



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**ALLIED SPECIAL OPERATIONS FORCES COMMAND:
KEY TO NATO'S 360-DEGREE MULTI-DOMAIN
OPERATIONS APPROACH WITH CYBER AND SPACE**

by

Alex Kaisler

December 2023

Thesis Advisor:
Second Reader:

Ryan Maness
Eric P. Wendt

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE December 2023	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE ALLIED SPECIAL OPERATIONS FORCES COMMAND: KEY TO NATO'S 360-DEGREE MULTI-DOMAIN OPERATIONS APPROACH WITH CYBER AND SPACE			5. FUNDING NUMBERS	
6. AUTHOR(S) Alex Kaisler				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) Allied Special Operations Forces (A-SOF) are crucial in addressing both NATO's strategic goal of evolving modern warfare from Joint Operations to a 360-degree Multi-Domain Operations (MDO) approach and the required integration of cyber and space capabilities into this evolutionary process. The allied countries laid the political-strategic course for this evolutionary MDO transformation with the "NATO 2022 Strategic Concept," but there is a lack of executive options at the strategic-operational level. The thesis created a semantic database through interviews with experts and applied hybrid analysis methods, including binary and semantic differential distribution analyses and semantic network analysis. These methods tested four hypotheses to address the research question: How can A-SOF enhance interoperability between A-SOF, cyber, and space? The testing of the hypotheses intended to identify options for action to address the research question practically. The analyses affirmed that A-SOF is uniquely qualified, possessing essential structures, generating knowledge through organic training facility, and improving interoperability by liaison elements. The thesis proposes three key recommendations: employ a tailored strategy, utilize A-SOF's organic training facility, and leverage liaison elements for interoperability. The recommendations aim to enhance interoperability between A-SOF, cyber, and space, aligning with NATO's 360-degree MDO approach.				
14. SUBJECT TERMS Allied Special Operations Forces, A-SOF, 360-degree Multi-Domain Operations approach, MDO, cyber, space, Special Operations Command, SOFCOM			15. NUMBER OF PAGES 181	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**ALLIED SPECIAL OPERATIONS FORCES COMMAND: KEY TO NATO'S 360-
DEGREE MULTI-DOMAIN OPERATIONS APPROACH WITH CYBER AND
SPACE**

Alex Kaisler
Oberstleutnant, German Army
MS, Bundeswehr University Munich, 2011

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN DEFENSE ANALYSIS
(IRREGULAR WARFARE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2023**

Approved by: Ryan Maness
Advisor

Eric P. Wendt
Second Reader

Carter Malkasian
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Allied Special Operations Forces (A-SOF) are crucial in addressing both NATO's strategic goal of evolving modern warfare from Joint Operations to a 360-degree Multi-Domain Operations (MDO) approach and the required integration of cyber and space capabilities into this evolutionary process. The allied countries laid the political-strategic course for this evolutionary MDO transformation with the "NATO 2022 Strategic Concept," but there is a lack of executive options at the strategic-operational level. The thesis created a semantic database through interviews with experts and applied hybrid analysis methods, including binary and semantic differential distribution analyses and semantic network analysis. These methods tested four hypotheses to address the research question: How can A-SOF enhance interoperability between A-SOF, cyber, and space? The testing of the hypotheses intended to identify options for action to address the research question practically. The analyses affirmed that A-SOF is uniquely qualified, possessing essential structures, generating knowledge through organic training facility, and improving interoperability by liaison elements. The thesis proposes three key recommendations: employ a tailored strategy, utilize A-SOF's organic training facility, and leverage liaison elements for interoperability. The recommendations aim to enhance interoperability between A-SOF, cyber, and space, aligning with NATO's 360-degree MDO approach.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	HISTORICAL EXAMPLE	1
1.	ViaSat Attack as a Failed First Strike and Lessons Identified for NATO	1
B.	DERIVATION OF THE RESEARCH QUESTION	4
1.	The Rapid Growth of Cyber and Space in the Context of the Great Power Competition and NATO's MDO Capabilities	4
2.	Allied Special Operations Forces, a Foundation for Interoperability	6
3.	Research Question (RQ).....	7
C.	LITERATURE REVIEW	7
1.	NATO's Perspective on Evolution in Cyber and Space and the Rise of Multi-Domain Operations	7
2.	Cyber and Space in Armed Conflicts.....	9
3.	Cyber Strategies	10
4.	Space Strategies.....	12
5.	A-SOF, Cyber, and Space Warfare, and a Required Symbiosis for MDO Capabilities	14
D.	HYPOTHESES	17
1.	Research Assumption	17
2.	Research Statement	17
3.	Hypotheses	18
E.	APPROACH.....	20
1.	Chapter I: Introduction.....	20
2.	Chapters II and III: Background	21
3.	Chapter IV: Integrating Cyber, Space, and A-SOF	21
4.	Chapter V: Assessment.....	24
5.	Chapter VI: Conclusion with Findings, Recommendations and Outlook.....	25
II.	PRINCIPLES OF THE FUNCTIONAL DOMAIN A-SOF	27
A.	ALLIED SPECIAL OPERATIONS FORCES	28
1.	How NATO Considers Allied Special Operations Forces	29
2.	Characteristics of Special Operations in NATO	30
3.	Principle Tasks for A-SOF in NATO	32

4.	Key Elements within the A-SOF Organization and SOFCOM Mission.....	36
5.	A-SOF Potential for Further Research.....	40
III.	PRINCIPLES OF CYBER, SPACE DOMAINS	43
A.	CYBER IN NATO.....	44
1.	How NATO Considers Cyberspace.....	45
2.	Characteristics, Principles, and Types of CO in NATO.....	47
3.	SCEPVA Framework Mechanism, OCO, and the Role of CyOC.....	51
4.	Additional Cyber Organizations in or for NATO.....	54
5.	Potential for Further Research on Cyber.....	55
B.	SPACE IN NATO	56
1.	How NATO Considers the Space Domain	57
2.	Space Domain Principles and Fundamentals	59
3.	NATO Space Centre of Excellence, a Thinktank for Space Development	62
4.	Space Framework Mechanism and the Role of the Private Sector.....	64
5.	Space Potential for Further Research.....	67
IV.	INTEGRATING CYBER, SPACE AND A-SOF	69
A.	INTERVIEWS AND DATA COLLECTION	69
1.	Interview Principles and the Setup for Data Collection.....	70
B.	DATA ANALYSIS.....	75
1.	Binary Distributions Analysis and Semantic Differentiation Distributions Analysis	76
2.	Semantic Network Analysis	88
V.	ASSESSMENT AND FINDINGS.....	107
A.	DISTRIBUTIONS ANALYSIS ASSESSMENT	107
1.	Binary Distribution Analysis Assessment.....	108
2.	Semantic Differentiation Distribution Analysis Assessment	109
B.	SEMANTIC NETWORK ANALYSIS ASSESSMENT	111
1.	Assessments for Community #14.....	111
2.	Assessments for Community #6.....	114
3.	Assessments for Community #1.....	116
C.	SUMMARY OF THE ASSESSMENTS OF THE ANALYSES	118

VI.	CONCLUSION WITH FINDINGS, RECOMMENDATIONS AND OUTLOOK.....	121
A.	REVIEW OF THE RESEARCH DEVELOPMENT AND APPROACH.....	121
B.	MAIN FINDINGS.....	122
C.	RECOMMENDATIONS.....	127
1.	A-SOF Strategy 2030 as a Communications Campaign.....	128
2.	NSOU: Short and Long-Term Education Packages	132
3.	Interoperability Elements	136
D.	WAY AHEAD	137
	APPENDIX A. LIST OF INTERVIEW QUESTIONS AND STATEMENTS	139
	APPENDIX B. QUESTION-RESPONDENT MATRIX FROM 1 – 300.....	143
	LIST OF REFERENCES.....	145
	INITIAL DISTRIBUTION LIST	153

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	Thesis Development Approach.....	21
Figure 2.	A-SOF in NATO.....	32
Figure 3.	Qualitative Illustration of the Demand for SO in the Spectrum of Conflict.	34
Figure 4.	SOFCOM Mission, Vision, the Lines of Operation (LOO) and the Lines of Effort (LOE).	37
Figure 5.	Abstract Illustration of SOFCOM’s Organizational and Command Structure.....	38
Figure 6.	The Three-Layer Model, how NATO considers Cyberspace.	46
Figure 7.	NATO Level of Warfare.....	47
Figure 8.	Responsibility and Task Spectrum of the CyOC in the Cyber Directorate SHAPE.....	50
Figure 9.	Commander NCISG/DCOS CIS and Cyber Defense.	53
Figure 10.	Conception and Organization of Space Support between NATO and Contribution Nations.....	62
Figure 11.	Organizational chart of NATO Space Centre of Excellence.	63
Figure 12.	U.S. Spacepower Relationship.....	65
Figure 13.	U.S. Space Force (USSF) Information Mobility.	66
Figure 14.	The Distribution of Interview Partners at the SOFCOM.....	70
Figure 15.	Substantial Knowledge and the Role of SOFCOM’s NSOU for Education	77
Figure 16.	Importance of Basic Knowledge about each for A-SOF, Cyber, And Space.....	78
Figure 17.	SOFCOM’s Unique Qualification for Interoperability with Cyber, and Space	79
Figure 18.	How qualified is SOFCOM to advance Interoperability with Cyber and Space	80

Figure 19.	Integrating Specific Liaison Elements to Enhance Interoperability	81
Figure 20.	Liaison Elements Enhancing Interoperability between SOFCOM, Cyber, and Space	82
Figure 21.	Binary Responses over H1, H2, H3, H4	83
Figure 22.	Semantic Differential Distribution analysis with 1 to 5 over H1, H2, H3, H4.....	84
Figure 23.	SOFCOM’s Positive or Negative Impact on the 7 Challenges.....	85
Figure 24.	Distribution of the Semantic Differential Assessments with 1 to 5 to Q1–Q6.....	87
Figure 25.	SME Assessments on OCO Scenarios 1–2.....	88
Figure 26.	Utilizing the SNA on the entire SN and collapsing it into 25 Semantic Communities	91
Figure 27.	Degree Centrality, Formula and a Qualitative Graphical Illustration.....	92
Figure 28.	Eigenvector Centrality, Formula, and a Qualitative Graphical Illustration.....	93
Figure 29.	Harmonic Closeness Centrality, Formula and a Qualitative Graphical Illustration.....	94
Figure 30.	Betweenness Centrality, Formula and a Qualitative Graphical Illustration.....	95
Figure 31.	Left: 3 Largest Communities with 579 Nodes and 1145 Edges; Right: 3 Largest Communities shrunk to 6-Core Nucleus Cluster	96
Figure 32.	Right: 6-core Nucleus Cluster scaled by SGA; Left: 6-core Nucleus Cluster Scaled by BC.....	97
Figure 33.	Top Left: Collapsed 25 Communities.....	98
Figure 34.	Community #14 4-Core Cluster, Scaled with BC.....	100
Figure 35.	Top Left: Collapsed 25 Communities.....	101
Figure 36.	Community #6 4-Core Cluster scaled with BC	102
Figure 37.	Collapsed 25 Communities.....	103
Figure 38.	Community #1 3-Core Cluster Scaled with BC.....	105

Figure 39.	Summary of the Results from the BDA of the Interviews with Experts	108
Figure 40.	Summary of the Results from the SDDA of the Interviews with Experts	110
Figure 41.	Education, as a Key finding for Interoperability	112
Figure 42.	Liaison Elements for Better Interoperability	113
Figure 43.	SOFCOM’s Role and Positioning toward Integration Efforts.....	114
Figure 44.	Cyber and its Offensive Effects as Structural Power Components for Better Interoperability	115
Figure 45.	Space, SOF and Integration, the Central Components within Community #1	117
Figure 46.	Three Main Recommendations to address the Research Question	128
Figure 47.	Consistent Communication Campaign derived from an “A-SOF Strategy 2030”	131
Figure 48.	Global Programming – Development Methodology.....	135

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Cyber Effect through DCO and OCO by STANAG 2287.....	51
Table 2.	Cyber and Space Sector Contributions during the Ukraine War	67
Table 3.	Qualitative Illustration of the Interview Part I: Closed-Ended Approach.....	72
Table 4.	Qualitative Illustration of the Interview Part II, Open-Ended Approach.....	73
Table 5.	Qualitative Illustration of the Interview Part III: Scenarios Discussion	74
Table 6.	Open-Ended Questions Q1 – Q6.....	86
Table 7.	Quantitative and Qualitative Interpretation of Centrality Measures in Semantic Network Elements (SNE).....	89
Table 8.	Centrality Results of the 3 Largest Communities	96
Table 9.	Centrality Results of the Community #14 within the SN	99
Table 10.	Centrality Results of the Community #6 within the SN	101
Table 11.	Centrality Results of the Community #1 within the SN	104
Table 12.	Main Findings derived from the Assessment Process	119

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

3C	competition-crisis-conflict
A-SOF	Allied-Special Operations Forces
ACO	Allied Command Operations
AAR	After Action Report
ACT	Allied Command Transformation
AIRCOM	Allied Air Command
AJO	Allied Joint Operations
AJP	Allied Joint Publication
AOO	Area of Operation
ARCYBER	US Army Cyber Command
ARSOF	Army Special Operations Forces
ASC	J2 all-source cell
BDA	binary distributions analysis
C2	command and control
CAS	Close Air Support
CBRN	chemical, biological, radiological and nuclear
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CCDR	Combatant Commanders
CCMD	Combatant Commands
CDCC	Cross Domain Command Concept
CHT	Counter Hybrid Threats
CIA	confidentiality, integrity and availability
COE	Centers of Excellence
COIN	Counter-insurgency
COM	Commander
COM SOFCOM	SOFCOM Commander
CS	Combat Support
CSS	Combat Service Support
CT	Counterterrorism
CyCon	International Conference on Cyber Conflict

CyOC	Cyber Operations Centre
DA	Direct Action
DC	Degree Centrality
DCO	defensive cyber operations
DCOS	Deputy Chief of Staff, Deputy Chief of Staffs
DSC	defensive space control
EOD	Explosive Ordnance Disposal
ESPI	European Space Policy Institute
FFT	Friendly Force Tracking
FN	Framework Nation
FOB	Forward Operation Base
FULLCOM	full command
GeoMetoc	Geological Meteorological Oceanographic
GPC	Great Powers Competition
H1, H2, H3, H4	Hypotheses
HN	Host Nation
HRO	Hostage Release Operation
IA	Information Activity
IC2I	International Command and Control Institute
IE	Information Environment
IO	Information Operations
JISR	Joint Intelligence, Surveillance and Reconnaissance
JO	Joint Operations
JOA	Joint Operations Areas
LI	Lessons Identified
LOA	Level of Ambition
LOE	Lines of Effort
LOO	Lines of Operation
MA	Military Assistance
MC	Military Committee
MDO	Multi-Domain Operations Center
NATO SAT	NATO System Approach to Training

NCIA	NATO Communication and Information Agency
NCIO	NATO Communications and Information Organization
NCISG	NATO Communication Information System Group
NCS	NATO Command Structure
NDC	NATO Defense College in Rome
NFS	NATO Force Structure
NRF	NATO Response Force
NSO	NATO School Oberammergau
OCO	Offensive Cyber Operations
OCOC	Offensive Cyber Operations Capability
OPCOM	Operational Command
OPSEC	operational security
OSC	offensive space control
OSO	Office of Special Operations
OSS	Operational Space Support
PCR	Post Course Reviews
PIR	Priority Intelligence Requirement
PMOSII	Political, Military, Economic, Social, Infrastructure and Information
PNT	Positioning, Navigation and Timing
PO	Performance Objectives
PR	Performance Requirement
RQ	Research Question
SACEUR	Supreme Allied Commander Europe
SATCOM	Satellite Communication
SCEPVA	Sovereign Cyber Effects Provided Voluntarily by Allies
SDA	Space Domain Awareness
SDC	Space Domain Coordination
SDDA	semantic differential distribution analysis
SEW	Shared Early Warning
SGA	Spinglass community detection algorithm
SME	subject matter experts

SN	semantic network
SNA	semantic network analysis
SNE	semantic network elements
SO	Special Operations
SOA	Special Operations Area
SOCC	Special Operations Component Command
SOF	Special Operations Forces
SOSCIC	Special Operations Space and Cyber Integration Cell
SpCen	NATO Space Centre
SpCMA	Space Control Mission Area
SpCOE	NATO Space Centre of Excellence
SpSC	NATO Space Support Coordination
SR	Special Reconnaissance
SSA	Space Situational Awareness
SSEC	Space Security
STANAG	Standardization Agreement
STP	Strategic Training Plan
TCN	Troop-Contribution Nations
TNA	Training Needs Analysis
TRA	Training Requirements Analysis
USARSOF	United States Army Special Operations Forces
USASMD	US Army Space and Missile Defense Command
USASOC	United States Army Special Operations Command
USCYBERCOM	United States Cyber Command
USSF	United States Space Force
USSOCOM	United States Special Operations Command
USSPACECOM	United States Space Command
WFD	Warfare Development
WMD	weapons of mass destruction

EXECUTIVE SUMMARY

Allied Special Operations Forces (A-SOF) play a pivotal role in NATO's shift to Multi-Domain Operations (MDO), integrating cyber and space into both the NATO Force Structure (NFS) and NATO Command Structure (NCS). Aligned with the "NATO 2022 Strategic Concept," the alliance commits to adapting its Lines of Ambition (LOA) profile for the full spectrum of competition, crises, and conflict (3C). Given NATO's proactive stance against hybrid threats in the 3C realm, A-SOF, emphasizing a 360-degree approach, must address a key question: ***"Given that there is a politically initiated adaptation process in NATO aiming at a 360-degree MDO approach against hybrid threat scenarios and with a requirement of a direct dependency between Cyber, Space, and MDO capabilities, how can A-SOF contribute to this process and evolve better interoperability between A-SOF, Cyber, and Space?"*** NATO's adjustment to LOA addresses modern threats and aligns the alliance with evolving geopolitical challenges. Over the past decade, adversaries have exploited the operational spectrum to gain an edge. The Russian attack on Ukraine revealed the need for comprehensive operational integration of cyber and space capabilities in the armed forces, a crucial factor for success in conflicts. The adaptation requires deploying cyber and space-enabled A-SOF for a 360-degree cross-domain approach across the 3C threat spectrum. The thesis argues that A-SOF, with its operational-strategic Special Operations Forces Command (SOFCOM), can contribute to better cyber and space interoperability through a tailored campaign, complementary education, and interoperability liaison.

The research employs subject matter expert (SME) interviews for data collection, deriving the interview framework from a comprehensive literature review. The research assumes a direct relationship between NATO's strategic goal of evolving modern warfare from Joint Operations (JO) to MDO as a 360-degree approach and the integration of cyber and space domains and capabilities into this evolutionary process. The research statement asserts that A-SOF, through established structures in NFS and NCS, enhances capabilities and interoperability with cyber and space, contributing to NATO's strategic goals. The four hypotheses explore A-SOF's knowledge of cyber and space, the importance of SOFCOM's

NSOU in fostering interoperability, SOFCOM's unique qualifications for advancing interoperability, and the impact of integrating specific liaison elements on space, cyber, and A-SOF interoperability capabilities. To test these hypotheses, the research employed a hybrid semantic analysis methodology, incorporating both binary distribution analysis (BDA) for closed-ended statements, and semantic differential distribution analysis (SDDA) for open-ended questions and semantic network analysis (SNA) utilizing a community detection algorithm and centrality measures for analyzing semantic networks.

The comprehensive assessment of all analyses unequivocally affirms the validity of hypotheses and derives further findings to substantiate the research and support the RQ. The thesis identified a total of 7 findings:

F1: A-SOF lacks significant expertise in cyber and space domains, hindering the development of sustainable interoperability

F2: SOFCOM's integral training facility, NSOU, holds significant importance in cultivating fundamental and supplementary knowledge for achieving interoperability with Cyber and Space.

F3: SOFCOM is uniquely qualified to advance interoperability with cyber and space to enhance NATO's 360-degree approach

F4: Integrating specific liaison elements enhances space, cyber, and A-SOF interoperability capabilities

F5: SOFCOM must take an active and committed role in shaping and improving interoperability with cyber and space

F6: Cybers OCO offer a promising avenue for achieving MDO-oriented interoperability with A-SOF

F7: A-SOF, a warfighting element, fosters interoperability, particularly with space entities, driving integration.

As a result, the thesis asserts the correctness of the research assumption, ***“NATO's strategic goal, to evolve modern warfare from JO to MDO as a 360-degree approach, directly relates to cyber and space domains and their interoperability with other domains and warfighting elements.”*** Simultaneously, the thesis contends that its research argument, ***“A-SOF enhances capabilities and interoperability to cyber and space with established structures in NFS and NCS, thus supporting the 360-degree MDO approach capability,***

contributing to NATO’s strategic goals,” stands as a critical component for a conclusive response to the research question in the recommendations.

The thesis finally suggests three recommendations as potential pathways to further explore and address findings F1 to F7, ultimately responding to the RQ: ***“How can A-SOF contribute to this process and evolve better interoperability between A-SOF, Cyber, and Space?”***

The first of the three proposed recommendations suggests a broad approach to the research question, emphasizing the need for a tailored campaign strategy. A-SOF requires a comprehensive strategy to unify its community and establish communication channels with cyber and space domains. SOFCOM should strengthen its operational-strategic Lines of Operations (LOO), specifically “Advise, Enable, Synchronize, and Empower,” aligning them to develop 360-Degree MDO Approaches with cyber and space operational C2 levels. To achieve this, SOFCOM should create an A-SOF strategy 2030, share it within the ANTO community, and transparently communicate its value externally.

