideas, fears, perceptions, and decision-making (CJCS 2012, 6).

Inform and Influence Activities (IIA). The integration of designated information-related capabilities in order to synchronize themes, messages, and actions with operations to inform the United States and global audiences, influence foreign audiences, and affect adversary and enemy decision making (HQDA 2017, 6).

Information Operation (IO). 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. Also called IO (HQDA 2014, 7).

Information-Related Capability (IRC). A tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions. Also called IRC. (Approved for inclusion in JP 1-02.) Designated information-related capabilities that support inform and influence activities (IIA) and its lines of effort typically include, but are not limited to, public affairs operations, military information support operations (MISO), combat camera, soldier and leader engagement, civil affairs operations, civil and cultural considerations, operations security (OPSEC), and military deception (CJCS 2006a, 7).

Information Warfare (IW). IO is conducted during the time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries and also called IW. Information Warfare is any action to deny, exploit, corrupt or destroy the enemy's information and its functions; protecting ourselves against those actions and exploiting our military information functions (CJCS 2006a, 8).

Influence. The act or power to produce a desired outcome or end on a target audience (CJCS 2012, 9).

Influence Operations. Operations focused on affecting the perceptions and behaviors of leaders, groups, or entire populations. Influence operations employ capabilities to

affect behaviors, protect operations, communicate the commander's intent, and project accurate information to achieve desired effects across the cognitive domain (CJCS 2012, 9).

Message. A narrowly focused communication directed at a specific audience to support a specific theme (CJCS 2012, 11).

Operations Security (OPSEC). OPSEC is a process that identifies critical information to determine if adversary intelligence systems can observe friendly actions, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information (CJCS 2012, 11).

Psychological Operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives. Psychological Operations is also called Military Information Support Operations (HQDA 2006, 12).

Recruitment. To seek out, evaluate, obtain a commitment from, place, and orient new employees to fill positions required for the successful conduct of the work of an organization (Andrews 1988, 12).

Signal Intelligence (SIGINT). The generic term SIGINT is used to describe communications intelligence (COMINT) and electronic intelligence (ELINT) when there is no requirement to differentiate between these two types of intelligence. Technical and intelligence information derived from EM non-communications transmission (e.g., radar, navigational aids, jamming transmissions) by other than intended recipients are known as ELINT. Technical and intelligence information derived from EM communications and communications systems (e.g., Morse, voice, teleprinter, facsimile) by other than intended recipients are known as COMINT (Canada DND 2004, 12).

REFERENCE LIST

- 1st IO Command. 2019. "1st IO Command." U.S. Army. Accessed 06 February 2019.
<https://www.1stiocmd.army.mil/Home/index>.
- Ali, LTC Abu Sayeed Mohammad. 2010. "Trends of Future Warfare and Options Available." Master's Thesis, Bangladesh Army.
- Allen, Patrick D. 2007. *Information Operations Planning*. Norwood, MA: Artech House.
- Andrews, Yvonne. 1988. *The Personnel Function*. Pretoria: Pearson South Africa.
- Arquilla, John, and David Ronfeldt. 1997. *Cyberwar is Coming*. Santa Monica: RAND Corporation.
- Ash, Lucy. 2015. "How Russia outfoxes its enemies." *BBC News*, 29 January. Accessed 26 March 2019. <https://www.bbc.com/news/magazine-31020283>.
- Bassford, Christopher. 1993. *Jomini and Clausewitz-Their Interaction*. Atlanta, GA: Georgia State University.
- Black, Jeremy. 2013. "Into the Future." In *War and Technology*, 245-263. Bloomington, IN: Indiana University Press.
- Bleyder, K. 2012. *Cyber Security: The Emerging Threat Landscape*. Dhaka, Bangladesh: Bangladesh Institute of Peace and Security Studies.
- Brainy Quote. 2019. "Abraham Lincoln Quotes". Accessed 01 January 2019.
https://www.brainyquote.com/quotes/abraham_lincoln_163082.
- Brantly, Aaron F., Nerea M. Cal, and Devlin P. Winkelstein. 2017. *Defending the Borderland, Ukrainian Military Experiences with IO, Cyber, and EW*. New York: Army Cyber Institution, West Point.
- The British Army. 2019. "77th Brigade." 01 February. Accessed 01 March 2019.
<https://www.army.mod.uk/who-we-are/formations-divisions-brigades/force-troops-command/77-brigade/>.
- British Broadcasting Corporation (BBC). 2016 "Bangladesh siege: Twenty killed at Holey Artisan Bakery in Dhaka." 02 July. Accessed 02 August 2018.
<https://www.bbc.com/news/world-asia-36692613>.
- Brock, Mark E., Major. 2005. "How to Organize the Headquarters for Information Operations at the Brigade and Division." Master's Thesis, U.S. Army Command and General Staff College, Fort Leavenworth, KS.