The second element within the framework of these recommendations centers on the role of the NATO Special Operations University (NSOU) as the key entity for the A-SOF strategy, aiming at enhancing interoperability with the cyber and space domains through education and knowledge sharing. NSOU enjoys flexibility through its Memorandum of understanding (MOU) organizational structure, offering advantages over NFS institutions. Additionally, being NATO certified and accredited ensures the delivery of training in line with NATO quality standards. NSOU can efficiently integrate components for cross-domain awareness training into existing courses, with course directors empowered to initiate and implement such measures promptly. Moreover, with adequate resources, NSOU can undertake a comprehensive and timely adaptation of its curriculum to align with MDO requirements. Leveraging the NATO Global Programming Method, NSOU can implement a coordinated, complementary educational concept, fostering the evolution of an MDO knowledge base.

Finally, the thesis presents a third recommendation, introducing a specific approach. This approach outlines how SOFCOM can proactively shape and advance

operational-level interoperability. It does so by deploying dedicated liaison elements, including cyber and space liaison elements. These elements are instrumental in implementing an exchange and interoperability culture, serving as a common ground for synchronizing, enabling, and developing. It is crucial to emphasize that all three components must be coordinated in sequence and timing, each building upon the other.

ACKNOWLEDGMENTS

As a German Army Special Operations Forces officer and a dedicated soldier, I take pride and humility in successfully merging my extensive military expertise with my profound passion for science. I reflect this achievement in the creation of my thesis, which delves into a highly relevant and impactful topic. The entire project demanded considerable effort, encompassing extensive literature research, navigating uncertainties surrounding data acquisition and analysis organization, among other challenges. Simultaneously, it brought forth a wealth of positive experiences, including the expansion of my knowledge, engaging conversations with individuals from military, science, and the economy, and the successful advancement of my work. The journey from the initial idea to the completed product brought me joy and fostered personal growth. At the Naval Postgraduate School in Monterey, situated along the picturesque Pacific Coast, I had the distinct privilege of being one of the few international officers afforded a remarkable opportunity to delve into research on NATO Special Operations Forces. This allowed me to seamlessly integrate my military experience into an academic endeavor—an unforgettable journey.

First and foremost, I extend my heartfelt gratitude to my family—my wife, Margarita, and our children, Valerian, Vincent, and Ilian. I take immense pride in each of you. Our collective efforts have made this academic journey possible and truly meaningful. Margarita, I want to express my deep gratitude for your unwavering support throughout my service as an officer. Your courage in navigating the uncertainties and creating a welcoming home for our children and me has not gone unnoticed. Time and time again, you have demonstrated resilience and strength, turning every challenge into an opportunity for our family to thrive. Your commitment to our journey together is the bedrock upon which I draw inspiration and motivation. Your sacrifices and enduring spirit do not go unnoticed, and I am truly fortunate to have you by my side. Thank you for being the pillar of support and love that sustains our family through the unknown. To my boys, I am a proud father; your courage and curiosity in embracing a new world, learning a new language, and immersing yourselves in a different culture alongside Mom and Dad are sources of enduring pride. These experiences will shape us as a family, leaving an indelible mark on us forever.

I am deeply grateful to my academic advisory team, Professor Ryan Maness, and Lieutenant General (R) Eric P. Wendt. You have provided invaluable academic and militarily relevant support, enabling me to delve into a complex military topic with purpose and depth. Professor Ryan Maness, I extend my thanks to you. Your support has granted me academic freedom and reflects your confidence in my thoughts, actions, and written work. Lieutenant General (R) Eric Wendt, I appreciate your generosity sharing decades of experience as an Army Special Operations Forces general. Your insights provided crucial momentum during pivotal moments, and your guidance opened doors I might not have otherwise reached. Thank you for your invaluable contributions.

I sincerely thank several individuals at NPS who played pivotal roles at different stages of my thesis development. First and foremost, I am deeply thankful to Professor Sean Everton for his unwavering commitment and invaluable assistance during the analysis phase, especially in applying SSNA, alongside his involvement in various other projects. Special appreciation goes to Graduate Writing Center coach George Lober for his insightful critiques and steadfast support throughout the writing process. To Greta E. Marlatt, the Academic Support Manager, and Rebecca Pieken, the Thesis Processing Office advisor, I express my heartfelt thanks for your indispensable assistance in structuring the thesis format. Your dedicated contributions were instrumental in ensuring the quality of my thesis met the desired standards, and I am truly grateful for your efforts.

I extend my sincere gratitude to all the interviewees, including Prof. Dr. Ryan Mannes, LTG Antonio Fletcher, LTG (R) Eric P. Wendt, MG Frank Schloesser, BG Neil Grant, COL Dario Giovanni, COL Andreas Barck, COL Przemyslaw Kwiecien, LTC Michael Andersen, LTC Aurimas Kuprys, LTC Tomp Urmet, LTC Gaboli Corbacho, CDR Wolfgang Schoendorf, LTC Giovanni Vuocolo, LTC Thomas Mott, LTC Sven Rieche, M Larissa Ebeling-Bach, Carry Kangur, David Bobby Charlton, David Takaki, Paul Montanus, Denis P. Garman, and Dr. Rique Orzuri. Their invaluable participation was essential for the targeted and comprehensive data collection that formed the foundation of my research. The insights gained from these interviews have the potential to contribute to the development of NATO significantly.

I. INTRODUCTION

Tomorrow's conflicts cannot be won with today's or yesterday's skillsets, processes or technology.

—Allied Command Transformation (ACT), 04 May 2023¹

A. HISTORICAL EXAMPLE

1. ViaSat Attack as a Failed First Strike and Lessons Identified for NATO

A major cyberattack on the commercial-military space service provider ViaSat as a first strike preceded the Russian forces' military invasion of Ukraine on 24 February 2022. This large-scale cyber-space-land hybrid war approach failed because of a failure of coordination and complementation of offensive means through SOF with the created advantage through cyberspace.² An effect created in cyberspace is always limited in time. One must enhance and complement such a cyber effect with offensive means to make a strategically relevant impact.³ The Russians intended to degrade Ukrainian strategic Command and Control (C2) capabilities through an Offensive Cyber Operation (OCO) against ViaSat, a communication Space-service provider, and create strategically relevant preconditions for further actions. With the precondition, Russia intended to enable a rapid invasion of its kinetic forces without resistance to take over the strategic nodes and thus take over the control of Ukraine. This purpose failed because there was no effective coordination between the cyber forces, which were responsible for the initial strike, and the ground forces, which were responsible for the invasion. Moreover, Russia did not

¹ "Allied Command Transformation," NATO What We do, May 4, 2023, 1, https://www.nato.int/cps/en/natohq/topics_52092.htm.

² Nicolò Boschetti, Nathaniel Gordon, and Gregory Falco, "Space Cybersecurity Lessons Learned from the Viasat Cyberattack," in *AIAA Ascend 2022* (AIAA Ascend 2022, Las Vegas, NV: American Institute of Aeronautics and Astronautics, Inc., 2022), 1, <https://doi.org/10.2514/6.2022-4380>.

³ Jeffrey Reynolds, "NATO Multi-Domain Operations: Adapting beyond Joint Doctrine," *The Three Swords*, no. 38 (2022): 25–29.

utilize its SOF to seize and control the C2 nodes, as it did in the Crimea annexation in 2014. A complementary deployment of SOF against critical communications infrastructure could have created the necessary physical C2 degradation and would have maintained the communications advantage.

Russia utilized a conventional OCO mechanism that targeted the ground segment of the ViaSat communications network. Communication networks such as ViaSat are composed of the satellites as the space segment, the data stream as the link segment, and the ground segments for organizing the network service. A malicious wiping software utilized weaknesses in the provider's VPN to access selected modems (consumers) and degrade access to the Internet by using the wiping software.⁴ With this approach, Russia degraded the C2 capability of the Ukrainian military. Thus, Russian hackers initially created the intended operational conditions for the offensive forces, so the invasion took place as planned. Russia relied exclusively on the success of the planned OCO and invaded under the assumption that the cyberattack would be sufficient to maintain the strategic advantage. Russia subsequently did not physically utilize its SOF to preserve the created C2 degradation to keep the operational advantage alive. Russia miscalculated that commercial companies such as Microsoft, Amazon, and SpaceX, which have a strong presence in cyber and space services segments, would assist the Ukrainian state, build a robust cyber defense, and enable the Ukrainian military to communicate. Ukraine quickly countered the C2 degradation, so the Russian advantage promptly evaporated. The result is well-known: Russia has now been stuck in the so-called special operation for more than 16 months and has not been able to achieve its political goal.

Studies on the Russian cyberattack on the ViaSat service show that cyber and space technologies are essential factors in the evolution of modern warfare.⁵ Further analysis also indicates that cyber and space technologies and capabilities should be complementary

⁴ Boschetti, Gordon, and Falco, "Space Cybersecurity Lessons Learned," 3.

⁵ Kaitlyn Johnson, "NATO in Space," in *NATO 2030: Towards a New Strategic Concept and Beyond*, ed. Jason Blessing, Katherine Kjellström Elgin, and Nele Marianne Ewers-Peters (Washington, DC: Johns Hopkins University, 2021), 235–59, <https://sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>.

in armed conflict, and an actor cannot utilize them in isolation.⁶ To successfully use cyber and space capabilities to help achieve strategic objectives in an armed conflict, cyber and space capabilities must be combined with offensive and kinetic forces and measures. The use of SOF can be a promising component in this regard, providing a connecting function to transfer the effects produced by cyber and space technology into physical space. A-SOF was and is an engine for change. NATO has structurally maintained its own A-SOF since 2010, and A-SOF will have to play a critical role in this process. The development of A-SOF in NATO and its adaptations to the strategic environment is an essential task of SOFCOM. Effective integration of cyber and space with their unique capabilities into A-SOF is a vital action area in the development approach of SOFCOM. NATO must learn the lessons of these Russian failures for its adaptations in the continued evolution of warfare.

NATO must constantly transform and adapt itself to the changing geostrategic environment. One of the significant realms that drives this changing process in NATO is the continued evolution of warfare, as the invasion of the Russians in Ukraine exemplarily showed on different levels. The most recent impulse for adaptation in NATO occurred in 2022 at the NATO Summit in Madrid with the release of the strategy paper, NATO 2022 Strategic Concept.⁷ A dynamic, changing hybrid threat environment demands an interoperable 360-degree approach from NATO and its NCS and NFS. In response to the evolution of warfare, NATO is developing the concept of MDO, reflecting the influence of cyber and space domains on operations. The MDO concept requires a holistic integration of cyber and space into the Joint Operations (JO) concept. Cyber and space extend operational considerations include cognitive, physical, and virtual aspects.⁸

NATO can draw valuable lessons from the failures of the Russian cyber-attack and utilize them for its evolution. In the following sections, the thesis derives a research

⁶ James Andrew Lewis, *Cyber War and Ukraine* (Washington, DC: Center of Strategic and International Studies, 2022), 3, <https://www.csis.org/analysis/cyber-war-and-ukraine>.

⁷ NATO, *NATO 2022 Strategic Concept* (Brussels: NATO, 2022), <https://www.nato.int/strategic-concept/#StrategicConcept>.

⁸ Reynolds, "NATO Multi-Domain Operations."

question from the historical example above and the lessons identified (LI) for NATO's MDO development and 360-degree approach. The following paragraphs review the current literature to identify research gaps. Further, the following sections define the framework for the research by proposing hypotheses and developing an approach to answering the research question by supporting or invalidating the hypotheses.

B. DERIVATION OF THE RESEARCH QUESTION

The current approach to Alliance Command and Control does not fully enable NATO to plan, prepare, orchestrate and execute synchronized activities, across all domains and environments, at scale and speed and in collaboration with other instruments of power, partners and stakeholders.

—Allied Command Transformation, 2023⁹

This thesis examines capabilities and operational application mechanisms of cyber, space, and A-SOF in NATO to measure the impact of cyber and space and the warfighting element A-SOF on the NATO idea of MDO and a 360-degree approach. The goal is to see if the thesis can develop a specific contribution of the three components to the NATO idea of a 360-degree approach.¹⁰ From an A-SOF perspective, the thesis will consider improving interoperability between cyber, space, and A-SOF to optimize NATO's 360-degree approach within NCS and NFS.¹¹

1. The Rapid Growth of Cyber and Space in the Context of the Great Power Competition and NATO's MDO Capabilities

The rapid growth of cyber and space provides an important new context for political power projection in an emerging world of great power competition (GPC). A low threshold for entry, low cost, anonymity, transnationality, and asymmetry characterize cyber activities. On the other hand, space is not accessible to all but provides users and the

⁹ Allied Command Transformation, "Cross-Domain Command Concept" (powerpoint presentation, Norfolk, VA, September 12, 2023), 7

¹⁰ NATO, *NATO 2022 Strategic Concept*, 7.

¹¹ NATO Standardization Office, *Allied Joint Doctrine*, Edition F Version 1, NATO Standard AJP-01 (Brussels: NATO Standardization Office, 2022), 1, <https://www.cimic-coe.org/resources/external-publications/ajp-01-cdf-v1-f.pdf>.

military with unique capabilities, making these capabilities strategically irreplaceable. As a result, many nations have classified both cyber and space as military domains and developed abilities in and through cyber and space. NATO followed that path and integrated centrally organized cyber and space structures into its NFS and NCS. NATO cyber and space can ensure limited organic assets. In addition to its limited capabilities, NATO maintains cooperative platforms for cyber and space to coordinate and ensure that allied nations can voluntarily contribute to specific cyber or space activities.¹² Based on the so-called framework mechanism “Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA),” NATO can indirectly facilitate OCO. As the youngest domain, such a mechanism is still under development in space.

Nevertheless, nations such as the U.S., UK, France, Germany, Italy, and Luxembourg voluntarily enable operational and functional capabilities and allow NATO to operate in the space domain. As the Director of the Cyber Directorate in SHAPE, Major General Schloesser elaborates that national caveats and sensitivities in the applications in cyber and space require that NATO organize both domains in a very centralized and isolated manner.¹³ On the one hand, this form of organization creates the necessary structural security to avoid compromising operational sensitivity; on the other hand, it creates the risk of isolated capabilities that are only operable on their domains and have insufficient interconnection with different domains.¹⁴ The isolated application mechanisms listed above lead to the conclusion that NATO’s approach creates disadvantages in the overall context of an MDO and 360-degree approach. At the same time, the example of Russian failure through isolated cyber projection underlines the urgent need to improve NATO’s interoperability and 360-degree approach to cyber and space.

¹² NATO, *Framework Mechanism for the Integration of Sovereign Cyber Effects Provided Voluntarily by Allies into Alliance Operations and Missions*, MCM-0112–2018 (Brussels: NATO, 2018).

¹³ Alex Kaisler, unpublished data gathered from expert interviews with Director of NATO’s Cyber Directorate, Juli 17, 2023

¹⁴ Mikkel Storm Jensen, “Five Good Reasons for NATO’s Pragmatic Approach to Offensive Cyberspace Operations,” *Defence Studies* 22, no. 3 (2022): 473, <https://doi.org/10.1080/14702436.2022.2080661>.

2. Allied Special Operations Forces, a Foundation for Interoperability

Special operations are military activities conducted by specially designated, organized, trained, and equipped forces using distinct techniques and modes of employment. These activities may be conducted independently or with conventional forces across the full range of military operations.

—Allied Joint Doctrine for Special Operations , 2019¹⁵

NATO characterizes SO as, by nature, joint and defines A-SOF as a functional domain. SO can be applied functionally across all military operational spectrums. Additionally, NATO provides domain-specific SOF (Army SOF, Maritime SOF, Air SOF) in the land, maritime, and air dimensions. A-SOF are subordinated to NATO occasionally through Troop-Contribution Nations (TCN). Since 2010, NATO has established SOFCOM as an operational-strategic command in the form of a Memorandum of Understanding (MOU). This command is incorporated into the NCS but organized, maintained, and led by the United States as the framework nation (FN). The organization and structure of SOFCOM are unique in NATO; SOFCOM has been established for over ten years and provides solutions to challenges resulting from modern multi-domain requirements. SOFCOM can respond flexibly to situational changes through its FN mechanisms, and A-SOF is more efficient than other NATO organizations. SOFCOM offers the new cyber and space domains and an already proven command structure that can be utilized and expanded as a blueprint. In addition to the standing command structure, SOFCOM has a training and education facility, NATO Special Operations University (NSOU), which can ideally support and expand the idea of interoperability between cyber, space, and A-SOF. Through the NSOU, SOFCOM has explicitly mapped and designed training and a curriculum that supports the objective of interoperability between A-SOF, cyber, and space.¹⁶

¹⁵ NATO Standardization Office, *Allied Joint Doctrine for Special Operations*, NATO Standard AJP-3.5 (Brussels: NATO Standardization Office, 2019), 1.

¹⁶ NATO Special Operations Headquarters, *NATO Special Operations School Course Catalogue 2022–2023* (Mons, Belgium: NATO Special Operations Headquarters, 2022).

3. Research Question (RQ)

Given the observations above and the historical example in the preceding section, the thesis derives the following research question:

RQ: Given that there is a politically initiated adaptation process in NATO aiming at a 360-degree MDO approach against hybrid threat scenarios and with a requirement of a direct dependency between Cyber, Space, and MDO capabilities, how can A-SOF contribute to this process and evolve better interoperability between A-SOF, Cyber, and Space?

C. LITERATURE REVIEW

In order to maintain warfighting advantage, we must have ironclad processes in place across all five military warfighting domains. NATO is developing and aligning concepts like multi-domain operations so that Allied nations can operate seamlessly together to defend our nations and people.

—General Philippe Lavigne Supreme Allied Commander Transformation,
March 17, 2022¹⁷

1. NATO's Perspective on Evolution in Cyber and Space and the Rise of Multi-Domain Operations

NATO has been considering for some time how to better implement cyber and space into the operability of the NFS, first, to actively participate in the continuous evolution of warfare, and second, to align forces with modern threat scenarios better. Reynolds argues in the Three Swords magazine that ACT's answer to JO is the new MDO approach, where cyber and space are not just parts of the concept but prerequisites.¹⁸ In this way, NATO organizations such as SOFCOM must operationalize the 360-degree approach of NATO strategy. From this finding, the thesis can assume that, in terms of a NATO MDO approach, the integration of cyber and space is a mandatory requirement criterion. As this literature review progresses, other analyses highlight and even specify

¹⁷ Reynolds, "NATO Multi-Domain Operations."

¹⁸ Reynolds.

that an MDO symbiosis between SOF, cyber, and space is essential for operational command and control in the modern and hybrid threat environment and terms of the continuous evolution of warfare.¹⁹ Therefore, this thesis can derive that the MDO, 360-degree approach and cross-domain agility depend on cyber and space interoperability with A-SOF.

According to Blessing, Elgin, Ewers-Peters, and Tiderman, transformation, adaptation, and evolution in NATO are subject to three major challenges. First, the changing threat landscape; second, shifting internal dynamics; and third, the continued evolution of warfare as the third set.²⁰ NATO faces a new threat scenario after twenty years of stabilization and Counter Terrorism (CT) in Afghanistan. The shift in the threat landscape forces NATO to undergo the evolution of warfare. As mentioned above, with cyber and space as new military domains, new technologies generate a new context for political power projection in the GPC. According to United States Cyber Command (USCYBERCOM), modern warfare no longer depends exclusively on achieving superiority in the physical environment but increasingly on achieving dominance in the digital environment.²¹ The rapid development of various digital technologies enormously impacts the set continued evolution of warfare and requires technological and structural adjustments in NATO.

With the NATO 2022 Strategic Concept, the policy set the course and has underlined a need for action for the expansion and continuous development in the cyber and space domains. NATO's goal for continuous warfare development is the MDO Concept regarding cross-domain agility and a 360-degree approach. With this transformation, MDO capability enables NFS and NCS to ensure the strategic triad of

¹⁹ Sergey Sukhankin, "Russian Special Operations Forces: Image Versus Substance," *Eurasia Daily Monitor* 16, no. 43 (March 27, 2019): 1–4.

²⁰ Jason Blessing et al., "New Decade, New Challenges, and New Opportunities: The Way Ahead to NATO 2030," in *NATO 2030: Towards a New Strategic Concept and Beyond*, ed. Jason Blessing, Katherine Kjellström Elgin, and Nele Marianne Ewers-Peters (Washington, DC: Johns Hopkins University, 2021), 1, <https://sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>.

²¹ U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority* (Fort George G. Meade, MD: U.S. Cyber Command, 2018), <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf>.

Deterrence and Defense, Crisis Prevention and Management, and Cooperative Security on an operational layer of power projection.²² The Allies intend to expand the deterrence and defense strategy, previously composed of the classical components (nuclear deterrence, missile defense shield, and conventional forces), with capabilities from the cyber and space domains. With the wording “We will expedite our digital transformation, adapt the NATO Command Structure for the information age and enhance our cyber defenses, networks, and infrastructure.” in paragraph 24, NATO signals that it is willing to take all necessary adaptation steps to its actions in the cyber and space domains in all conflict spectrums.²³

2. Cyber and Space in Armed Conflicts

We are going to have to think about fighting against enemies which have lots of guided rockets, artillery, mortars and missiles, and are using informationalized warfare to completely disrupt our heavily netted force. So what does AirLand Battle 2.0 look like? I don’t know. The Army needs to figure this out.