- BTRC. 2018. "Internet Subscribers Bangladesh." January. Accessed 01 January 2019. <http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-january-2018>.
- Buckenmaier III, Chester "Trip", Colonel (retired). 2016. "It is curious that physical courage should be so common in the world and moral courage so rare." *U.S. Medicine*, 08 July. Accessed 01 June 2018. <http://www.usmedicine.com/editor-in-chief/it-is-curious-that-physical-courage-should-be-so-common-in-the-world-and-moral-courage-so-rare/>.
- Carter, Joe. 2018. "What You Should Know About the National Defense Strategy." *Providence*, 23 February. Accessed 01 February 2019. <https://providencemag.com/2018/02/know-national-defense-strategy/>.
- Cavelty, Myriam Dunn. 2008. *Information Operations: Trends and Controversies*. Zurich: Center for Security Studies.
- Chairman Joint Chiefs of Staff (CJCS). 2006a. Joint Publication 1-02, *Dictionary of Military and Associated Terms*. Washington, DC: Joint Chiefs of Staff.
- . 2006b. Joint Publication 3-13.4, *Military Deception*. Washington, DC: Joint Chiefs of Staff.
- . 2012. Joint Publication 3-13, *Information Operations*. Washington, DC: Joint Chiefs of Staff, November.
- Churchill, Winston S. 2006. "Excerpts from the Sixth Churchill Lecture 'Winston Churchill: Leadership in Times of Crisis'." *Finest Hour* 133 (Winter 2006-2007): 17. Accessed 14 January 2019. <https://winstonchurchill.org/publications/finest-hour/finest-hour-133/excerpts-from-the-sixth-churchill-lecture-winston-churchill-leadership-in-times-of-crisis/>.
- Commonwealth of Australia, Department of Defence (Australian DOD). 2013. Australian Defence Doctrine Publication 3.13, *Information Activities*. Edition 3. Canberra ACT: Defence Publishing Service.
- Cordesman, Anthony H. 2014. *Russia and the "Color Revolution": A Russian Military View of a World Destabilized by the US and the West*. Washington, DC: Center for Strategic and International Studies.
- Dahl, Dejan Stojkovic, and Robert Bjørn. 2007. *Methodology for Long Term Defence Planning*. Kjeller, Norway: Norwegian Defence Research Establishment.
- Darczewska, Jolanta. 2014. *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study, Point of View*. Warsaw: Warsaw: Centre for Eastern Studies.