—Bob Work, 2015, Deputy Secretary of Defense at U.S. Army War College ²⁴

The historical example states that a large-scale hybrid cyberspace and land offensive failed because offensive assets such as SOF were not coordinated and synchronized with the preceding cyber operation. In “Cyber War and Ukraine,” Lewis analyzes Russia’s failure as missing a strategic impact because it didn’t combine the OCO with kinetic capabilities, such as SOF.²⁵ The summaries of Lilly, Rattray, Geers, and Koch during the 15th International Conference on Cyber Conflict (CyCon) underline the analysis of Lewis. The outlines support that civilian companies, such as Amazon, Microsoft, and SpaceX, intercepted the temporary degradation of C2 of the Ukrainian military during the invasion. Russia lost the advantage because it hadn’t planned or coordinated kinetic

²² NATO, *NATO 2022 Strategic Concept*.

²³ NATO, 7.

²⁴ Kelly McCoy, “The Road to Multi-Domain Battle: An Origin Story,” Modern War Institute, October 27, 2017, <https://mwi.westpoint.edu/road-multi-domain-battle-origin-story/>.

²⁵ Lewis, *Cyber War and Ukraine*, 2.

alternatives within the OCO.²⁶ The Russian failure is a statement for NATO about how cyber and space should play out in an armed conflict and how they should interact with other domains. One prominent area of action is the need for interoperability of capabilities across all domains, in all phases of conflict, and mainly when the phase of armed conflict occurs. From the perspective of the A-SOF, the question arises as to what role the A-SOF can play and what responsibilities the strategic-operational leadership in SOFCOM can assume.

3. Cyber Strategies

As Jasper describes, Russia operates in cyber as a domain not only for competition between great power nations but specifically as a continuum of conflict against the U.S. and NATO.²⁷ Gouré also clarifies that NATO must invest in cyber with high priority to counter Russian cyber strategy and asymmetric cyberspace operations.²⁸ Russia utilizes the inflexible adversary component of its asymmetric arsenal, and in doing so, Russia expands its sphere of influence through cyber operations significantly. NATO has now changed its cyber strategy and is investing heavily in cyber to avoid leaving this domain to adversaries such as Russia. In OCO, however, there is still a need for action because it is precisely in this area that an actor like NATO must be able to counter an adversary offensively better and more effectively. As General Nakasone already makes clear, offensive capabilities contribute to NATO's forward defense, open options for action, and do not leave the digital environment to aggressors.²⁹

²⁶ Bilyana Lilly et al., "Business@War: The IT Companies Helping to Defend Ukraine," in *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), Tallinn, Estonia: CyCon, 2023), 71–83, <https://doi.org/10.23919/CyCon58705.2023.10181980>.

²⁷ Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict* (Washington, DC: Georgetown University Press, 2020), 5.

²⁸ Daniel Gouré, *A Competitive Strategy to Counter Russian Aggression against NATO* (Arlington, VA: Lexington Institute, 2018), <https://www.lexingtoninstitute.org/competitive-strategy-counter-russian-aggression-nato/>.

²⁹ Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly: JFQ*, no. 92 (2019): 10–14.

Jensen illustrates, through his five reasons for employing OCO, the barriers NATO nations must overcome to allow NATO to utilize OCO pragmatically.³⁰ It becomes clear that a multi-national alliance such as NATO cannot easily engage in sensitive activities such as offensive cyber. Due to the specificity of cyber domain requirements and the many national caveats, especially for the execution of OCO, NATO will not be able to utilize cyber to its full extent anytime soon. Under the current circumstances, however, NATO must provide adjustments to achieve the set goal of interoperability, cross-domain capability, 360-degree approach, and MDO.³¹ This defined objective is of critical importance to NATO. Moore says in his book *Offensive Cyber Operations*, “To use cyber warfare effectively, it is essential to distinguish where it begins and ends. The specter of cyberwar can and should be turned into a spectrum of offensive cyber operations, or OCO.” It underlines the importance in his research on using OCO properly in a military context.³² As Valeriano, Jensen, and Maness elaborate, NATO faces Russia, one of the most aggressive states competing in cyberspace.³³ They address cyber strategies in their work, *Cyber Strategy, The Evolving Character of Power and Coercion*. They show, for example, that Russia has mastered the whole portfolio of the three essential strategies in cyberspace: disruption, espionage, and degradation. In particular, they emphasize projecting the cyber degradation strategy; the Russian SOF is vital in operationalizing cyber and effectively linking it with other domains (land, air, sea, and space) in the strategic environment.³⁴ According to Maness, states and NATO need an integration step of cyber capabilities with SOF capabilities to counter Russia in a strategic competition throughout the whole

³⁰ Jensen, “Five Good Reasons,” 473–80.

³¹ James A. Lewis, *The Role of Offensive Cyber Operations in NATO’s Collective Defence*, Tallinn Paper No. 8 (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015), https://ccdcoe.org/uploads/2018/10/TP_08_2015_0.pdf.

³² Daniel Moore, *Offensive Cyber Operations: Understanding Intangible Warfare* (Oxford, UK: Oxford University Press, 2021).

³³ Ryan C. Maness, Benjamin M. Jensen, and Brandon Valeriano, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford, UK: Oxford University Press, 2018).

³⁴ Patrick Michael Duggan, “Strategic Development of Special Warfare in Cyberspace,” *Joint Force Quarterly: JFQ*, no. 79 (2015): 46–53.

spectrum of conflict.³⁵ This symbiosis is how a successful implementation of all cyber strategies can succeed.

4. Space Strategies

The evolution in the uses of space and rapid advances in space technology have created new opportunities, but also new risks, vulnerabilities, and potentially threats for the Alliance's and Allies' security and defence.

—NATO, “NATO’s Overarching Space Policy,” January 17, 2022³⁶

Remuss writes at the European Space Policy Institute (ESPI), “In Europe, space is increasingly used as a supportive tool for providing security. In a similar vein, NATO’s Allied Joint Doctrine for Air and Space Operations highlights the potential of space assets in achieving the Alliance’s security objectives.”³⁷ It describes why space is essential to NATO. NATO Space Policy shows the importance of Remuss details, representing many areas of interest, opportunities, risks, and threats associated with using space. In all of them, the security of NATO’s defense capability is the main objective of the military use of space. In this sense, NATO considers the space domain to be contested, congested, and competitive. Therefore, NATO must be able to operate in a disrupted, degraded, and denied space.³⁸ Since 2020, NATO has conducted a joint NATO Space Centre, which provides SATCOM, sharing space situational awareness (SSA), intelligence, surveillance and reconnaissance (ISR), shared early warning (SEW), Positioning, Navigation and Timing (PNT), Space Security (SSEC), and Geospatial, Meteorological, Oceanographic (METOC) organically or through national contributions in the form of framework mechanisms. As Johnson notes, the allies recognize the need to integrate space, its capabilities, and

³⁵ Ryan C. Maness, “Conflict and Cyberspace: Intro to Course and Concepts, DA 3105” (lecture Naval Postgraduate School, Monterey, CA, July 12, 2022).

³⁶ “NATO’s Overarching Space Policy,” NATO Official Texts, January 17, 2022, https://www.nato.int/cps/en/natohq/official_texts_190862.htm.

³⁷ Nina-Louisa Remuss, “NATO and Space: Why Is Space Relevant for NATO?,” *ESPI Perspectives*, no. 40 (October 2010): 1–9.

³⁸ NATO, “NATO’s Overarching Space Policy.”

applications into NATO to ensure the freedom and security of its members.³⁹ According to the Allied Command Transformation (ACT), the space domain is still in a very early phase of its development and is undergoing a cyber-like evolution in NATO.⁴⁰ As in the cyber domain, space in NATO is subject to a centralized command and control structure characterized by classification.

On the one hand, such an organizational form meets the need to protect activities in and through space. Still, on the other hand, it creates limitations in interoperability due to classification protection measures. How can NATO find a balance between providing structural and operational security to the space domain and enabling interoperability with other domains to contribute to NATO's 360-degree approach?

As Maness explains to his students, an essential attribute of space is that access and technology are expensive, and not every state can afford to spend the necessary funds on it.⁴¹ NATO, therefore, offers all allies a fair chance to share common interests in and through space. According to Johnson, individual nations such as the U.S., U.K., France, Germany, Italy, and Luxembourg are engaging and providing space applications for NATO to share. The United States, by far the most significant contributor, has a unique role. The U.S. also places cooperation with NATO in the U.S. Space Doctrine (Joint Publication 3-14 Space Operations) and, in this way, integrates NATO interests into national strategic considerations for the use of space.⁴² Despite its monopolistic position of power, the U.S. makes clear that a partnership with NATO is becoming increasingly important in an increasingly congested and contested space environment, contributing to greater resilience and, thus, to better space security.⁴³ According to ACT, NATO wants to generate further and more comprehensive space capabilities via a coordinative mode of use, with the NATO

³⁹ Johnson, "NATO in Space," 238.

⁴⁰ Alex Kaisler, unpublished data gathered from expert interviews with ACT, August 15, 2023

⁴¹ Maness, "Conflict and Cyberspace."

⁴² Joint Chiefs of Staff, *Space Operations*, Joint Publication 3-14 (Washington, DC: Department of Defense, 2020), 3–15, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14Ch1.pdf.

⁴³ U.S. Space Force, *Operations: Doctrine for Space Forces*, Space Doctrine Note (Washington, DC: Headquarters, United States Space Force, 2022), 12, <https://media.defense.gov/2022/Feb/02/2002931717/-1/-1/0/SDN%20OPERATIONS%2025%20JANUARY%202022.PDF>.

Space Centre as the central coordinating body and through voluntary framework mechanisms, as in cyberspace (SCEPVA).⁴⁴ With improved operational functions, NATO should be able to coordinate space domain operations in the future and with Space Domain Awareness (SDA), Operational Space Support (OSS), and Space Domain Coordination (SDC) to be able to conduct space military operations.⁴⁵ The space segment in NATO is in a dynamic phase of development. Interoperability, 360-degree approach, and MDO are essential for space in NATO and its strategic considerations. In considering the status of Space development, the question arises as to how NATO, as a complex allied entity, could make such capabilities available and interoperable to other domains.

5. A-SOF, Cyber, and Space Warfare, and a Required Symbiosis for MDO Capabilities

Sukhankin confirms that the Crimean invasion did not require cyber or Russian SOF units but their combined deployment.⁴⁶ Duggan's 2015 article further supports this analysis.⁴⁷ During the 2022 invasion of Ukraine, Russia relied in isolation on the advantage gained through cyber against a civil-military space service. Unlike the Crimean attack, this operation occurred for the first time in an armed conflict environment, and no synchronized kinetic measures took place between SOF and cyber. As Mueller, Jensen, Valeriano, Maness, and Macias analyze in *Cyber Operations during the Russo-Ukrainian War*, cyber operations must support an armed conflict in major theater wars to produce strategically relevant effects.⁴⁸ For a holistic use of cyber and space in the 21st-century conflict environment, physical forces such as A-SOF must unite both domains with all domains and integrate them appropriately to gain better interoperability. Research into appropriate forms of implementation is already in progress, and academic work shows that the need to combine SOF with cyber already exists. For example, van Hooren addresses the research

⁴⁴ "We Coordinate NATO Space Matters," NATO Space Centre, 2023, <https://ac.nato.int/missions/we-coordinate-nato-space-matters>.

⁴⁵ Alex Kaisler, unpublished data gathered from expert interviews with ACT, Juli 17, 2023

⁴⁶ Sukhankin, "Russian Special Operations Forces."

⁴⁷ Duggan, "Strategic Development of Special Warfare."

⁴⁸ Grace B. Mueller et al., *Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures*, 2023, <https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war>.

question, “How can Dutch Special Operations Forces enhance the national cyber capabilities to counter the hybrid threats the Netherlands currently faces?” He concluded that the symbiosis between SOF and cyber can be a strategic power tool and generate effects at the operational and tactical levels in hybrid conflicts.⁴⁹ This thesis broadens the perspective and looks at NATO.

The current approach in NATO to execute or provide offensive measures in or through cyber and space is operationally coordinated through central operations centers (NATO CyOC and NATO SpCen) and is subject to high OPSEC requirements.⁵⁰ In asking how better interoperability through integration/fusion can succeed without compromising OPSEC requirements, a logical link to the A-SOF in NATO arises. The A-SOF are joint and overlap all domains. A-SOF perfectly balances two apparent opposites. On the one hand, A-SOF operates under strict OPSEC requirements, and on the other hand, it has developed structures that allow sharing of information and bundle multinational capabilities. A-SOF is balanced and has a high value for NATO operability. Additionally, since A-SOF is familiar with the form of structural and operational security (OPSEC) and has been working with OPSEC for two decades, A-SOF may be able to provide structural solutions both for cyber and space, to improve the dilemma between OPSEC and interoperability and NATO’s 360-degree approach. There are no answers yet on implementing better interoperability between A-SOF, cyber, and space.

The dominant influence of the new dimensions on the strategic conflict environment demands clear adaptation steps of structures and capabilities between SOF, Space, and Cyber, according to USASOC Lieutenant General Jonathan P. Braga in Army Special Operations Forces (ARSOF) Strategy 2023.⁵¹ NATO has recognized those

⁴⁹ Jonas van Hooren, “The Imperative Symbiotic Relationship between SOF and Cyber: How Dutch Special Operation Forces Can Support Cyber Operations” (master’s thesis, Naval Postgraduate School, 2019), <http://hdl.handle.net/10945/64086>.

⁵⁰ Kaisler Alex, unpublished data gathered from expert interviews with Director of NATO’s Cyber Directorate, July 17, 2023

⁵¹ U.S. Army Special Operations Command, *Army Special Operations Forces Strategy* (Fort Bragg, NC: U.S. Army Special Operations Command, 2023), https://www.soc.mil/temp-pages/strategy/ARSOF_STRATEGY_2030.pdf.

demands and is ready to make necessary developments and adjustments.⁵² To enhance NATO's operational cross-domain capabilities, especially for counter and response operations,⁵³ NATO has to require integration of cyber capabilities with kinetic forces, according to scholars such as Ryan Maness, Gady, Franz-Stefan, and Alexander Stronell, and Allen, Patrick D.⁵⁴ Similarly, Schwarzbauer and Tuinman show how NATO would have to align and organize I-SOF in the context of Great Power Competition (GPC). They elaborate that A-SOF is also facing an adjustment period and need to recalibrate.⁵⁶ They explore how to improve the strategic impact of A-SOF, particularly concerning deterrence. There is a need to determine whether a higher grade of interoperability between A-SOF cyber and space can lead to a measurable improvement in NATO's 360-degree approach and better cross-domain ability regarding the NATO strategic concept 2022 and further substantiate the findings of Chace A. Falgout's research.

Political guidelines have been set in motion, providing military structures with the necessary framework for adjustments and development. Changes must follow, especially on the operational level. NATO and the NFS must approach political goals holistically with a long-term, pragmatic, and short-term perspective. Enhancing interoperability across all domains aligns with the strategic goal of a 360-degree approach. Still, NATO must implement it at the physical force level (operational level of the NFS and NCS). Based on the literature, this thesis identifies an MDO developmental step, a gap, and an area for action in NATO's view and how it shapes interoperability. First, holistic, long-term projects, such as SAS 143, are under development and contribute substantially to NATO's

⁵² NATO, *Brussels Summit Declaration* (Brussels: NATO Public Diplomacy, 2018).

⁵³ NATO, *NATO 2022 Strategic Concept*.

⁵⁴ Maness, Jensen, and Valeriano, *Cyber Strategy*.

⁵⁵ A. Ertan et al., eds., *Cyber Threats and NATO 2030: Horizon Scanning and Analysis* (Tallinn, Estonia: NATO CCDCOE Publications, 2020).

⁵⁶ Joost Martijn Tuinman and Matthias Johann Schwarzbauer, "The Strategic Utility of SOF in Great Power Competition: A NATO Perspective" (master's thesis, Naval Postgraduate School, 2022), <https://hdl.handle.net/10945/71557>.

MDO capability.⁵⁷ Secondly, structurally, no pragmatic solutions take place at the operational level. The forces seem to shy away from practical interdisciplinary exchanges for complexity reasons and the characteristic distinctions of cyber and space from the usual domains. In addition, because of the operational classification of many cyber and space activities, there is an organizational barrier that NATO must take to achieve the goal of MDO and a 360-degree approach. Third, due to the type-specific definition of SOF as a joint warfighting element, A-SOF is designated to develop a structural, organizational, and practice-oriented solution in the context of better interoperability to cyber and space.

D. HYPOTHESES

1. Research Assumption

Based on the literature review, the thesis determines that the MDO concept reflects NATO's 360-degree approach and intends to implement the considerations for better cross-domain interoperability operationally. With this finding, the thesis makes the following assumption for the development of the hypotheses:

NATO's strategic goal, to evolve modern warfare from JO to MDO as a 360-degree approach, directly relates to cyber and space domains and their interoperability with other domains and warfighting elements.

2. Research Statement

From the consideration of a historical example of a failed attack by Russia due to insufficient interoperability between offensive forces and cyber, from the development of the research question, a literature review on the state of development of A-SOF in the current strategic situation of NATO, and the defined characteristics of A-SOF, the thesis develops the following argument:

A-SOF enhances capabilities and interoperability to cyber and space with established structures in NFS and NCS, thus supporting the 360-degree MDO approach capability, contributing to NATO's strategic goals

⁵⁷ International Command and Control Institute (IC2I), "Agile Multi-Domain C2," in *23rd ICCRTS* (23rd International Command and Control Research and Technology Symposium (ICCRTS), Pensacola, FL: International Command and Control Institute, 2018).

Based on the argument, the thesis connects to the research question: “Given that there is a politically initiated adaptation process in NATO aiming at a 360-degree approach against hybrid threat scenarios and with a requirement of a direct dependency between Cyber, Space, and MDO capabilities, how can A-SOF contribute to this process and evolve better interoperability between A-SOF, Cyber, and Space?.”

3. Hypotheses

Derived from the assumption, argument, and research question, the section formulates the following four hypotheses (H1, H2, H3, H4) to support the argument. If the thesis confirms the hypotheses, then the thesis can answer the research question and identify solutions.

H1: A-SOF lacks significant expertise in cyber and space domains, hindering the development of sustainable interoperability.

Blessing, Elgin, Ewers-Peters, and Tiderman argue that good strategy requires knowledge of the operational environment and oneself.⁵⁸ This principle is especially true for NATO’s strategic adaptation measures, which are subordinate to the MDO and 360-degree approach goals. Before A-SOF undertakes adaptation actions with cyber and space, A-SOF must know the strategic and operational fundamentals of the new domains. Suppose most SMEs from all domains (A-SOF, cyber, and space) confirm that there is little foundational knowledge between the cyber and space domains and the warfighting element A-SOF. In that case, there is likely a substantial knowledge gap that NATO must first address.

H2: SOFCOM’s integral training facility, NSOU, holds significant importance in cultivating fundamental and supplementary knowledge for achieving interoperability with Cyber and Space.

⁵⁸ Blessing et al., “New Decade, New Challenges, and New Opportunities.”

NATO considers Education and Training a core activity to prepare NCS and NFS for current and future NATO missions along the LOA.⁵⁹ Knowledge transfer via NATO's training facilities enables the requirement authorities to achieve framework conditions set via Education and Training. NSOU, as SOFCOM's organic training facility, can quickly and directly implement SOFCOM's requirements for A-SOF through a targeted curriculum. The more SMEs consider knowledge distribution in different domains necessary for interoperability between A-SOF, Space, and Cyber, the more likely SOFCOM with NSOU is crucial for interoperability and achieving NATO 360-degree approach MDO capability.

H3: SOFCOM is uniquely qualified to advance interoperability with cyber and space to enhance NATO's 360-degree approach.

The allies established SOFCOM in 2010 based on a memorandum of understanding (MOU). Since then, SOFCOM has provided a hybrid command construct of MOU contributions and NFS elements within NCS. As Moon argues, A-SOF, by nature, has served NATO since its founding as an innovation engine for adaptations to challenging situations.⁶⁰ NATO's 360-degree objective is one such modern challenge that SOFCOM, with over 13 years of complex mission experience, can utilize. The more SMEs confirm that A-SOF characteristics and SOFCOM structures possess suitability potential for enhancing interoperability with the cyber and space domains, the more likely SOFCOM will be able to support the evolution of NATO's 360-degree approach.

H4: Integrating specific liaison elements enhances Space, Cyber, and A-SOF interoperability capabilities.

Lewis argues that cyber and space can only produce strategic value and a strategic success perspective in a more complimentary role with kinetic elements. Thus, liaison

⁵⁹ Supreme Allied Commander, Europe and Supreme Allied Commander, Transformation, *Bi-SC Education and Individual Training*, Directive (E&ITD) 075-007 (Mons, Belgium: Supreme Allied Commander, Europe and Supreme Allied Commander, Transformation, 2015), 8.

⁶⁰ Madeleine Moon, *NATO Special Operations Forces in the Modern Security Environment* (Brussels: NATO Parliamentary Assembly, 2018), 1, <https://www.nato-pa.int/document/2018-special-operations-forces-moon-report-169-dscfc-18-e-rev1-fin>.

elements would improve a holistic situational picture, enabling better situational assessments and thus leading to better-synchronized deployments.⁶¹ Suppose most of the SMEs surveyed confirm, based on outlined scenarios, that it would be reasonable, possible, and purposeful to use and exchange liaison elements for better support synchronization permanently. In that case, integration at the operational level is possible and even makes logical sense.