- Dickens, Charles. 2005. *A Tale of Two Cities*. Edited by Philip M. Parker. San Diego, CA: ICON Group International, Inc.
- Ehrhart, Hans-Georg. 2017. "Postmodern warfare and the blurred boundaries between war and peace." *Defence and Security Analysis*, no. 3: 264.
- Elliott, Josh K. 2018. "Theatricality and deception: How Russia uses 'maskirovka' to shake the world." *The Global News*, 19 June. Accessed 07 March 2019. <https://globalnews.ca/news/4260938/russia-strategy-maskirovka-military-politics-putin/>.
- Elstad, Peter L., Major. 1988. "Overcoming Information Operations legal limitations in Support of Domestic Operations." Master's Thesis, U.S. Army Command and General Staff College, Fort Leavenworth, KS.
- Ettrich, Brian B. 2005. "The Principles of War: Are They Still Applicable?" Thesis, Naval Postgraduate School, Monterey, CA.
- Financial Times. 2015. "Army revives Chindits as 'Facebook warriors' for smart battle." 11 February. Accessed 04 March 2019. <https://www.ft.com/content/537c7436-a892-11e4-ad01-00144feab7de?siteedition=uk#axzz3RKXxu5GH>.
- Gause, Bill, Reverend. 2017. "Moral Courage, Revisited." Sermon, Overbrook Presbyterian Church, 29 January. Accessed 19 March 2019. <http://overbrookchurch.org/wp-content/uploads/2017/09/Sermon-2017-01-29-Moral-Courage-Revisited.pdf>.
- Giles, Keir. 2012. "Russia's Public Stance on Cyberspace Issues (Cyber Conflict (CYCON), 2012)." 4th International Conference, Tallinn, Estonia, 5-8 June.
- Giles, Lionel. 2000. *Sun Tzu on the Art of War*. Edited by Lionel Giles. Leicester LE2 1WS, England: Allandale Online Publishing.
- Government of Bangladesh (GoB). 2007. *Bangladesh Vision 2021*. Dhaka: Centre of Policy Dialogue.
- Government of Canada, Department of National Defence (Canada DND). 1998. Canadian Forces Joint Publication 3.10, *Information Operations*. Ottawa, ON: Chief of the Defence Staff.
- . 2018. B-GL-300-005/FP-001, *Information Operations*. Ottawa, ON: Chief of the Defence Staff.
- Headquarters, Department of the Army (HQDA). 1996. Field Manual 100-6, *Information Operation*. Washington, DC: Government Printing Office, August.

- . 2013. Field Manual 3-13, *Information and Influence Activities*. Washington, DC: Government Printing Office, January.
- . 2017. Army Doctrine Reference Publication 3-0, *Operations*. Washington, DC: Government Publishing Directorate, October.
- Hirschman, Albert O. 1970. *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States*. Cambridge, MA: Harvard University Press.
- Iasiello, Emilio J. 2017. “Russia’s Improved Information Operations: From Georgia to Crimea.” *Parameters* 47, no. 2: 51-63.
- Info Security. 2012. “Cyberwar between India and Bangladesh escalates.” 16 February. Accessed 02 March 2019 <https://www.infosecurity-magazine.com/news/cyberwar-between-india-and-bangladesh-escalates/>.
- Islam, Shariful. 2018. “Digital Bangladesh a reality now.” *Dhaka Tribune*.
- IT Law Wiki. 2019. “Information Operations.” 01 April. Accessed 25 October 2018. https://itlaw.wikia.org/wiki/Information_operations#cite_ref-1.
- Jha, Saurav. 2014. “Indian Army C4ISR trends.” *News 18*, updated 22 August.
- JohnWayne.com. 2018. “Quotes.” Accessed 15 January 2019. <https://johnwayne.com/quotes/>.
- Kahneman, Daniel. 2011. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.
- Kidder, Rushworth M. 2005. *Moral Courage*. New York, NY: HarperCollins Publishers Inc.
- Knox, MacGregor, and Williamson Murray. 2003. *The Dynamics of Military Revolution*. New York: Cambridge University Press.
- Koshkin, Pavel. 2015. “The Paradox of Kremlin Propaganda: How It Tries to Win Hearts and Minds.” *Russia Direct*, 2 April.
- Kostadinov, Dimitar. 2011. “Cyber Threat Analysis.” InfoSec Institute, Elmwood Park, IL.
- Krulak, Charles C., General. 1999. “The Strategic Corporal: Leadership in the Three Block War.” *Marines Magazine* (January): 1-7. Accessed 15 March 2019. http://www.au.af.mil/au/awc/awcgate/usmc/strategic_corporal.htm.
- Lauder, Matthew A. 2007. *Masters of Chaos: The Application of Political Warfare by the Russian Federation*. Canada: Defence Research and Development.