E. APPROACH

1. Chapter I: Introduction

For the research approach, the thesis chooses LTG Wendt's Problem-solving and first downs models (see Figure 1). The research question (RQ), ***“Given that there is a politically initiated adaptation process in NATO aiming at a 360-degree MDO approach against hybrid threat scenarios and with a requirement of a direct dependency between Cyber, Space, and MDO capabilities, how can A-SOF contribute to this process and evolve better interoperability between A-SOF, Cyber, and Space?”*** provides the core of the problem statement and sets the starting point. The objective of this work will be to propose suggestions, supported by research analysis, for decision-makers at the operational-strategic level (SOFCOM, NATO CyOC, and NATO SpCen) as options for action.

⁶¹ Lewis, *Cyber War and Ukraine*, 8.

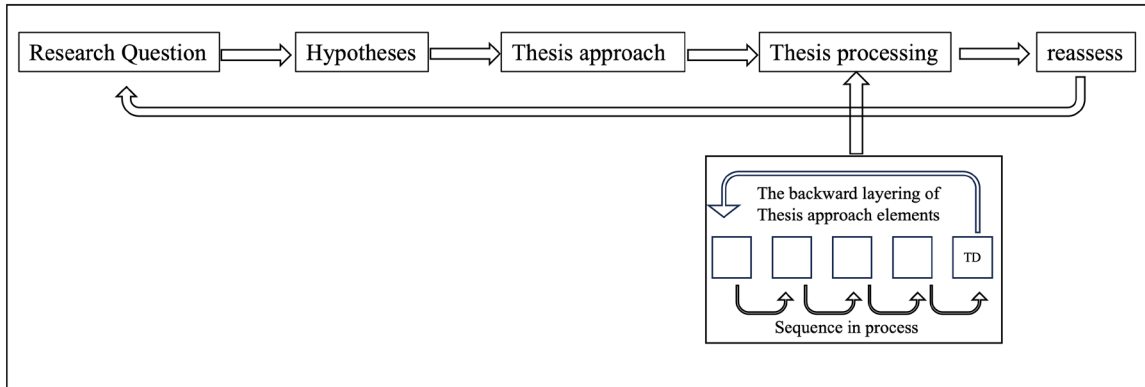


Figure 1. Thesis Development Approach⁶²

2. Chapters II and III: Background

As a baseline and background, Chapter II will elaborate on A-SOF, Cyber, and Space, how NATO organizes these domains, which structures NATO maps for the strategic and operational levels, which specific characteristics define cyber and space domains and A-SOF, and which conclusions regarding interoperability considerations can the thesis derive. For this purpose, the chapter uses the most recent but unclassified policy decision documents from the North Atlantic Military Committee (MC), operational-strategic documents such as NATO doctrines and executive orders, the so-called Allied Joint Publications (AJP), Bi Strategic Concepts between SHAPE and ACT, and recent scientific publications related to continues evolution of warfare in NATO on cyber, space, and A-SOF.

3. Chapter IV: Integrating Cyber, Space, and A-SOF

Chapter IV provides the core of the thesis. It illustrates three sections. The first section of Chapter IV describes the interview setup and how the thesis collected the data. In the second section, Chapter IV will conduct quantitative and qualitative analysis methods with the collected interview data and illustrate the results. In the third and final section, Chapter IV will assess the effects and conclude the assessment by defining the area of action for the strategic-operational level of A-SOF, Cyber, and Space.

⁶² Adapted from Eric P. Wendt, “Problem-Solving, First-Downs Models” (lecture, Command and Leadership course, DA 4500, Naval Postgraduate School, Monterey, CA, April 13, 2023).

a. Interviews and Data Collection

Interviews with experts from A-SOF, cyber, space, economy, and academia provide the basis for the subsequent analysis methodology. By conducting expert interviews, Chapter IV intends to capture and document an expert perspective in order to subsequently apply two different methods of analysis. The aim of the thesis is to test the hypotheses H1, H2, H3, and H4 quantitatively and qualitatively with the data collection as a basis, and thus to make a reliable statement for the assumption and the statement.⁶³

The thesis carried out the data collection with the help of interviews with SME. This chapter aimed to capture broad expert knowledge in the section and quantify qualitative assessments based on knowledge and years of experience. Twenty-six interviews were conducted with NATO leadership, decision-makers, and SMEs in strategic-operational layers and supplemented with perspectives from civil-commercial sectors and academia. The intention was to obtain a broad NATO military strategic perspective, such as those from commanding Generals in place, SHAPE Cyberspace Directorate, OSO, and ACT, but also an operational perspective from SOFCOM departments, CyOC, and the SOFCOM's training education institution NSOU. The method aims to augment the military view with an academic-scientific component. Interviews within CCDCOE, schoolers, and SMEs from the economy, particularly in strategy policy and training, will play a central role. The overall goal of the Data collection is to determine how practical interoperability of A-SOF and the cyber and space domains could occur. In addition, interviews with scholars such as Dr. Ryan Maness, who has been researching cyber and space for decades, and retired personnel in academia such as LTG (R) Eric Wendt, who experienced command and leadership in his military carrier and commanded SOFCOM 2019 – 2021, will provide another component and perspective, to test the Hypotheses.

The interview frame focused on three parts: firstly, covering an intuitive rather fundamental range by conducting closed-ended questions based on Hypotheses H1 – H4,

⁶³ SOFCOM, CCDCOE, ACT, Academia, SHAPE, economy, Interview recordings and summaries with SME, September 2023.

then secondly, a specific range of open-ended questions harvesting experts' knowledge for a later SNA on this data. Finally, the interview discussed two current scenarios to assess cyber, space, and A-SOF interoperability from different SME perspectives and to harvest closed-ended data as well as open-ended data for further analysis (see Appendix B. question-respondent matrix from 1 – 300). In all three parts of the interview, the chapter recorded qualitative SME responses such as tendencies, assessments, and evaluations in semantic differentiations on open-ended questions and binary assessments, with the goal that the thesis can compare the results in the analysis part.

b. Quantitative Analysis Method, Binary Distributions Analysis and Semantic Differentiations Distribution Analysis

In the data analysis portion, the thesis will use two methods to develop sufficient evidence about the four hypotheses H1, H2, H3, and H4, and subsequently conduct a focused evaluation. The first method of analysis will be a quantitative analysis from binary assessment of close-ended statements and semantically differentiated evaluations of open-ended questions.⁶⁴ The goal will be to graphically visualize the distribution of the binary and semantically differentiated expert responses so that the thesis can provide a first quantitative distinct perspective and test the hypotheses.

The thesis will apply BDA and SDDA to quantitatively analyze the expertise from up to 26 interviews and to harvest a tendency towards the Hypotheses. The first type of method in the section is the binary approach, where the thesis illustrates a positive or negative tendency of the experts by using closed-ended statements, such as hypotheses H1 – H4. A second type of method in the following section is the semantic differential evaluation of open-ended questions, where the thesis illustrates a tendency expression, with 1 = low ranking and with 5 = high ranking of answers.⁶⁵ The thesis will divide the approach of BDA and SDDA into three parts. Part I will focus on hypotheses H1, H2, H3, and H4. Part II will focus on six open-ended questions that highlight different facets of hypotheses

⁶⁴ Matthias Emde, “Open-Ended Questions in Web Surveys – Using Visual and Adaptive Questionnaire Design to Improve Narrative Responses” (PhD diss., Technical University Darmstadt, 2014), <http://tuprints.ulb.tu-darmstadt.de/id/eprint/4219>.

⁶⁵ Emde, chap. 5.

H1, H2, H3, and H4 (see Table 6). Finally, Part III will quantify experts opinion based on two OCO scenarios (see Appendix A).

c. Mixed Analysis Method, Semantic Network Analysis

The second analysis method is a quantitative-qualitative semantic network analysis (SNA).⁶⁶ This SNA methodology will process the documented SME responses (see Appendix B. Question-Respondent Matrix from 1 – 300) as a semantic network (SN) and analyze it by utilizing community detection algorithms and centrality-based algorithms. The goal is then to detect semantic network elements (SNE) with high centrality, and this allows the thesis to interpret the importance of such SNE regarding the RQ. The SNE then will provide the thesis with quantitative data such as the degree-, eigenvector, closeness-, and betweenness centrality.⁶⁷ Additionally, the SNA will then provide an opportunity of a qualitative analysis part. In that part, the thesis will apply and illustrate different semantic interpretations of the SNE and their quantitative analysis data. In this way, the thesis will generate an overall second perspective and will be able to further test the Hypotheses and develop a position toward the assumption and the statement.

4. Chapter V: Assessment

In the assessment chapter, the thesis presents an evaluation of the results derived from the BDA SDDA, and SNA. The comprehensive assessment will apply the hypotheses H1, H2, H3, and H4 criteria to conclude with findings. The goal of the Chapter V will be, to substantiate or refute the research assumption, *“NATO’s strategic goal, to evolve modern warfare from JO to MDO as a 360-degree approach, directly relates to cyber and space domains and their interoperability with other domains and warfighting elements.”* Further, the chapter will confirm or refute the research statement, *“NATO’s strategic goal, to evolve modern warfare from JO to MDO as a 360-degree approach,*

⁶⁶ Philipp Drieger, “Semantic Network Analysis as a Method for Visual Text Analytics,” *Procedia – Social and Behavioral Sciences* 79 (June 2013): 4–17, <https://doi.org/10.1016/j.sbspro.2013.05.053>.

⁶⁷ Sean F. Everton, “Social Network Analysis Network Topography” (DA 4600: Disrupting Dark Networks, lecture, Monterey, CA, September 14, 2022).

directly relates to cyber and space domains and their interoperability with other domains and warfighting elements.”

5. Chapter VI: Conclusion with Findings, Recommendations and Outlook

In Chapter VI, the thesis will develop specific products and solution options derived from the findings in Chapter V. The goal is to transfer the obtained results from the academic analysis in Chapter IV into comprehensible and militarily feasible products. This thesis links a scientific topic analysis and a structural and military-strategic reality. The solution options summarized in Chapter VI will be available to the cyber, space, and A-SOF community. The thesis will present the developed solution options to the military decision-making level in NATO in a separate briefing process.

The final step in Chapter VI is the summary and conclusion of the thesis. This chapter outlines an outlook and possible further research areas from cyber, space, A-SOF, interoperability in NATO, and the continuous evolution of warfare.

THIS PAGE INTENTIONALLY LEFT BLANK

II. PRINCIPLES OF THE FUNCTIONAL DOMAIN A-SOF

The Space-Cyber-SOF Triad describes an interdependent and mutually supporting relationship between cyberspace, space, and SOF. Special operations often rely upon the information advantage provided by cyberspace and space capabilities to see, sense, and stimulate to influence relevant populations or strike deep into the physical nodes of an adversary's system and assess the results. Cyberspace operations may rely on SOF's physical access and placement to deliver effects. Cyberspace, space, and SOF are unique in their global reach, persistence, endurance, and responsiveness. The cross-domain convergence of capabilities enables effects at all levels and can be seamlessly integrated into irregular warfare campaigns.

—LTG Jonathan P. Braga, Commander United States Army
Special Operations Command, 2023⁶⁸

The Commanding General of the United States Army's John F. Kennedy Special Warfare Center and School has described the interaction between Cyber, Space, and SOF as a convergence phenomenon and considers it a key aspect to maximize strategic effects.⁶⁹ The mentioned importance was also noted by NATO successively in 2016 and 2019 for cyber and space and consequently has ordered structural integration measures for NFS and NCS. To date, NATO in these two new warfighting domains is undergoing structural adaptation and development processes at different speeds but with many similar components. On the other hand, the A-SOF have been brought into NATO through an initiative as early as 2006.⁷⁰ Since then, the A-SOF have undergone extensive structural development and proven themselves in the NATO-led Afghanistan mission. To adequately answer the RQ, "Given that there is a politically initiated adaptation process in NATO aiming at a 360-degree approach against hybrid threat scenarios and with a requirement of a direct dependency between Cyber, Space and MDO capabilities, how can A-SOF

⁶⁸ U.S. Army Special Operations Command, *Army Special Operations Forces Strategy*, 15.

⁶⁹ Will Beaurpere and Ned Marsh, "Space, Cyber, and Special Operations: An Influence Triad for Global Campaigning," Modern War Institute, June 9, 2022, <https://mwi.usma.edu/space-cyber-and-special-operations-an-influence-triad-for-global-campaigning/>.

⁷⁰ "Riga Summit Declaration," NATO Official Texts, July 6, 2022, para. 24, https://www.nato.int/cps/en/natohq/official_texts_37920.htm.

contribute to this process and evolve better interoperability between A-SOF, Cyber and Space?,” the following chapter will develop foundations for A-SOF, cyber, and space to provide a framework to determine evidences that support or not support H1, H2, H3, and H4.

This chapter aims to first provide baseline knowledge of A-SOF as NATO’s joint and warfighting element (functional domain) to generate effective evaluation criteria for the following research in Chapter V. This chapter will also present fundamental considerations, principles, and operational characteristics in A-SOF applicable NATO doctrines (Allied Joint Publication [AJP]) and enacted policy guidance (Military Committee [MC]) so that NATO cross-domain capabilities and 360-degree approach can be optimized (see I.A.3 Research Question).

Second, the chapter will capture important key bodies, organizations, and elements in the structures of A-SOF strategic design, discuss critical processes or mechanisms that project significant impacts on the essential considerations and the operational characteristics to frame further research about how the integration of A-SOF, cyber, and space into NATO’s standing structure (NFS, NCS) can succeed (see I.A.3 Research Question).

Third, all sections will conclude by determining what potentials from A-SOF are already observable for follow-up research and what influences on the research question have already resulted. The following paragraph will do these steps with the conditions (see I.A.3 Research Question) of how A-SOF can better operate across the entire threat spectrum.

A. ALLIED SPECIAL OPERATIONS FORCES

Capable Special Operations Forces are essential to dealing with the challenges of today and tomorrow’s international security environment. International security competitors and those elements seeking to undermine the Alliance will increasingly attempt to do so via grey zone tactics – coercion, co-option, espionage, sabotage, political and economic pressure, propaganda, cyber tools, clandestine techniques, etc. These instruments allow competitors to attempt to remain below the threshold of Article 5, which would bring to bear the overwhelming power of the Alliance into a

conflict – which, at present, any opponent would lose. To parry competitors' grey zone tactics, Allied Special Forces can provide essential special reconnaissance, intelligence, and precision operations.

—Madeleine Moon, 2018, Report on NATO Parliamentary Assembly,
Defence and Security Committee (DSC) ⁷¹

SOFCOM is the operational strategic command element of A-SOF in NATO. SOFCOM is organized and led as a MOU organization by the United States as Framework Nation (FN), making it a unique C2 construct in NATO. In the following sections, Allied Joint Publication 3.5 Allied (AJP 3.5) Joint Doctrine for Special Operations (SO) is used to present NATO considerations for A-SOF, identify characteristics for SO, define principal tasks of A-SOF, and illustrate the organization, mission, and structure of SOFCOM. This section intends to lay the foundation for a holistic understanding of A-SOF, to understand specifics in the organization and design, and to derive the proper evaluation criteria to confirm or falsify H1, H2, H3, and H4 to answer the RQ. For this thesis, A-SOF must take the perspective from which A-SOF, as the most structurally developed element, must drive and shape the interoperability of cyber and space. First, this section's objective should be to identify structural nodes in the organizational structure of A-SOF that appear to be appropriate as points of connection for integration considerations with space and cyber. Second, the intent is to filter out A-SOF capabilities that can serve as composite capabilities and appear particularly conducive to integration. Third, this section intends to identify gaps in A-SOF's structure and capability portfolio that require mitigation to enable successful integration/fusion of cyber, Space, and A-SOF.

1. How NATO Considers Allied Special Operations Forces

NATO defines attributes that frame A-SOF and SO to generate strategic or operationally significant effects. SO are military activities conducted by specially designated and specially trained personnel. NATO must specifically organize and specially

⁷¹ Moon, *NATO Special Operations Forces in the Modern Security Environment*, 12.

equip these personnel, too. Then, these elements can conduct activities across the full spectrum of military operations.⁷²

The NATO military pillar maps different concept levels to implement NATO Military Committee requirements for policy considerations and objectives for Special Operations Policy.⁷³ NATO defines A-SOF conceptually on two levels. AJP 3.5 Allied Joint Doctrine for Special Operations builds the military-strategic layer for A-SOF. It provides a framework to plan, conduct, and support SO.⁷⁴ The AJP 3.5, Allied Force Standards (AFS) Volume X and Volume XI define the operational requirements.⁷⁵ The operational level also ensures the defined NATO standards through a certification process, which is mandatory for national SOF units. AFS Volume X and AFS Volume XI are classified and will not be considered further in this thesis. In this respect, the hybrid model of SOFCOM can react more flexibly than other forms of organization.⁷⁶

2. Characteristics of Special Operations in NATO

As SOFADs, through your ability to integrate, align and connect with the SOF network, you provide the breadth and depth of SOF to your organization and the ability to connect SOF and conventional forces through active campaigning.

—LTG Antonio Fletcher, Commander Allied-Special Operations
Command, May 4, 2023⁷⁷

⁷² NATO Standardization Office, *Allied Joint Doctrine for Special Operations*, 1.

⁷³ J. Bornemann, “Final Decision on MC 0437/2 Special Operations Policy” (Brussels: North Atlantic Military Committee, 2011).

⁷⁴ NATO Standardization Office, *Allied Joint Doctrine for Special Operations*.

⁷⁵ SHAPE, *Allied Command Operations Forces Standards Volume X: Special Operations Forces* (Mons, Belgium: SHAPE, 2018).

⁷⁶ Department of Defence, *North Atlantic Treaty Organization (NATO) Special Operations Headquarters (NSHQ)*, DOD Directive 3801.02 (Washington, DC: Department of Defense, 2019), <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/380102p.pdf?ver=2019-05-28-134326-997>.

⁷⁷ “NATO Special Operations Senior Leaders Convene in Slovakia,” NATO Special Operations News, May 5, 2023, https://portal.nshq.nato.int/home/sofad_conf_role_of_sof_and_collective_defence.

NATO characterizes SO as, by nature, joint and defines A-SOF as a functional domain. SO can be applied functionally across all military operational spectrums. Additionally, NATO provides domain-specific SOF (Army SOF, Maritime SOF, Air SOF) in the land, maritime, and air dimensions. A-SOF are subordinated to NATO occasionally through Troop-Contribution Nations (TCN). With this framework mechanism, NATO maintains no A-SOF elements subordinate to the NFS.

SO are strategic options that NATO executes through Joint Operations Areas (JOA) in a cross-domain approach (NATO-Forces integrate A-SOF Activities and conventional Operations in JOA) and in terms of the 360-degree approach (SO are to bring in various capabilities in a synchronized manner to maximize strategic effects). For this purpose, A-SOF embeds liaison and advisory (see Figure 2) as unique capability disciplines for coordination, synchronization, and de-conflicting means. An example of an integrative deployment of A-SOF with NATO's conventional force in a joint theater is that in the NATO Response Force (NRF). The NRF is a rapid reaction force that includes the A-SOF component as well as conventional troops and provides for the cross-domain deployment of A-SOF in an Area of Operation (AOO) or independently as battlespace owner in a Special Operations Area (SOA) in NATO's JOA.⁷⁸ Additionally, NATO projects the SO separately from conventional forces in uncertain, hostile, and politically sensitive environments, so clandestine means, classification, and concealment are supporting characteristics.

⁷⁸ "NATO Response Force," NATO What We do, July 27, 2022, https://www.nato.int/cps/en/natohq/topics_49755.htm.

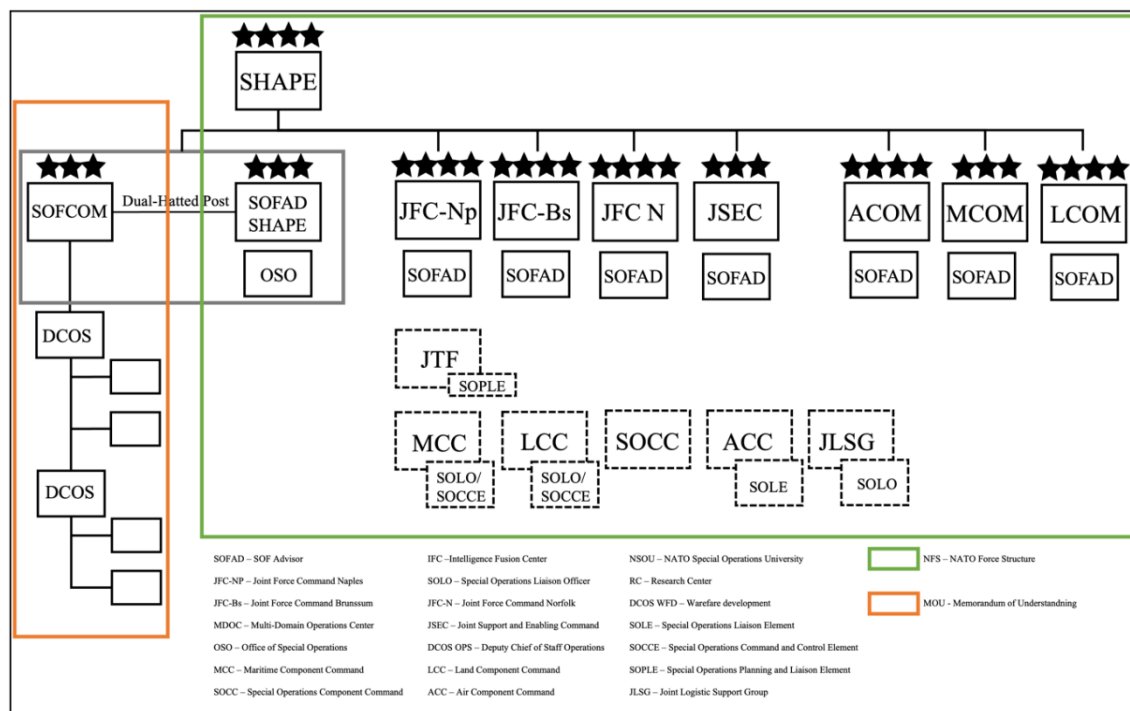


Figure 2. A-SOF in NATO.⁷⁹

SO can occur independently or in conjunction with conventional forces. SO can also occur on a sizeable interagency basis. In this way, A-SOF links military areas of responsibility and provides cross-agency cooperation. In most cases, SO require the support of non-SOF forces. As an integral part of NATO's Great Power Competition (GPC) campaign, SO continue to be characterized by A-SOF's use of specific and exclusive assets and by providing extensive liaison networks to decision-makers.⁸⁰

3. Principle Tasks for A-SOF in NATO

Special operations forces (SOF) offer the Alliance an additional and unique capability to achieve objectives and perform tasks to create strategic and/or

⁷⁹ Adapted from NATO Special Operations Headquarters (presentation, Mons, Belgium, August 23, 2023), 12.

⁸⁰ NATO Standardization Office, *Allied Joint Doctrine for Special Operations*, 1–2.

operational level effects that no other forces in North Atlantic Treaty Organization (NATO) are able to conduct.⁸¹

As a functional domain, SOF are primarily there for the national interests of individual states and are always subject to national caveats. Most NATO countries reserve SOF for strategic and politically relevant tasks. One such central task is, for example, the release of own national citizens from hostile environments (Hostage Release Operation (HRO)). Besides this very exclusive national functional task, there is also a NATO common need to employ A-SOF for NATO strategic and NATO political relevant interests.

In terms of Allied Joint Operations (AJO), NATO assigns its A-SOF three principal tasks in NATO's area of interest and responsibility: Military Assistance (MA), Special Reconnaissance (SR), and Direct Action (DA) (see Figure 3). The A-SOF principle tasks apply to support NATO's activities in the realms of Counter-insurgency (COIN), Counterterrorism (CT), Counter Hybrid Threats (CHT), HRO and countering proliferation of weapons of mass destruction (WMD) chemical, biological, radiological, and nuclear (CBRN) materials, and Faction liaison.⁸² As mentioned above, HRO is first subject to national caveats and bilateral or multilateral agreements of involved countries. NATO provides a complementary support platform to its allies to adequately ensure this national mission worldwide. For the TCN, a standard communication, coordination, and synchronization platform exists in the form of the NATO A-SOF structure.

⁸¹ NATO Standardization Office, 7.

⁸² NATO Standardization Office, 11–12.

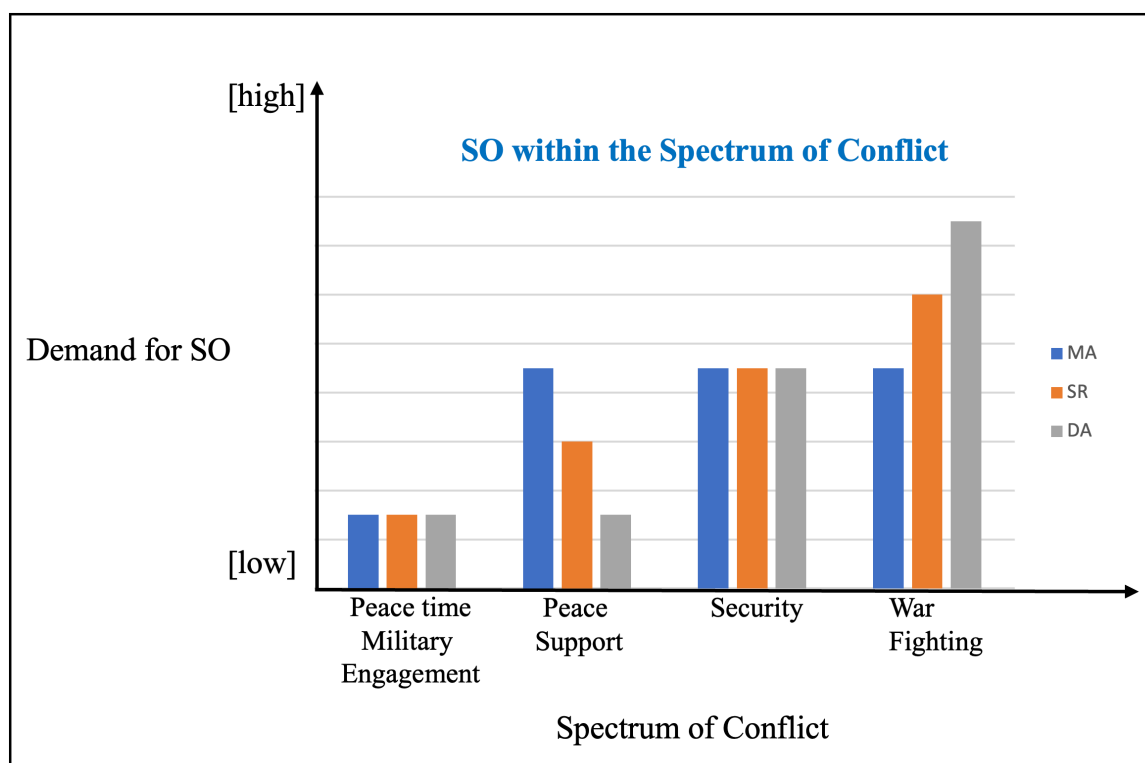


Figure 3. Qualitative Illustration of the Demand for SO in the Spectrum of Conflict.⁸³

a. Military Assistance, high value for peace support

MA covers a broad range of tasks for A-SOF, so with Training, Advising, Monitoring, Partnering, and Interagency Support, NATO can take preventive action in the early phases of conflicts.⁸⁴ At a very early stage, NATO can use the spectrum of MA to technically improve different areas of state actors, close capability gaps, bring together local and regional security forces from other sectors, and thus increase a state's effectiveness of action. With MA, NATO can influence conflict regions in the interest of allies and send strategic signals.⁸⁵

⁸³ Adapted from NATO Standardization Office, 3.

⁸⁴ Eric P. Wendt, "Comprehensive Defense, a Whole-of-Society Approach via Irregular Forces," *Special Warfare* 34, no. 2 (June 2021): 2–13.

⁸⁵ NATO Special Operations Headquarters, *Comprehensive Defence Handbook—Vol I*, Edition A Version 1 (Mons, Belgium: NATO Special Operations Headquarters, 2020), <https://www.nshq.nato.int/library>.

b. Special Reconnaissance is necessary for battlefield preparation and PIR

SR expands NATO's Joint Intelligence, Surveillance, and Reconnaissance (JISR) spectrum to include environmental surveillance, threat assessment, target assessment, and post-action reconnaissance capabilities. SR can complement other and primarily technical information collection methods and, in this way, usually provides a required augmented component for confirmation. For commanders and other strategic decision-makers, A-SOF use SR capabilities to collect sensitive and time-critical information classified as a Priority Intelligence Requirement (PIR). NATO strategic leadership can deploy SR in the context of PIR at a vast distance and at very early planning stages to open up planning and action options in the interest of NATO.⁸⁶

c. Direct Action, small footprint with a significant strategic outcome

DA forms the visible kinetic capability spearhead of A-SOF. Under the principle of relative superiority, A-SOF can conduct raids, ambushes, assaults, terminal guidance operations, recovery operations, and precision destruction operations. A-SOF execute these actions with a numerically small footprint but with a significant outcome against an adversary's critical elements. NATO can deploy these SO in a stand-alone approach or within the AJO framework.⁸⁷ With DA, NATO can focus on strategic targets, operationally significant enemy elements, or critical tactical operations. Through DA, A-SOF can seize, destroy, or capture targets; furthermore, with DA, A-SOF can inflict strategic damage to an adversary or recover or protect strategically relevant objects.⁸⁸

As the SO demand carrier, NATO must create all structural conditions to enable SO execution (planning, preparation, execution, return, and post-processing). For the planning of SO, operational security and integrated mission planning, with coordination of timing, definition of planning priorities, integrated approach of available resources, and synchronization of forces are crucial. A-SOF deployment (employment considerations)

⁸⁶ NATO Standardization Office, *Allied Joint Doctrine for Special Operations*, 8–9.

⁸⁷ William H. McRaven, "The Theory of Special Operations" (master's thesis, Naval Postgraduate School, 1993), 5–11, <https://hdl.handle.net/10945/14838>.

⁸⁸ NATO Standardization Office, *Allied Joint Doctrine for Special Operations*, 9–10.

must focus on critical operations and prioritize targets.⁸⁹ SO require the best possible intelligence situational awareness in the planning phase because SO generally affect the political, military, economic, social, infrastructure, and information (PMOSII) environments. For this, NATO must ensure all available intelligence resources within JISR and through intelligence fusion in the J2 all-source cell (ASC) and a PMOSII-tailored targeting process.⁹⁰

Other considerations in combat, C2, and sustainability are vital in successful SO execution. The requirement, coordination, and synchronization of Combat Support (CS) elements such as Explosive Ordnance Disposal (EOD), Close Air Support (CAS), and other CS elements are essential for increasing fighting power. A specific form of Combat Service Support (CSS), such as strategic airlift, special medical care, and forward base facilities, such as Forward Operation Base (FOB) through FN or Host Nation (HN) support, significantly increases A-SOF sustainability. SO also require stable and globally functioning C2 support. CIS capabilities that enable global communications with and for A-SOF enable dislocated strategic C2.⁹¹

4. Key Elements within the A-SOF Organization and SOFCOM Mission

SOFCOM coheres the NATO SOF enterprise to establish a theatre architecture for the SOF Domains. SOFCOM will build and operate an organization to deliver SOF effects in a rapidly evolving strategic context. Furthermore, SOFCOM will build and enable NATO SOF capability and interoperability, with a renewed focus on developing strategic advantages to deter and defend against all threats from all directions.

—Allied Special Operations Forces Command (SOFCOM), 2023,
Statement to Adapting to Change⁹²

⁸⁹ NATO Standardization Office, *Allied Joint Doctrine for Joint Targeting*, AJP-3.9 (Brussels: NATO Standardization Office, 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1033306/AJP-3.9_EDB_V1_E.pdf.

⁹⁰ NATO Standardization Office, *Allied Joint Doctrine for Special Operations*, 33–36.

⁹¹ NATO Standardization Office, 36–42.

⁹² “Allied Special Operations Forces Command (SOFCOM) – NSHQ Portal,” accessed August 23, 2023, <https://cyber.nshq.nato.int/> Transforming SOF.

SOFCOM provides the operational and strategic leadership for A-SOF in NATO. NATO and the MOU are organizing the SOFCOM to ensure the essential mission of providing strategic advice, developing A-SOF towards the SOFCOM vision, and synchronizing activities within NCS and NFS (see Figure 4).

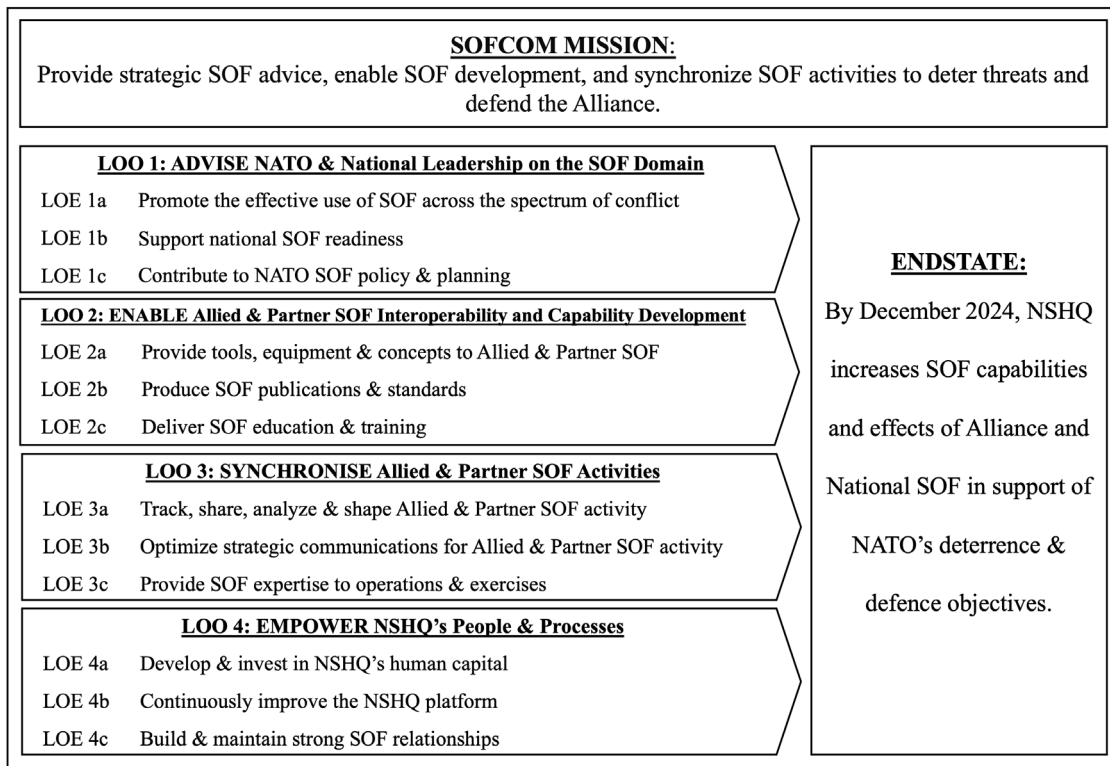


Figure 4. SOFCOM Mission, Vision, the Lines of Operation (LOO) and the Lines of Effort (LOE).⁹³

In Figure 5, one can see the SOFCOM's unclassified C2 structure. To perform the four LOOs (advise, develop, and synchronize), one can divide the SOFCOM into three areas (Advising responsibilities, FN responsibilities, and Operational responsibility), with the commander being the central interface for all areas.

⁹³ Source: Allied Special Operations Forces Command, "NSHQ's 2-Year Strategic Approach (2022-24)" (Mons, Belgium: SOFCOM, 2022), 1.

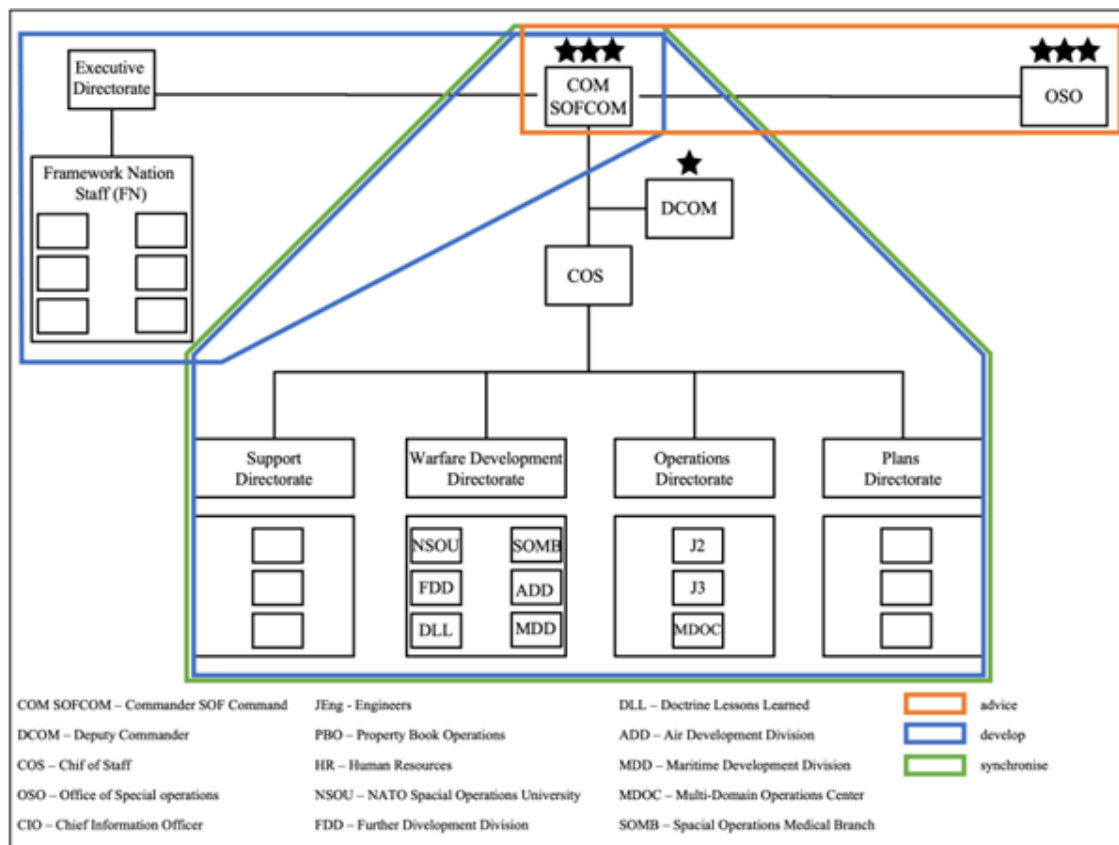


Figure 5. Abstract Illustration of SOFCOM's Organizational and Command Structure.⁹⁴

a. Office of Special Operations (OSO)

SHAPE SOFAD/SOFCOM Commander (COM SOFCOM) leads the OSO. With OSO, COM SOFCOM covers the strategic command level for A-SOF in NATO. OSO is the specialist advisor to the Command Group SHAPE and must ensure A-SOF unity for NATO's strategic operations, planning, and support efforts. From this strategic starting point, the OSO has the authority to issue directives to the SOFADs in the NCS and NFS. COM SOFCOM is the senior NATO SOFAD and advises SACEUR that all SO is subordinate to the NCS and is structurally not mapped into SOFCOM. Organizationally,

⁹⁴ Adapted from Allied Special Operations Forces Command, "Allied Special Operations Forces Command (SOFCOM)" (Mons, Belgium: Allied Special Operations Forces Command, August 23, 2023), 1.

the OSO is very much an integral part of SOFCOM. For this reason, the COM SOFCOM serves in a dual lead role.⁹⁵

b. Executive Director element

The Executive Director element is embedded in the SOFCOM structure to ensure the FN's responsibility. In addition to the advisory role and directive authority in the NCS and NFS, the COM SOFCOM must provide leadership to SOFCOM, which was agreed to under the MOU on September 12, 2011, and placed under the United States as FN. Within this staff department, SOFCOM ensures three essential elements by the FM. First, the U.S. provides necessary funding for the sustained operation of SOFCOM. Second, the U.S. delivers the logistical support for the operations of SOFCOM, and third, the U.S. offers additional supporting personnel not foreseen under the MOU.⁹⁶

c. SOFCOM, a small footprint in NFS

SOFCOM, as an MOU organization, structurally A-SOF has a small footprint in NFS. NATO subordinates the SOFCOM through operational command (OPCOM) to SACEUR but doesn't map it within NFS. SOFCOM provides the backup for OSO and NATO forces in the NFS on order and as required. On behalf of SACEUR, SOFCOM provides the competency hub for various operational and strategic responsibilities. SOFCOM must enable the integration of A-SOF and other NATO forces. It must also develop and ensure the interoperability of A-SOF, NATO forces, and partner nations through collaboration, training, education, and evaluation.⁹⁷ SOFCOM's staff departments form the core and working engine of SOFCOM. Here, various specialist elements combine to implement many strategic and operational tasks under the Operational Responsibility. SOFCOM divides tasks among four directorates led by Deputy Chief of Staffs (DCOS) in Support, Operations, Plans and Policy, and Warfare Development. The subdivisions listed in Figure 5 represent a broad range of competencies at the operational-strategic level.

⁹⁵ NATO Standardization Office, *Allied Joint Doctrine for Special Operations*, 15.

⁹⁶ Department of Defence, *North Atlantic Treaty Organization (NATO)*.

⁹⁷ NATO Standardization Office, *Allied Joint Doctrine for Special Operations*, 15–16.

d. NSOU, SOFCOM flagship, an essential component for development

NSOU organically subordinates to SOFCOM and is the central and most important educational entity for the A-SOF (see Figure 5). It flexibly translates the authority's requirements into a targeted curriculum and thus contributes significantly to the A-SOF's development and operational A-SOF readiness.⁹⁸ Admiral McRaven, the visionary behind the consolidation of all A-SOF into the present-day SOFCOM, has consistently advocated for the establishment of an integrated A-SOF educational institution.⁹⁹ This educational institution should serve two main objectives. First, this institution should be directly subordinated to the A-SOF requirement authority to provide the consolidated requirements for A-SOF directly, flexibly, and without further structural or bureaucratic obstacles. This approach has proven itself and has been a successful model, particularly for the Afghanistan mission with its standardized A-SOF requirements. Second, with the largest share of the FN budget for SOFCOM, this educational institution should become the flagship for SOF command in strategic communications and a HUB for A-SOF global networking. This approach has also proven successful to date. NSOU is the most critical component of SOFCOM today and contributes significantly to the readiness and development of operational A-SOF.