- Lee, Harper. 2016. "Moral Courage." Bartleby Research, 30 April. Accessed 01 February 2019. <https://www.bartleby.com/essay/Moral-Courage-By-Harper-Lee-PKVUCJHV36Y3W>.
- Leonard, Robert R. 1998. *The Principles of War for the Information Age*. Novato CA: Presidio Press.
- Logue, Jason, Major. 2010. "Rethinking Information Dominance and Infuence Battlespace Effect." *The Australian Army Journal* 7, no. 3 (Summer).
- Mannion, Luke F., Captain. 2018. "Institutionalizing Information Operations." *Marine Corps Gazette* (April): 1.
- Marlatt, Greta E. 2008. *Information Warfare and Information Operations (IW/IO): A Bibliography*. Monterey, CA: Dudley Knox Library Naval Postgraduate School.
- Matheny, Michael R., Colonel. 2001. "The Roots of Modern American Operational Art." Air University, Montgomery, AL.
- Matt, Jacob M., Major. 2008. "Moral Courage or Heresy: The Benefits and Pitfalls of Military Leaders Speaking Out." USMC Command and Staff College, Quantico, VA.
- McGrath, James R. 2016. "Twenty-First Century Information Warfare and Third Offset Strategy." *Joint Forces Quarterly* 82 (3rd Quarter, 1 July): 16-23.
- Melman, Gavi. 2016. "Moral Courage: Heroes." Kellman Brown Academy, Voorhees, NJ, 1 June.
- Miller, Carl. 2018. "Inside the British Army's secret information warfare machine." *Wired*, 14 November.
- Miller, Rielle. 2005. "Moral Courage: Definition and Development." Ethics Resource Center, Washington, DC.
- Monaghan, Andrew. 2012. *The New Russian Foreign Policy Concept: Evolving Continuity*. London, England: Chatham House.
- Mukherjee, Riddhi. 2017. "India and Bangladesh sign MOU for cyber security." *Medianama*, 14 July. Accessed 01 February 2019. <https://www.medianama.com/2017/07/223-cyber-security-india-bangladesh/>.
- National Intelligence Council (NIC). 2017. *Global Trends: A Paradox of Progress*. Washington, DC: Office of the Director of National Intelligence, January.
- North Atlantic Treaty Organization (NATO). 2009. Allied Joint Publication 3.10, *Allied Joint Doctrine for Information Operations*. Brussels, Belgium: NATO.