5. A-SOF Potential for Further Research

In summary, the A-SOF open five areas of action that the thesis needs to test concerning hypotheses H1 – H4 in the analysis chapter. These include the organizational form of SOFCOM as an MOU FN entity, the NSOU training institution and its role, the A-SOF's dependence on preconditions for deployments, and the A-SOF's experience with FN contribution mechanisms.

⁹⁸ Allied Special Operations Forces Command, "NATO Special Operations University: The Crossroads of NATO SOF," NATO Special Operations University, 2023, <https://www.nshq.nato.int/nsou>.

⁹⁹ John D. Gresham, "Interview with Adm. William H. McRaven, USN, Commander, U.S. Special Operations Command," Defense Media Network, June 29, 2012, <https://www.defensemedianetwork.com/stories/interview-adm-william-h-mcraven-usn-commander-u-s-special-operations-command/2/>.

a. *SOFCOM, as an MOU organization in NCS, offers chances for integration.*

However, NATO's NFS provides only a small strategic and operational command element for A-SOF. Structurally, only small advisory capabilities exist in the NFS, the so-called Special Operations Forces Advisor (SOFAD), and the Office of Special Operations (OSO). In addition to the NFS and its integrated advisory elements, NATO has established SOFCOM as an operational strategic command in the form of an MOU since 2010. ACO integrates this command into the NCS but organizes, maintains, and leads it through the United States as the FN. The mix of NFS and MOU in the NCS provides NATO integration opportunities between A-SOF, cyber, and space. Regarding obstacles such as bureaucracy, culture, political interests, regulations, and national caveats, NATO must practically overcome these obstacles to successfully implement integration/fusion and provide the goal of a 360-degree approach.¹⁰⁰

b. *Liaison as an essential pillar*

According to the A-SOF doctrine, liaison is a crucial capability pillar of A-SOF and highlights SOFCOM's cross-domain capability. A-SOF can thus operate synchronously across multiple theaters and coordinate with all participating theater authorities. This perspective indicates a need for SOFCOM to integrate cyber and space into liaison naturally.

c. *Precise conditions to generate operational-strategic reasonable effects with A-SOF*

In summary, the section shows that NATO requires precise conditions and complex constraints if NATO wants to generate operational-strategic reasonable effects in a dynamic multi-domain environment of NATO activities (COIN, CT, CHT, HRO, WMD, CBRN through principal tasks of the A-SOF (MA, DA, SR) in SOA or AJO). Capabilities from the domains of cyber and space can significantly improve and optimize the mentioned precise conditions and complex requirements, such as ASC, precise targeting,

¹⁰⁰ Gerald G. Brown et al., "How U.S. Air Force Space Command Optimizes Long-Term Investment in Space Systems," *Interfaces* 33, no. 4 (2003): 1–14, <https://doi.org/10.1287/inte.33.4.1.16369>.

synchronization of all forces, operation security, strategic C2, etc. This work must determine to which degree of improvement an integration/fusion of the cyber and space domains in SOFCOM can lead.

d. SOFCOM as a flexible FN mechanism

The organization and structure of SOFCOM with the Advising, FN, and Operational responsibility components do not exhibit a novel or unique command structure. However, in the NCS and NFS, SOFCOM is a unique element that provides solutions to challenges resulting from modern multi-domain requirements. Through its FN mechanisms, SOFCOM can respond to situational changes with significantly more flexibility than other NATO organizations. Through the Advising Responsibility component, SOFCOM offers the new domains of cyber and space an already standing and effective liaison system that can be utilized and expanded as a blueprint. Finally, with the SOFCOM Staff, SOFCOM can not only perform the C2 function (DCOS Ops with J2, J3, and Multi-Domain Operations Center [MDO]) but also drive education and development (DCOS Warfare Development [WFD]). With the background research, this section indicates not whether it would be purposeful to integrate cyber and space into SOFCOM but how NATO can integrate cyber and space into SOFCOM and with each other. The research in the analysis chapter must determine whether the SOFCOM is uniquely qualified to advance interoperability with cyber and space to enhance NATO's 360-degree approach.

e. NSOU, the bridge to knowledge and interoperability

NSOU is uniquely embedded in the SOFCOM command structure as A-SOF's central training facility, providing SOFCOM with greater freedom of action than other operational commands. In addition, NSOU is NATO certified and connected to the NATO Education and Individual Training Directive and thus interconnected with all other NATO training facilities. The fundamentals of the A-SOF indicate that NSOU could develop courses of action to better connect cyber and space to SOFCOM and thus contribute. Evaluation of the SME interviews should determine whether SOFCOM's organic training facility, NSOU, is substantively vital to developing better interoperability between A-SOF, cyber, and space. (See H2 in I.A.3).

III. PRINCIPLES OF CYBER, SPACE DOMAINS

Today, small teams of special operators armed with asymmetric cyber-tools, irregular warfare tactics, and mass disinformation can have truly strategic effects.

—General Joseph L. Votel, 2014, USSOCOM¹⁰¹

As early as 2014, the commanding general of USSOCOM at the time, General Joseph L. Votel, recognized that combining SOF capabilities with those of cyber offered strategic potential. As in previous chapters, the following chapter lays the baseline for Cyber and Space to adequately answer RQ: “Given that there is a politically initiated adaptation process in NATO aiming at a 360-degree approach against hybrid threat scenarios and with a requirement of a direct dependency between Cyber, Space and MDO capabilities, how can A-SOF contribute to this process and evolve better interoperability between A-SOF, Cyber and Space?” This chapter also defines the framework in which the thesis will prove or falsify the four hypotheses (H1, H2, H3, H4).

This chapter aims to first provide baseline knowledge of cyber and space as the most recent NATO domains to generate effective evaluation criteria for the following research. This chapter will also present fundamental considerations, principles, and operational characteristics in and through these domains applicable NATO doctrines (Allied Joint Publication [AJP]) and enacted policy guidance (Military Committee [MC]) so that NATO cross-domain capabilities and 360-degree approach can be optimized (see I.A.3 Research Question).

Second, the chapter will capture important key bodies, organizations, and elements in the structures of the three domains and discuss critical processes or mechanisms that project significant impacts on the essential considerations and the operational characteristics to frame further research about how the integration of A-SOF, cyber, and

¹⁰¹ Duggan, “Strategic Development of Special Warfare,” 46.

space into NATO's standing structure (NFS, NCS) can succeed (see I.A.3 Research Question).

Third, all sections will conclude by determining what potentials from cyber and space are already observable for follow-up research and what influences on the research question have already resulted. The following paragraph, in accordance with the conditions outlined in I.A.3 Research Question) will take these steps to explore how A-SOF can better support and be better supported by cyber and space across the entire threat spectrum.

A. CYBER IN NATO

In an increasingly networked world, NATO needs to adapt to a global strategic environment drastically evolved, where both state and non-state actors are able to employ conventional, unconventional and hybrid methods, and are empowered to shape the narrative within a continuous information cycle. In this context, the Alliance will need to integrate, adapt and enhance the speed, connectivity and effectiveness of its overall Strategic Communications (StratCom) effort. The role of digital media and the accessibility of information systems have created a situation in which no Alliance decision or action should be taken without considering its potential impact on the Information Environment (IE) and its audiences. The ubiquitous nature of information and the potential strategic ramifications of tactical actions add to the challenge faced by NATO Commanders.

—MC 0422/6, 2019, NATO Military Policy for
Information Operations (IO) ¹⁰²

Cyberspace has been a military domain for NATO since the 2016 Warsaw Summit.¹⁰³ The idea of a defense-oriented alliance structure reflects a complex and very diverse organizational structure and very framed cyber capabilities. The military-political NATO cyber considerations are stated in the following sections to get a general understanding of cyberspace from the NATO perspective. Then, this section will characterize cyber operations (CO) in terms of NATO, outline their principles, and describe

¹⁰² North Atlantic Military Committee, *NATO Military Policy for Information Operations MC 0422/6* (Brussels: North Atlantic Military Committee, 2019), 2.

¹⁰³ “Warsaw Summit Communiqué,” NATO Official Texts, July 9, 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

different CO types. In the further section, the chapter highlights which effects procured by CO, which particularity affiliating to OCO, and what is behind the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) framework mechanism. The section concludes by illustrating extended NATO organizations and NATO partnerships that also maintain cyber capabilities. With this fact-finding, the section intends, on the one hand, to lay a foundation of understanding for the domain of cyber in NATO.

On the other hand, the following paragraph aims to make deductions from which it can develop questions for experts and frame evaluation criteria. In further research, the thesis will adequately answer the hypotheses and, finally, the research question. Ultimately, this section intends to elaborate logical fields of action for possible integration options between cyber, space, and A-SOF to extend the investigations with already identified conclusions.

1. How NATO Considers Cyberspace

Militarily, NATO conceptually implements the NATO Allies' policy for Information Activities (IA) through the MC in the Allied Joint Doctrine for Cyberspace Operations, Allied Joint Publication (AJP 3.20) as an IA discipline. As part of the NATO Operational Architecture, the overall purpose is to ensure the planning, executing, and assessing of operations in cyberspace and to organize principles of joint command and control (C2).¹⁰⁴ In the following section, the thesis-relevant components from AJP 3.20 are considered and used as essential knowledge for the investigation.

According to NATO, cyberspace is not boundless; the allies define a cyber structure and clear distinctions from the domains of land, air, sea, and space. First, humans have created cyberspace artificially, and computers projected cyber digitally. Unlike the natural dimensions, one cannot sense cyber and thus can only be imagined cognitively. Second, this space itself is subject to continuous adaptation and change. These two characteristics differ cyber from the other natural domains and require a unique strategic outlook. To

¹⁰⁴ NATO Standardization Office, *Allied Joint Doctrine for Cyberspace Operations*, AJP-3.20 (Brussels: NATO Standardization Office, 2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1.pdf.

understand this domain, NATO describes it with the so-called “Three-layer Model” (see Figure 6) consisting of the cyber persona-layer (virtual identity), the logical layer (entities manifested in code or data), and a physical layer (entities displayed in hardware components, physical personnel). Third, cyberspace is not subject to geographic constraints but is still under national authority.

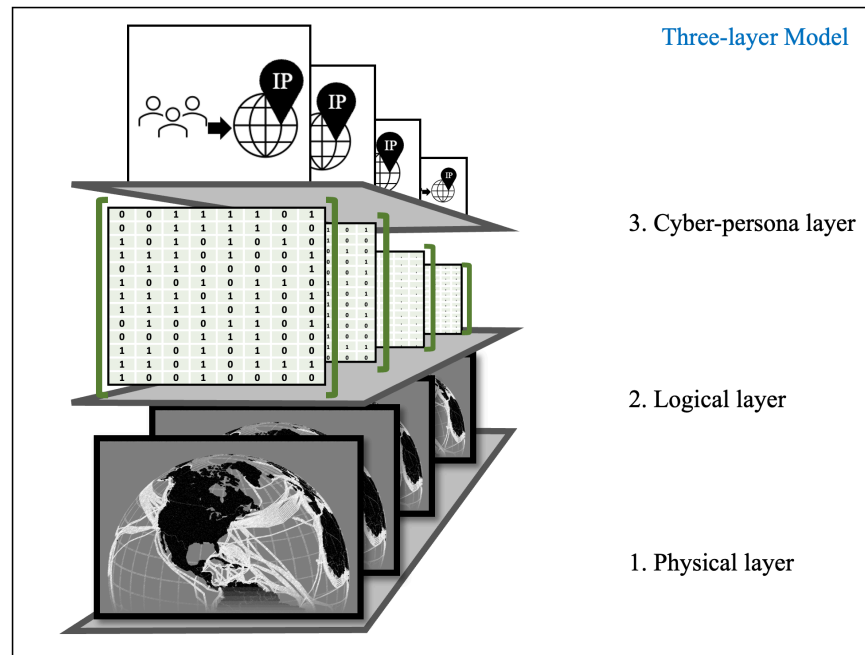


Figure 6. The Three-Layer Model, how NATO considers Cyberspace.¹⁰⁵

These distinctions make it challenging to assign operational boundaries to cyberspace (see Figure 7) and to set cyber capabilities according to the three components of fighting power.

¹⁰⁵ Adapted from NATO Standardization Office, 3.

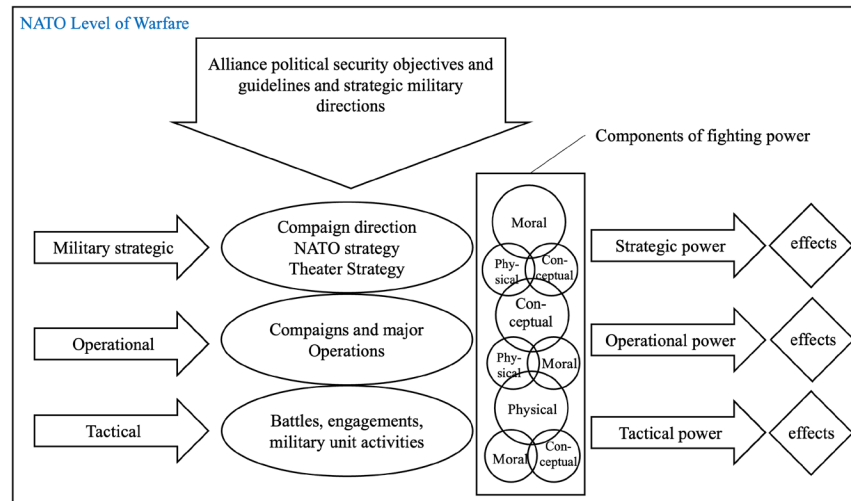


Figure 7. NATO Level of Warfare¹⁰⁶

2. Characteristics, Principles, and Types of CO in NATO

The growth of a global, interconnected cyberspace domain represents the most significant strategic development since 9/11. Activities and operations in, through, and from cyberspace now offer states the means to augment their power, degrade or usurp the power of others, and gain strategic advantage through competition without triggering armed conflict. Our adversaries have learned this and are leveraging it against us.

—General Paul M. Nakasone,
Commander U.S. Cyber Command, 2019¹⁰⁷

Allied Command Operations (ACO) considers CO one resource that comprehensively enables the foundation for NATO IA planning and execution and contributes to NATO operations. ACO views CO with two lenses. First, CO can contribute to joint operations under AJP 3 (Allied Joint Doctrine for the Conduct Operations). Through synchronization, NATO can utilize CO as a force multiplier and enabler, Combat Supporter, and Command and Control (C2) supporter for joint functions. The second perspective focuses on CO as independent operations with cyber-specific targets. NATO

¹⁰⁶ Adapted from Joint Chiefs of Staff, *Joint Publication 1 Volume 1 Joint Warfighting* (Washington, DC: Joint Chiefs of Staff, n.d.), III–2.

¹⁰⁷ Nakasone, “A Cyber Force for Persistent Operations,” 11.

can employ OCO or DCO to influence the enemy's cyber layer (three-layer model), thus minimizing the enemy's fighting power. This thesis will look at the two angles (OCO, DCO) on CO to find tie-ins to A-SOF and Space.

COs can act as joint function multipliers for a wide range of capabilities in the joint functions framework and thus act as cross-capabilities support. COs provide commanders with improved options for C2, sustainment, firepower, maneuver, intelligence, information superiority, civil-military cooperation, and force protection. In addition to OCO and DCO, both activities in and through cyberspace, the cyber directorate maintains two other capabilities, Electromagnetic Operations (EMO) and CIS Infrastructure Operations. Both types of NATO conceptualize and organize additional doctrines. AJP 3.6 Allied Joint Doctrine for Electromagnetic Warfare covers EMO, which NATO classifies and which the thesis cannot use in further research.¹⁰⁸ AJP 6 Allied Joint Doctrine for Communication and Information Systems covers CIS Infrastructure Operations.¹⁰⁹

ACO is embodying the cyber capabilities in the Cyber Directorate. NATO distinguishes five different CO characteristics (reach, asymmetric effects, anonymity, time, and speed), five CO principles (cyber security (CS), surprise, concentration of force, maintenance of morale, and freedom of action), and two CO types, OCO and defensive cyber operations (DCO), when CO is applied. The attribution effect is considerably different and thus differs significantly from those of other domains. Accurate naming is critical to capture the specifics of the cyber domain and compare it with other domains to conclude clearly.¹¹⁰

As a defensive alliance, NATO executes DCO. Thus, for only the CIS, EMO, and DCO capabilities, NATO operates the NATO Communication Information System Group (NCISG) as an organic element. Primarily, DCO can prevent adversary and hostile CO in

¹⁰⁸ NATO Standardization Office, *Allied Joint Doctrine for Electronic Warfare*, AJP 3.6 (Brussels: NATO Standardization Office, 2020).

¹⁰⁹ NATO Standardization Office, *Allied Joint Doctrine for Communication and Information Systems*, AJP-6 (Brussels: NATO Standardization Office, 2017), https://www.coemed.org/files/stanags/01_AJP/AJP-6_EDA_V1_E_2525.pdf.

¹¹⁰ NATO Standardization Office, *Allied Joint Doctrine for Cyberspace Operations*, 4.

or through cyberspace against NATO nations. For this task, appropriate means and cyber capabilities are to be maintained in a planned manner to prevent an adversary from its offensive intent. DCO aims to prevent malicious activities by adversaries and other actors to generate mission assurance (MA) by protecting networks and systems with NATO's CIS capacity. Furthermore, DCO aims at preserving the ability to use cyberspace to enable principles such as freedom of action in the network. DCO can initiate OCO and must be synchronized closely.¹¹¹

NATO does not exercise OCO (see Figure 8) or provide organic offensive cyber operations capabilities (OCOC). OCO are projected as independent sovereign national operations (not by NATO), and through a cooperation process, NATO participation in the achieved effects. The following section explains how NATO projects OCO and how NATO utilizes OCO effects. Even if NATO does not maintain organic resources for OCO, NATO still has a particular interest in being involved in the impact that supports and enables the idea of defense.

¹¹¹ NATO Standardization Office, 16–17.

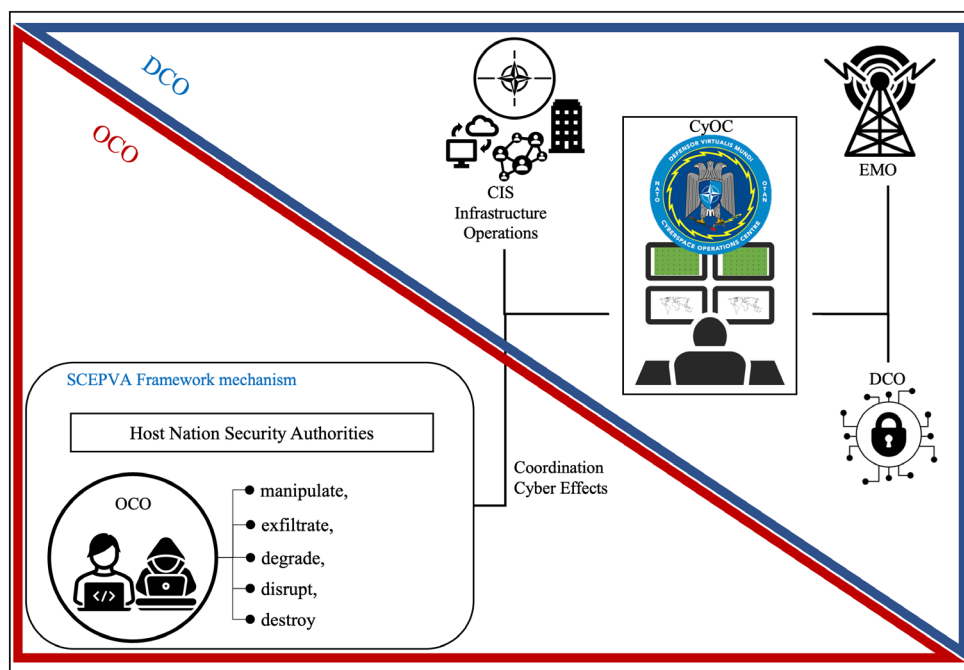


Figure 8. Responsibility and Task Spectrum of the CyOC in the Cyber Directorate SHAPE.¹¹²

The projection of CO takes place on the logical layer (Figure 6), creating effects that affect other layers of cyberspace and other domains. Due to the greater density of military, civil, and economic interconnections and dependencies in cyberspace, there is a higher risk of undesirable effects. Therefore, NATO must understand CO in its full scope (including OCO) to draw proper conclusions for its defense and minimize undesirable side effects (see Figure 7). The following results of CO are defined and aligned with Standardization Agreement (STANAG) 2287:¹¹³ Table 1 lists the STANAG 2287 terms with their respective effects and divides these into OCO and DCO.

¹¹² Adapted from Stelian Cristea, “NATO Cyberspace Operations Centre” (presentation, Mons, Belgium, March 5–6, 2023), 5

¹¹³ NATO Standardization Office, *Task Verbs for Use in Planning and the Dissemination of Orders*, STANAG 2287 Lo (edition 1) (Brussels: NATO Standardization Agency, 2006).

Table 1. Cyber Effect through DCO and OCO by STANAG 2287¹¹⁴

Effects	Definition	Type
Secure	to prevent compromise, the confidentiality, integrity, and availability (CIA) parts of a network	DCO
Isolate	to block adversaries' lines of communication within its Cyberspace	DCO/OCO
Contain	to stop the further spreading of adversaries' CO	DCO
Neutralize	to render malicious CO incapable of affecting Cyberspace	DCO/OCO
Recover	to restore the freedom of action	DCO
Manipulate	to affect adversaries' Systems or networks to support NATO's objectives	OCO
Exfiltrate	to gain possession of adversary's information to support NATO's objectives	OCO
Degrade	to deny access and to reduce adversaries' freedom of action	OCO
Disrupt	to completely deny access to or operation of an adversary's asset for a period of time	OCO
Destroy	to deny access entirely and irreparably to, or operation of, an asset	OCO

3. SCEPVA Framework Mechanism, OCO, and the Role of CyOC

As an organization, NATO does not provide offensive cyberspace operations (OCO). On the other hand, in conflict, NATO might come to a secular situation with requirements for offensive cyberspace effects. And therefore, NATO has a mechanism with allied nations, who sovereignly voluntarily would provide offensive cyber effects (Sovereign Cyber Effects Provided Voluntarily by Allies [SCEPVA]) if required, and possible.

—Major General Frank Schloesser, COM NCISG and DCOS Cyberspace SHAPE, 2023¹¹⁵

¹¹⁴ Adapted from NATO Standardization Office, *Allied Joint Doctrine for Cyberspace Operations*, 18.

¹¹⁵ Alex Kaisler, unpublished data gathered from expert interviews with Director of NATO's Cyber Directorate, Juli 17, 2023

Due to the principles and characteristics of CO in cyberspace, it is of crucial interest for NATO to understand offensive actions in cyberspace. It is also essential for NATO to integrate a process or mechanism that enables NATO to gain knowledge of OCO to minimize the designated risks and undesirable effects in cyberspace. The SCEPVA process incorporates a framework mechanism in the Cyber Operations Centre (CyOC) of the cyber directorate in the ACO that enables a balancing act between maintaining NATO's defensive nature on the one hand and ensuring NATO's CO capability on the other. Military legal expert Cdr Wiesław Goździewicz paraphrased this by saying: "The SCEPVA mechanism can be considered as cutting the Gordian knot of dilemmas related to the use of offensive cyber capabilities by NATO."¹¹⁶ The Military Committee Memorandum MCM-0112-2018 regulates the SOPs and the framework mechanism in the SCEPVA. NATO classifies the specific regulations and directives in MCM-0112-2018. It is sufficient for the work to understand that SCEPVA provides OCOs such as manipulate, exfiltrate, degrade, disrupt, and destroy, thus indirectly allowing NATO to participate and utilize offensive effects.

a. *Cyber Operations Centre (CyOC)*

Cyber Operations Centre (CyOC). Together with the Comprehensive Crisis Operations Management Centre (CCOMC), the CyOC forms the situation and operations center of NATO's highest military level. The tasks of the CyOC are to plan, coordinate, and optimize effects in or through cyberspace; it advises the Supreme Allied Commander Europe (SACEUR), the NATO Command Structure, and the NATO Force Structure.¹¹⁷ Another essential task is to facilitate the SCEPVA framework mechanism.¹¹⁸ The Cyber Operations Centre (CyOC) represents the operational level of NATO cyber capabilities. The CyOC coordinates and is responsible for NATO CO for the highlighted four tasks: CIS Infrastructure Operations (CIS), Electromagnetic Operations EMO, DCO, and the

¹¹⁶ Wiesław Goździewicz, "Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)," *Cyber Defense Magazine*, November 2019, <https://www.cyberdefensemagazine.com/sovereign-cyber/>.

¹¹⁷ UK Ministry of Defence, *Cyber Primer* (London: UK Ministry of Defence, 2022), <https://www.gov.uk/government/publications/cyber-primer>.

¹¹⁸ NATO, *Framework Mechanism for the Integration of Sovereign Cyber Effects*.

coordination of cyber effects (facilitating SCEPVA), as shown in Figure 8. With elements of the NCISG (see Figure 9), the CyOC represents NATO's organic capability for CO in the DCO and EMO domains.¹¹⁹

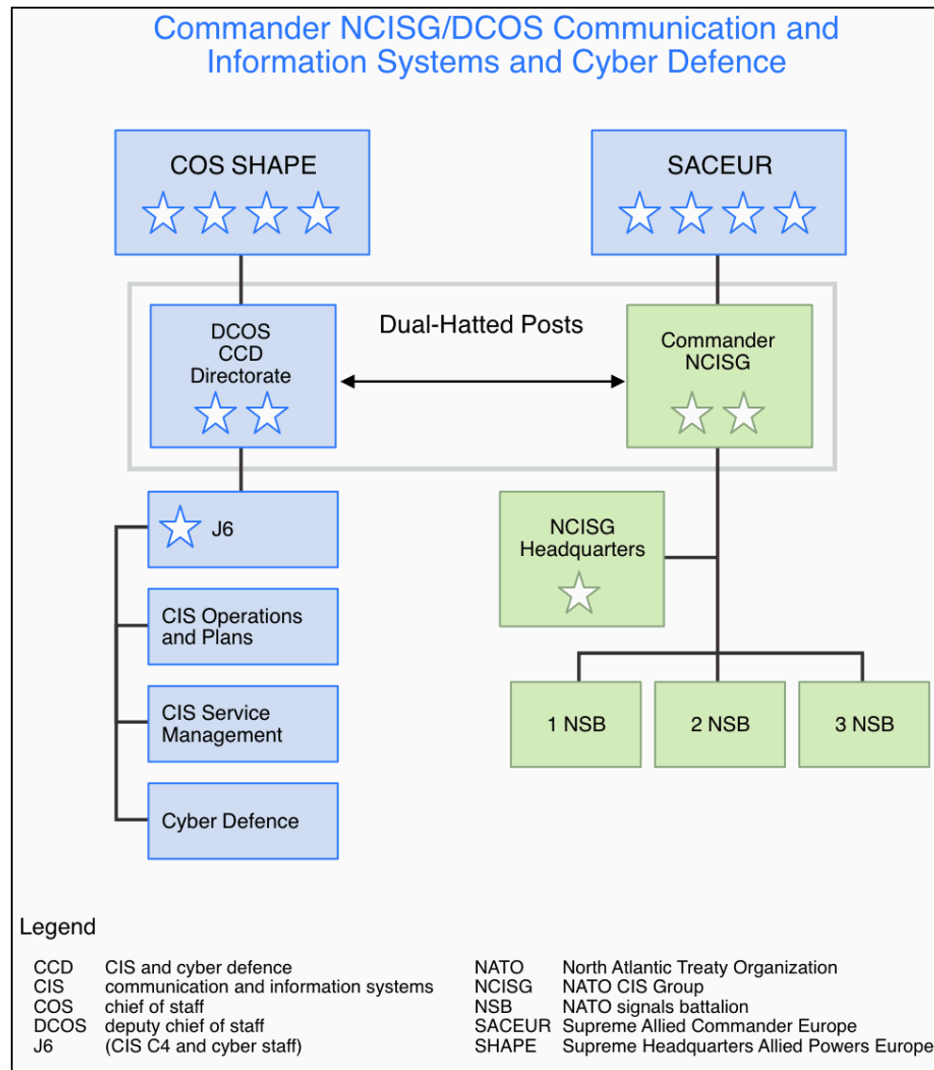


Figure 9. Commander NCISG/DCOS CIS and Cyber Defense.¹²⁰

¹¹⁹ NATO Standardization Office, *Allied Joint Doctrine for Communication and Information Systems*, 2-1 thru 2-7.

¹²⁰ Source NATO Standardization Office, 2-3.

4. Additional Cyber Organizations in or for NATO

a. NATO Communication and Information Agency (NCIA)

The NCIA is a civil-military agency that acts as a service provider for NATO with Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) capabilities. One of these services is providing and protecting NATO networks and cyber systems. The NCIA is one of the executive arms of the NATO Communications and Information Organization (NCIO). With elements of the NCISG subordinate to the cyber directorate, NCIA represents NATO's capability providers for CIS infrastructure operations (see Figure 9).¹²¹

b. Educational institutions with cyber competence for NATO Cyber Defense¹²²

There are 30 Centers of Excellence (COE), which are NATO's international military organizations providing innovation, training, and exercise expertise in many complex disciplines. The services of the COEs consist of driving doctrine and capability development, generating and identifying lessons learned, and experimentally testing concepts.¹²³ The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, covers the cyber defense field. Active contributions from another nine partner nations and the 30 NATO nations support the CCDCOE. With this support, the CCDCOE covers the services mentioned above in the cyber fields of Technology, Operations, Strategy, and Law.¹²⁴ In addition to a cyber curriculum, two major exercises, Cross Sward and Locked Shield, are offered and conducted annually at the operational strategic level. With the International Conference on Cyber Conflict (CyCon), the

¹²¹ "NATO Communications and Information Agency (NCI Agency)," NATO, April 4, 2022, https://www.nato.int/cps/en/natohq/topics_69332.htm.

¹²² NATO, "NATO Cyber Defence" (Brussels: NATO Public Diplomacy Division, April 2021), www.nato.int.

¹²³ Allied Command Transformation, "NATO-Accredited Centres of Excellence, 2023 Catalogue." Norfolk, Virginia, USA, Allied Command Transformation, 2023. https://www.act.nato.int/wp-content/uploads/2023/05/COE_CATALOG_DEC_2022_LR.pdf

¹²⁴ "About Us," Cooperative Cyber Defence Centre of Excellence, accessed February 26, 2023, <https://ccdcoe.org/about-us/>.

CCDCOE provides an annual platform where the military, civilian companies, and academia exchange views, present innovations, and set new impulses for future challenges. With the Tallinn Manual, the CCDCOE is driving the development of legal standards for cyberspace.¹²⁵

NATO has two educational institutions embedded in the NFS, the NATO School Oberammergau (NSO) and the NATO Defense College in Rome (NDC), which cover general education and training for the cyber domain. The NATO School Oberammergau offers a curriculum focusing on cyber's operational, strategic level, and defense-oriented aspects. The NATO College covers the strategic level and focuses on military-political aspects of cyber-strategic thinking.¹²⁶

In addition to the training facilities integrated into the NFS, the NCIA operates its CIS-specific school in Oeiras, Portugal, the NATO Communications and Information Academy (NCI Academy). This academy offers training according to NATO requirements for the specific area of CIS.¹²⁷

5. Potential for Further Research on Cyber

Two of the three unique characteristics: cyberspace is artificial and requires cognitive understanding. Second, this dimension's continuous adaptation and change are common to all military cyber considerations of all nations and actors. Thus, solutions and approaches already developed for NATO can be adapted for further research in this thesis. The third characteristic is that CA, across geographic boundaries in cyberspace, is subject to national responsibilities and is considered sensitive and classified within the alliance, posing a challenge to NATO as a multinational organization. This aspect challenges NATO to find NATO-specific solutions. This characteristic opens a separate field of action for NATO, for which this thesis intends to develop a NATO-specific solution.

¹²⁵ Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, UK: Cambridge University Press, 2017).

¹²⁶ "NATO Defense College Mission," NATO Defense College, January 1, 2022, <https://www.ndc.nato.int/about/organization.php?icode=23>.

¹²⁷ "NCI Agency," NATO Communications and Information Agency, accessed August 16, 2023, <https://www.ncia.nato.int/what-we-do/nci-academy.html>.

Conceptually, NATO cyber capabilities provide a broad portfolio of support services to a wide variety of NATO force's needs, including A-SOF and Space. Because NATO attributes unique characteristics to cyberspace and CA, cyber capabilities are centrally leveraged and organized. This Thesis considers the cyber organization form as a research requirement. Therefore, the studies in this thesis must find and elaborate connecting points and linking processes that practically couple the described capability portfolio of the cyber domain with the A-SOF structure on an operational and tactical level without violating requirements and constraints.

The separation of DCO and OCO in NATO is due in part to the nature of NATO's identity as a defense alliance and in part to national caveats for technologies, operational techniques, and other national interest reasons. SKEPVA integrates a framework mechanism into NATO that balances national interest with sharing offensive cyber effects internationally. Additionally, OCO play a critical role for A-SOF, and any integration/fusion is clearly in A-SOF's interest. Further research must identify and define how A-SOF integration/fusion with NATO CA and the SCEPVA process can succeed.

NATO leads and organizes cyber in a centralized manner, but in the projection of capabilities, in the development of the domain, and the education and enabling of personnel, diverse military and civil-military organizations are involved in the process and partially outsourced to these organizations. Further research must explore these organizations' role in developing a working integration of cyber with A-SOF and space.

B. SPACE IN NATO

The war in Ukraine, which started in February 2022, recalls once more the unique value and critical importance of space applications for security and defence purposes, from gathering intelligence and monitoring the situation to ensuring the availability of communication means. The recent cyberattack against a commercial satellite from the U.S. company ViaSat, which had repercussions for military actors in Ukraine, damaged the terminals of civilian customers across Europe and affected thousands of

wind turbines in Germany, also put under the spotlight the rising challenges to ensure the protection of the space infrastructure.

—ESPI Briefs, 2022, The War in Ukraine and the European Space Sector¹²⁸

Allies declared space a military domain in NATO in 2019, officially stated in the London Declaration.¹²⁹ The Space Domain is complexly organized and integrates not only military components but is based mainly on voluntary contributions from NATO-empowered nations and depends heavily on civil-commercial contributions, innovation, and cooperation. First, the section will address NATO's general considerations for the Space Domain, the threat environment, and the coherent importance of Space to NATO. Second, the section elaborates on the principles of Space assets (capabilities, products, and services) and how NATO operationalizes them. Third, the paper introduces the newly established NATO Space Centre of Excellence (SpCOE) and contextualizes its competencies. The section concludes by evaluating the existing structures of the NATO Space Domain. It determines along the hypotheses which further research steps the thesis must take to develop appropriate answers for the research question of the theory. The goal is to identify the dependencies and similarities between the Space domain, A-SOF, and the Cyber domain, as well as the gaps in the Space domain that the Section can address through integration/fusion with Cyber and A-SOF.

1. How NATO Considers the Space Domain

Today, ministers took important decisions for NATO's continuing adaptation. We have agreed that space should be a new operational domain for NATO – alongside air, land, sea and cyber. Space is part of our daily life here on Earth. It can be used for peaceful purposes. But it can also be used aggressively. Satellites can be jammed, hacked or weaponized. Anti-

¹²⁸ European Space Policy Institute, "The War in Ukraine and the European Space Sector," ESPI Briefs No. 57 (Vienna, Austria: European Space Policy Institute, May 2022), 1.

¹²⁹ "London Declaration Issued by NATO Heads of State and Government (2019)," NATO Official Texts, July 1, 2022, https://www.nato.int/cps/en/natohq/official_texts_171584.htm.

satellite weapons could cripple communications and other services our societies rely on, such as air travel, weather forecast or banking.

—Jens Stoltenberg, 2019¹³⁰

As of November 2019, NATO countries have recognized space as an operational domain.¹³¹ The Space domain is evaluated in NATO as very complex because, as in the cyber environment, there is a dual-use, both civil/commercial and military and sometimes even a mixed type, for space assets.¹³² Space is a physical dimension that redefines the factors of time, distance, and geographic boundaries. In a particular way, Space capabilities affect time and distances and thus significantly affect operational combat factors such as maneuver elements on the battlespace (JAO) by time. Using the Space domain across geographic boundaries creates additional legal challenges, primarily affecting democratic states projecting their interests.

Nevertheless, since the 2021 Brussels Summit, NATO has determined that attacks in or through space can categorize such a case as a North Atlantic Treaty Article 5 case. NATO covers the strategic concept of Space Support through AJP-3.3 Allied Joint Doctrine for Air and Space Operations. It derives its structure from political guidance through the final decision MC 0670 Policy on Space Support in NATO Operations.¹³³

a. Space-related threat environment

NATO directs the organization of space capabilities mainly against threats and for support. It maintains NATO's freedom of movement regarding the unrestricted use of assets and services in Space that NATO critically depends on. Overall, the threat spectrum in space covers a wide range. The scope starts with low-end non-kinetic threats and extends

¹³⁰ Jens Stoltenberg, "Press Conference by NATO Secretary General Jens Stoltenberg Following the Meeting of the North Atlantic Council at the Level of Foreign Ministers," NATO Press Conferences, November 20, 2019, http://www.nato.int/cps/fr/natohq/opinions_171022.htm.

¹³¹ "Foreign Ministers Take Decisions to Adapt NATO, Recognize Space as an Operational Domain," NATO News, November 20, 2019, https://www.nato.int/cps/en/natohq/news_171028.htm.

¹³² "NATO's Overarching Space Policy."

¹³³ North Atlantic Military Committee, *Policy on Space Support in NATO Operations*, MC 0670 (Brussels: North Atlantic Military Committee, 2018).

to kinetic and non-kinetic high-end threat capabilities. For NATO, there may be reversible small-scale or irreversible damages with long-term effects. In space, adversaries utilize space defense systems that the adversary can deploy specifically against systems and services critically required for NATO. Furthermore, adversaries with enhanced capabilities through the space domain can project power and their interests over greater distances and in a significantly faster time.¹³⁴

b. Space as a coherent element of NATO strategic concept

For NATO, space is an inherently global environment surrounding everything transnationally across geographic boundaries. Any conflict can thus affect the use of space. Therefore, space is a coherent element of NATO's strategic concept to protect the freedom of movement of all Allies in space. According to the Outer Space Treaty, space is free for peaceful use and not subject to national sovereignty.¹³⁵ Thus, NATO protects all Allied objects, resources, and capabilities in space. NATO does not see itself as an autonomous actor in space and does not aim to develop its space capabilities. Instead, NATO promotes an exchange of knowledge and abilities through a NATO joint coordination and synchronization platform and organizes itself through voluntary national contributions to secure NATO interests.

2. Space Domain Principles and Fundamentals

Minimal NATO-owned capabilities map NATO's space capacity, and national contributors deliver most assets synchronized and coordinated centrally by the NATO Space Centre (SpCen) since 2020.¹³⁶ The SpCen is an operational command and control element for the Space Domain embedded within the working, strategic NATO Allied Air Command (AIRCOM).

¹³⁴ NATO, "NATO's Overarching Space Policy."

¹³⁵ United Nations Office for Outer Space Affairs, "2222 (XXI). Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies," Committee on the Peaceful Uses of Outer Space – Meeting Schedule for 2023, June 31, 2023, <https://cyber.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html>.

¹³⁶ NATO HQ Allied Air Command, "We Coordinate NATO Space Matters."

a. *NATO Space Capabilities, Space Products, and Space Services*

NATO divides space capabilities into a total of seven functional areas: Satellite Communication (SATCOM), Positioning, Navigation, and Timing (PNT) services, including Blue Force Tracking (BFT), terrestrial and space environmental monitoring Space Situational Awareness (SSA) and Geological Meteorological Oceanographic (GeoMetoc), Space Security (SSEC), ISR, NATO Shared Early Warning (SEW).¹³⁷ In addition to space capabilities, NATO defines space products, which result from a data analysis process of a sensor located in space, such as maps and images produced by GeoMetoc. Finally, NATO distinguishes the so-called space services, which ensure a continuous data stream, such as SatCom and PNT, from space to a terminal device.¹³⁸

b. *NATO Space Support to Allied Operations*

As mentioned, NATO has limited space capabilities in the form of SATCOM capabilities and SATCOM units. Over these elements, NATO has the Operational Command (OPCOM).¹³⁹ The NCISG units operate with these capabilities, and the NCIA is responsible for their management (see A.4). In addition, NATO provides a platform through which NATO itself can request and coordinate its requirements and requests and thus provide security for the Allies in the Space theater. The intention is to create a collaborative space where nations, military organizations, and civilian-commercial entities can provide space support.

In the space domain, NATO considers three mission areas that create a support effect for NATO operations. First, SSA products and services, based on surveillance, tracking, and identification of space objects, enable decision-making, planning, and execution of operations at all levels. In addition, SSA products and services set the preconditions for space control missions. Second, SFE products and services maximize the

¹³⁷ Kaisler Alex, unpublished data gathered from Expert interviews with ACT, August 16, 2023

¹³⁸ NATO Standardization Office, *Allied Joint Doctrine for Air and Space Operations*, AJP 3.3 (Brussels: NATO Standardization Office, 2016), 2.

¹³⁹ NATO Standardization Office, *Allied Joint Doctrine for the Conduct of Operations*, NATO Standard AJP-3 (Brussels: NATO Standardization Office, 2019), 39.

effectiveness of operating units in all five domains. ISR, SEW, GeoMetoc, SATCOM, and PNT are all critical enablers for NATO Forces and NATO Operations. Finally, the Space Control Mission Area (SpCMA) addresses operational security in space for NATO through offensive space control (OSC) and defensive space control (DSC).¹⁴⁰

c. NATO Space Support Coordination (SpSC)

NATO has integrated the SpSC cycle/mechanism into its structure to organize the control of space capabilities and the request processes for space products and services at the strategic and operational levels of the military demand agencies and the national and civil-commercial counterparts (see Figure 10). To ensure targeted space support, NATO must consider complex factors, such as preparation, establishing coordination relationships, space dependency and operational risk, access and coverage, and persistence at the right time and in the right way.

¹⁴⁰ NATO Standardization Office, *Allied Joint Doctrine for Air and Space Operations*, 4–7.