- Norton, Richard J. 2003. "Feral Cities." *Naval War College Review* 56, no. 4 (Autumn).
- Otero, Christopher. 2011. "Reflections on Clausewitz and Jomini: A Discussion on Theory, MDM, and Design in the Post OIF Army." *Small Wars Journal* 25 (May): 1-12.
- Owens, Mackubin Thomas. 2008. "Reflections on Future War." *Naval War College Review* 61, no. 3 (Summer).
- Paret, Peter. 1986. *Makers of Modern Strategy*. New Jersey: Princeton University Press.
- Philosiblog. 2011. "The world is a dangerous place to live not because of the people who are evil but; because of the people who don't do anything about it." 09 November. Accessed 01 January 2019. <https://philosiblog.com/2011/11/29/the-world-is-a-dangerous-place-to-live-not-because-of-the-people-who-are-evil-but-because-of-the-people-who-dont-do-anything-about-it/>.
- Pike, John. 2016. "Coco Islands." Federation of American Scientists. Accessed 03 March 2019. <https://fas.org/irp/world/china/facilities/coco.htm>.
- Porche III, Isaac R., Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy Y. Min, and Bruce J. Held. 2013. *Redefining Information Warfare Boundaries for an Army in a Wireless World*. Santa Monica: RAND Corporation.
- Rabbi, Arifur Rahman. 2017. "Indian Hackers take Down Bangladeshi Defence Website." *Dhaka Tribune*, 29 April. Accessed 05 February 2019. <https://www.dhakatribune.com/bangladesh/crime/2017/04/29/indian-hackers-bangladesh-website>.
- RAND Corporation. 2018. "Information Operations." 23 September. Accessed 23 September 2018. <https://www.rand.org/topics/information-operations.html>.
- Rapp, William E., Major General. 2016. "Ensuring Effective Military Voice." *Parameters* 46, no. 4 (Winter): 13-25.
- Reuters, Thomson. 2016. "Cyberattack that crippled Ukrainian power grid was highly coordinated." *CBA*, 11 January. Accessed 01 January 2018. <https://www.cbc.ca/news/technology/ukraine-cyberattack-1.3398492>.
- Ross, Steven T. 1988. *Napoleon and Maneuver Warfare*. Edited by Harry R. Borowski. Washington, DC: Office of the Air Force History, US Air Force.
- Sotirovic, Vladislav B. 2017. "The Peace Treaty of Westphalia (1648) and its Consequences for International Relations." *Oriental Review*.

- Sun Tzu. 1963. *The Art of War*. Translated by Samuel B. Griffith. New York: Oxford University Press.
- Sunil. 2014. "Threat Modelling." Slide Share, 22 April. Accessed 16 January 2019. <https://www.slideshare.net/null0x00/threat-modelling-33806672>.
- The Times of India. 2018. "Bangladesh launches its first satellite, 'Bangabandhu-1'." Accessed 14 October 2018. <https://timesofindia.indiatimes.com/world/south-asia/bangladesh-launches-its-first-satellite-bangabandhu-1/articleshow/64144484.cms>.
- U.S. Army Cyber Command (CYBERCOM). 2019. "1st Information Operations Command (Land)." Accessed 01 April 2019. <https://www.arcyber.army.mil/Organization/1st-IO-Command/>.
- U.S. Army Training and Doctrine Command (TRADOC). 2018. TRADOC Pamphlet 525-92. *The Operational Environment and the Changing Character of Future Warfare*. Fort Eustis, VA: TRADOC.
- U.S. Army War College (AWC). 2018. *How the Army Runs: A Senior Leader Reference Handbook, 2017-2018*. Carlisle, PA: Department of Command, Leadership, and Management, AWC.
- U.S. Secretary of Defense (SecDef). 2018. *Summary of the 2018 National Defense Strategy of the United States of America*. Washington, DC: Department of Defense.
- United Kingdom Ministry of Defence (UK MOD). 2013. *Transforming the British Army*. London: Ministry of Defence.
- . 2015. *The Future Character of Conflict*. London: Defence Development, Concepts and Doctrine Centre.
- United Kingdom Parliament (UK Parliament). 2015. "Armed Forces: Information Warfare." 04 March. Accessed 03 March 2019. <https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2015-02-24/225283/>.
- Van Creveld, Martin. 1991. *The Transformation of War*. New York: Free Press.
- Von Clausewitz, Carl. 1989. *On War*. Edited by Michael Howard and Peter Paret. New Jersey: Princeton University Press.
- Watts, Barry D. 2004. *Clausewitzian Friction and War*. Rev. ed. McNair Paper 62. Washington, DC: Institute for National Strategic Studies, National Defence University.

Wikipedia. 2018. "77th Brigade (United Kingdom)." Accessed 01 March 2019.
[https://en.wikipedia.org/wiki/77th_Brigade_\(United_Kingdom\)](https://en.wikipedia.org/wiki/77th_Brigade_(United_Kingdom)).