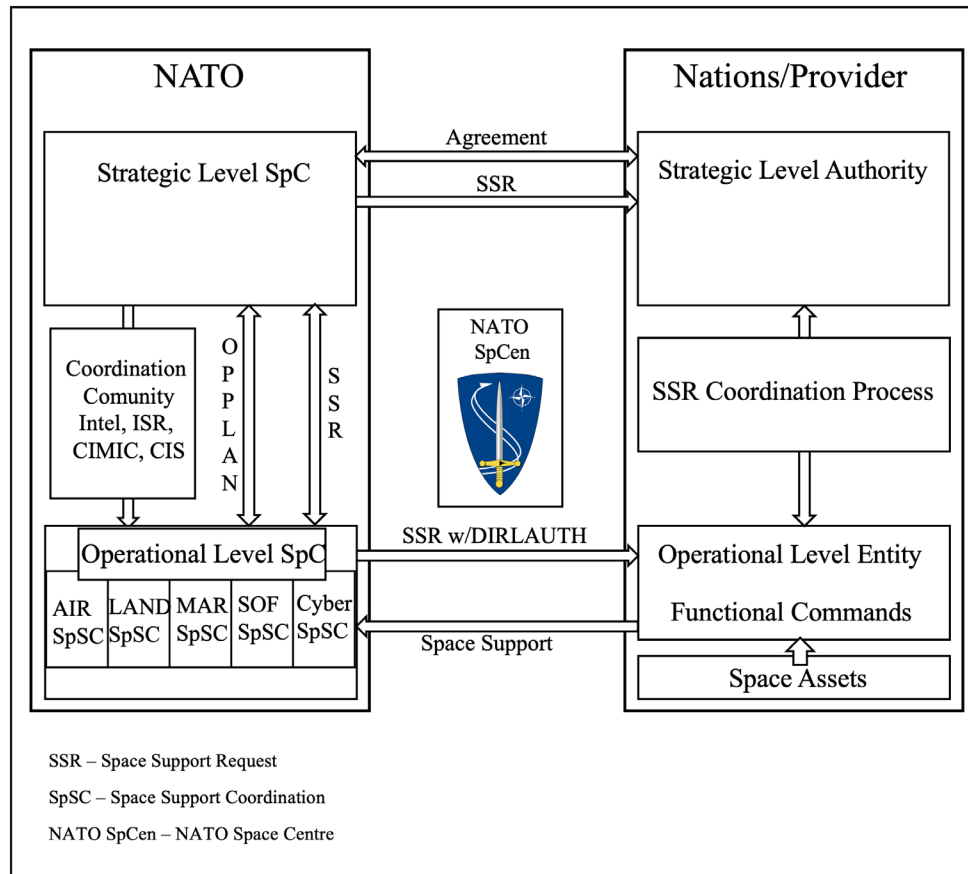


Figure 10. Conception and Organization of Space Support between NATO and Contribution Nations.¹⁴¹

3. NATO Space Centre of Excellence, a Thinktank for Space Development

The SpCOE is the thirtieth and currently the youngest NATO international military organization in the COE NATO environment. The SpCOE is the think tank for space affairs for NATO and the participating partner nations. The Center's areas of expertise are Strategy and Technology, Concept Development and Experimentation, Doctrine and Standardization, Education and Training, and Analysis and Lessons Learned (see Figure 11).

¹⁴¹ Adapted from NATO Standardization Office, 12.

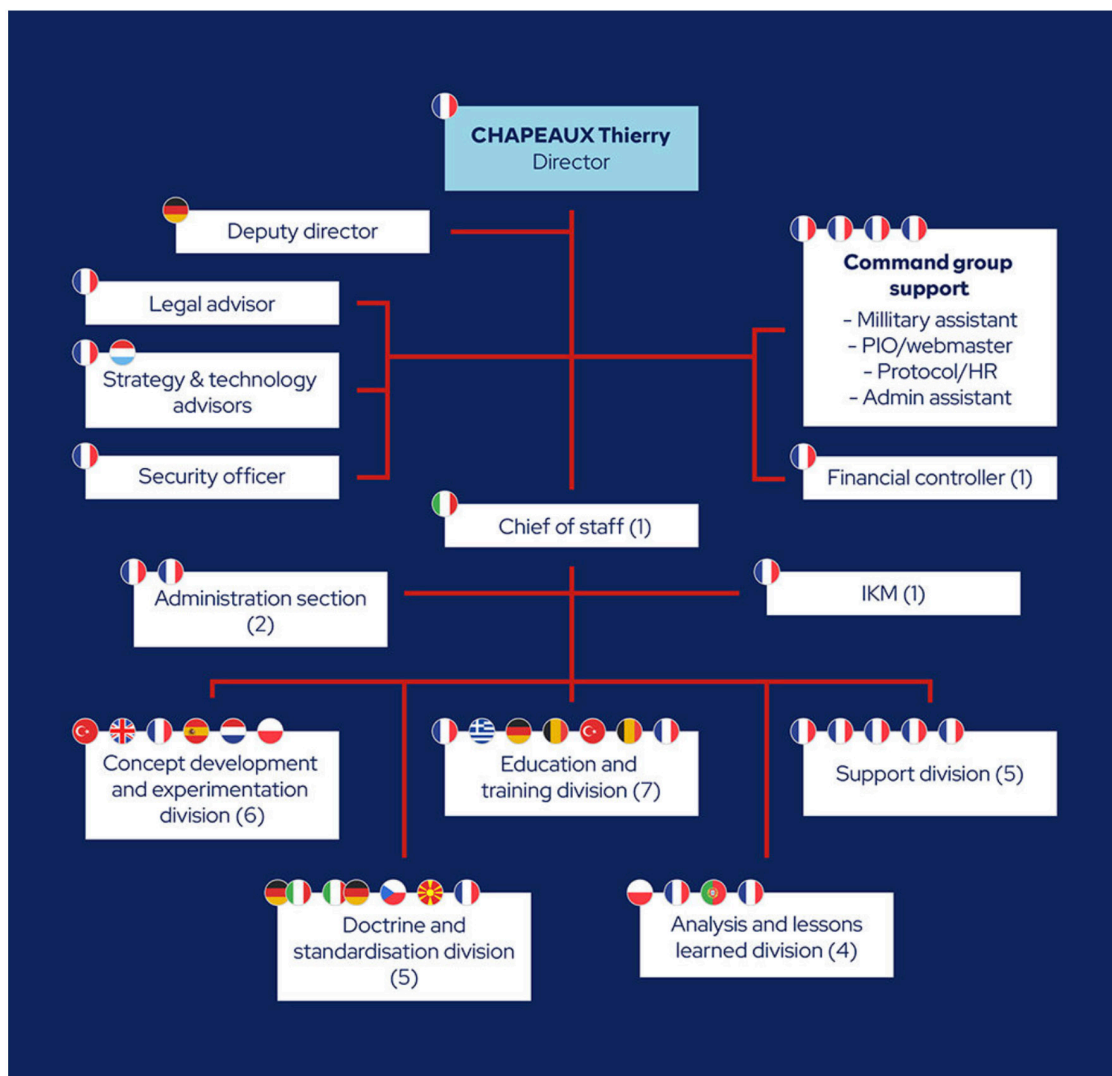


Figure 11. Organizational chart of NATO Space Centre of Excellence.¹⁴²

Through critical thinking and engagement with relevant and affected communities, it aims to capture space-related developments and help NATO enhance its space capabilities, thereby improving its posture toward adversaries. Furthermore, the SpCOE supports NATO in enhancing and optimizing its military structures and NATO forces in the 360-degree approach.¹⁴³

¹⁴² Source: “NATO Space Center of Excellence Home,” NATO Space Center of Excellence, accessed August 29, 2023, <https://www.space-coe.org>.

¹⁴³ “NATO Space Center of Excellence Organisation,” NATO Space Centre of Excellence, accessed August 31, 2023, <https://www.space-coe.org/organisation>.

4. Space Framework Mechanism and the Role of the Private Sector

Space Partnerships: Leveraging capabilities of allies and partners provides greater strength, resilience, and flexibility to space operations and complicates our adversary's decision making.

Joint Publication 3-14, Space Operations, 2020¹⁴⁴

Since NATO has limited resources for its capabilities in the space domain, voluntary contributions from allied nations play a central role in NATO's space capability structure. Thus, in addition to the U.S. as the primary contributor to NATO, governments such as the UK, France, Germany, Italy, and Luxembourg also play a role in this mechanism.¹⁴⁵ With its contributions, the USA provides comprehensive coverage of many NATO requirements in space. As shown in Figure 12, the U.S., with its competencies and capabilities, enables the U.S. Space Force, through close NATO involvement, to protect its interests and those of the community within NATO.

Components such as enabling space security NATO cannot ensure only through the projection of military power it arises in space through international relationships. NATO can significantly benefit from U.S. contributions in the competency areas of Space Security, Combat Power Projection, Space Mobility and Logistics, Information Mobility, and Space Domain Awareness. On the other hand, there is a great benefit to the U.S. and contributing nations from leveraging the NATO framework mechanism, which derives from the strength of international partnerships and positively impacts the competitive and campaigning continuum.¹⁴⁶ As illustrated in Figure 12, all U.S. NATO reflects space operability competencies in NATO's space requirements and functional areas.

¹⁴⁴ Joint Chiefs of Staff, *Space Operations*, I-6.

¹⁴⁵ Johnson, "NATO in Space."

¹⁴⁶ Joint Chiefs of Staff, *Competition Continuum*, Joint Doctrine Note 1-19 (Washington, DC: Joint Chiefs of Staff, 2019), 7.

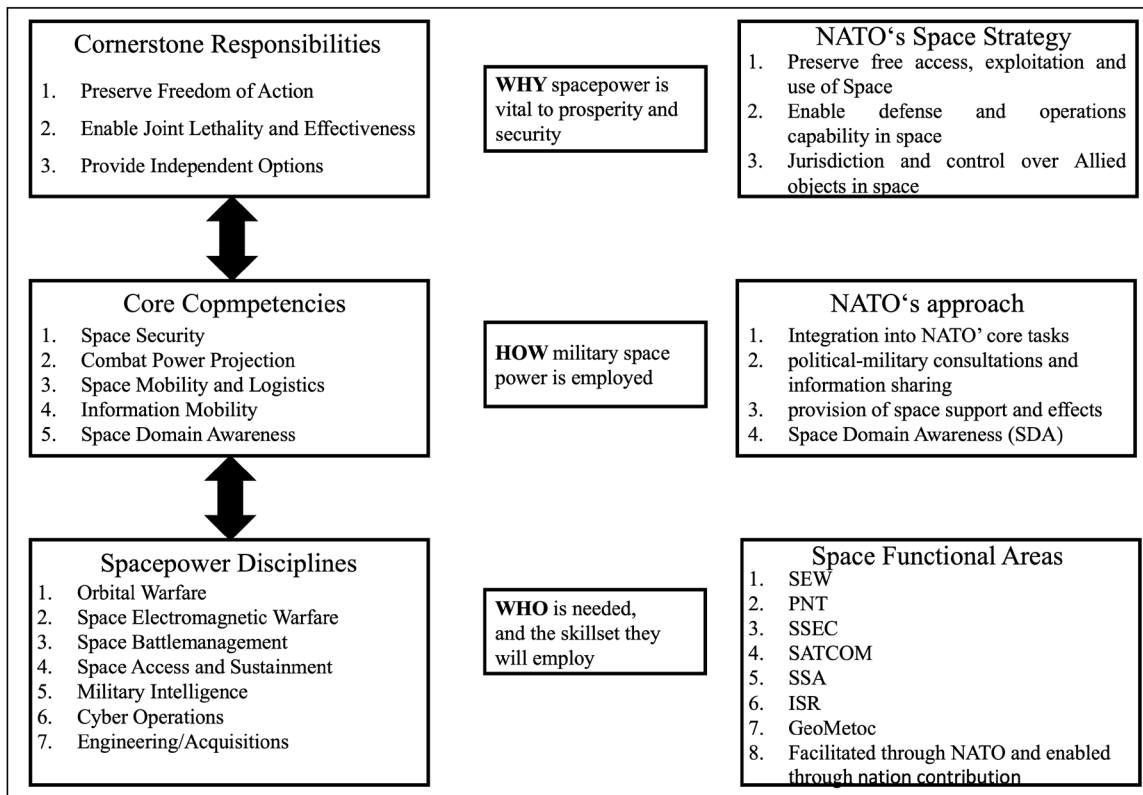


Figure 12. U.S. Spacepower Relationship.¹⁴⁷

Another component connects the space capabilities of the U.S. and NATO. In addition to U.S. Cyber, Strategic, Transportation, and SOF Commands, United States Space Command (USSPACECOM) also has a functional support role for the six other U.S. combatant commands all over the globe.¹⁴⁸ Since the commander of the ACO (SACEUR) is also the commander of the U.S. European Command (one of the 7 U.S. geographical combatant commands [CCMD]), the U.S. has an additional indirect functional responsibility to NATO territory interests, which the U.S. derives from the commitment to the U.S. European Command. For example, all U.S. Combatant Commanders (CCDRs) participate in the U.S. Space Force's Space Competency support process. Figure 13

¹⁴⁷ Adapted from U.S. Space Force, *Operations: Doctrine for Space Forces*, Space Doctrine Note (Washington, DC: Headquarters, United States Space Force, 2022), 6, <https://media.defense.gov/2022/Feb/02/2002931717/-1/-1/0/SDN%20OPERATIONS%2025%20JANUARY%202022.PDF>.

¹⁴⁸ "Combatant Commands," Department of Defense, 2023, <https://www.defense.gov/About/Combatant-Commands/>.

schematically depicts the Information Mobility sharing process as one of the core competencies of the U.S. Space Force. It illustrates the space capability requirements authority of all U.S. CCDRs and CCMDs.

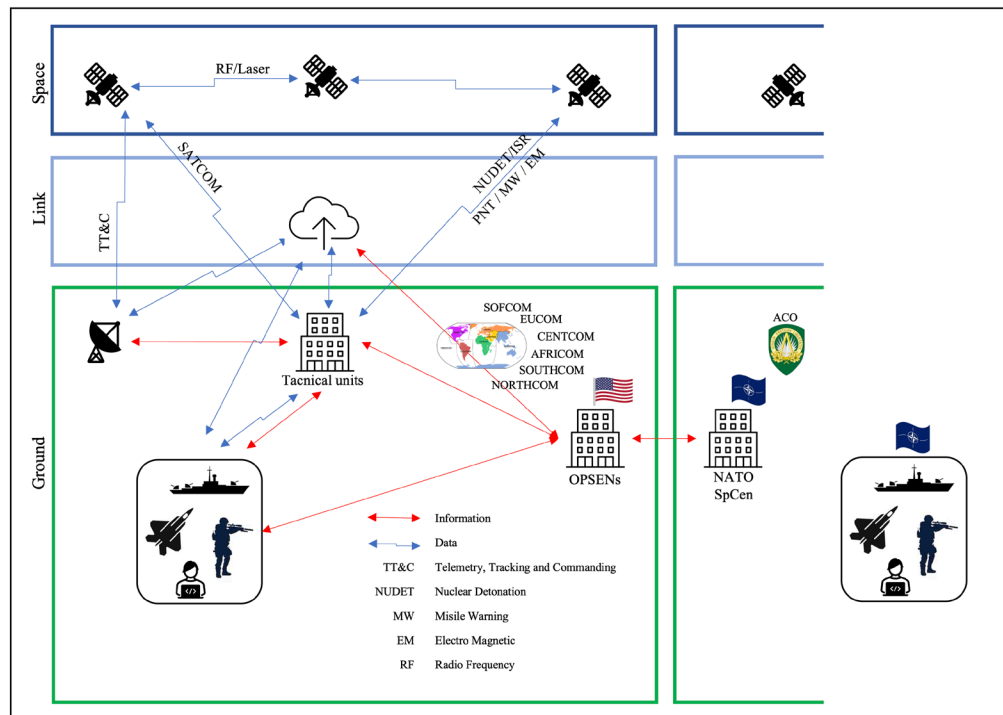


Figure 13. U.S. Space Force (USSF) Information Mobility.¹⁴⁹

A further and essential pillar for space capabilities and the projection of interests into or through space is the civil and commercial sector in space. As in the cyber sector, innovative development ties the space domain to civilian enterprises, and NATO cannot envision it without them. Operational activities in today's conflict scenarios cannot exist without civilian service providers. In the Ukraine conflict, there was a critical civilian space component and extensive support from civilian cyber products (see Table X). SpaceX's Starlink low-orbit satellites and small mobile ground stations established and maintained sustained satellite communications between the Ukrainian leadership and the Allies. Starlink provided highly encrypted and cyber-attack-resistant military and civilian satellite

¹⁴⁹ Adapted from U.S. Space Force, *Operations*, 19.

communications. Such a model will be a significant player in the NATO space capability.¹⁵⁰ Many cyber service providers utilize satellite communications as the basis of their products. The service representations for Ukraine in Table 2 underline the integrative approach of space, cyber, and civil service providers.

Table 2. Cyber and Space Sector Contributions during the Ukraine War¹⁵¹

Enterprise	Category	Product
Amazon	hardware, software, cyber services	Snowball devices, AWS cloud, software, educational devices to help children learn
Atlas VPN	software	VPN subscription
Avast	software	antivirus license
Bitdefender	cyber services	technical consulting, threat intelligence, cybersecurity technology
Nokia	hardware, software	software, telecommunications infrastructure
Outpost24	software, cyber services	vulnerability scans, threat intelligence
Recorded Future	software, cyber services	cyber threat intelligence, critical infrastructure protection
Sentinel One	software	endpoint protection
Sophos	software	endpoint protection, network security
Starlink	SATCOM	satellite communication
Vectra AI	software	monitoring tools, incident response tools

5. Space Potential for Further Research

From the NATO perspective, space is a young domain only at the beginning of implementing political decisions set in 2019. Looking at how NATO maps space capabilities and relies more on sovereign and voluntary contributions from allied nations

¹⁵⁰ Lilly et al., “Business@War.”

¹⁵¹ Adapted from Lilly et al., 77.

and civil-commercial enterprises, one can see parallels to NATO's approach to OCO in the cyber domain (see A.3). Further research needs to determine which existing mechanisms can be helpful to in the process of a possible integration/fusion between Space, Cyber and A-SOF. In addition, the Space authority in NATO should consider the SOFCOM structure to apply functional solutions according to the blueprint concept for space.

The AJP 3.3 introduces the conceptual mechanism of SpSC, but it only captures a generic idea and defines a goal. The operational practice of other domains shows that an abstract notion or purpose necessarily requires more detailed implementation steps. The cyber domain, which also has limited capabilities and depends on voluntary national contributions, shows with the SCEPVA framework mechanism that a domain authority must take further operational steps to implement conceptual requirements (compare A.3). For this transformation, SpCen will have to play an essential and central role. SOFCOM is a highly structured operational-strategic command that, as an A-SOF requirement authority, is particularly capable in the areas of liaison training and education (compare A.1). To bring Space capabilities, products, and services as a critical force and MDO enabler for SSA, SFE, and SpCMA, it is necessary to consider what role SOFCOM needs to take. The mentioned capabilities from space to other domains are essential for A-SOF and its MDO capability development. Space delivers critical components to align A-SOF with the modern threat spectrum better. The SpSC listed in AJP 3.3 may need to be expanded and adapted. The question that the Space doctrine has to answer is, at which interface would an integration/fusion of SOFCOM and SpCen in the SpSC process be reasonable? (see Figure 10).

In isolation, with the existing structures of the space domain, NATO has an organizational platform with critical competencies to MDO and 360 Grand empowerment of NATO and its Allied forces. From an A-SOF perspective, the thesis must further elaborate on how NATO can practically and feasibly link the critical structural components in the space domain, such as SHAPE as requirement authority, the SpCen as operational command element, and the SpCOE as think tank and innovation driver, with the A-SOF structures. Without linking the critical competencies, no MDO approach can take place and weaken the overall performance capability.

IV. INTEGRATING CYBER, SPACE AND A-SOF

This chapter presents a two-part approach detailing how the thesis addresses the research question. The first section of Chapter IV outlines the structure of the interviews and explains the methodology used to collect the data. In doing so, the RQ, ***“Given that there is a politically initiated adaptation process in NATO aiming at a 360-degree approach against hybrid threat scenarios and with a requirement of a direct dependency between Cyber, Space, and MDO capabilities, how can A-SOF contribute to this process and evolve better interoperability between A-SOF, Cyber, and Space?”*** formed the guideline structuring the questions and statements.

In the second section, Chapter IV presents quantitative and qualitative analysis methods with the collected interview data and illustrates the results. The first method, starting from quantitative evaluations of SMEs, utilizes distributional analysis and applies histograms for illustrative purposes, thus clearly validating and/or falsifying hypotheses H1 – H4. Subsequently, the section utilizes Semantic Network Analysis to establish key qualitative topics. In this way, the section aims to support further hypotheses H1 – H2 (see I.D.3) or additionally confirm the falsification and thus strengthen the opening argument, ***“A-SOF enhances capabilities and interoperability to cyber and space with established structures in NFS and NCS, thus supporting the 360-degree MDO approach capability, contributing to NATO’s strategic goals.”*** Additionally, the intention is to derive evaluation criteria from the analyses and apply to the assessment section for the final analysis evaluation.

A. INTERVIEWS AND DATA COLLECTION

The thesis carries out the data collection with the help of interviews with SME. This section aimed to capture broad expert knowledge and quantify qualitative assessments based on knowledge and years of experience. 26 interviews were conducted with NATO leadership, decision-makers, and SMEs in strategic-operational layers and provided with perspectives from civil-commercial sectors and academia (see Figure 14). The main volume of research data came from NATO SOFCOM, which provides the basis and

starting point for the analysis (see Figure 14). Additional interview data sets from the Cyber Directorate SHAPE, the NATO ACT Strategy and Policy for Space and Cyber, the CCDCOE Training, Strategy and Development, wargaming contractors and consultants, and representatives of the Science Sectors for Cyber, Space, and A-SOF completed a holistic survey.

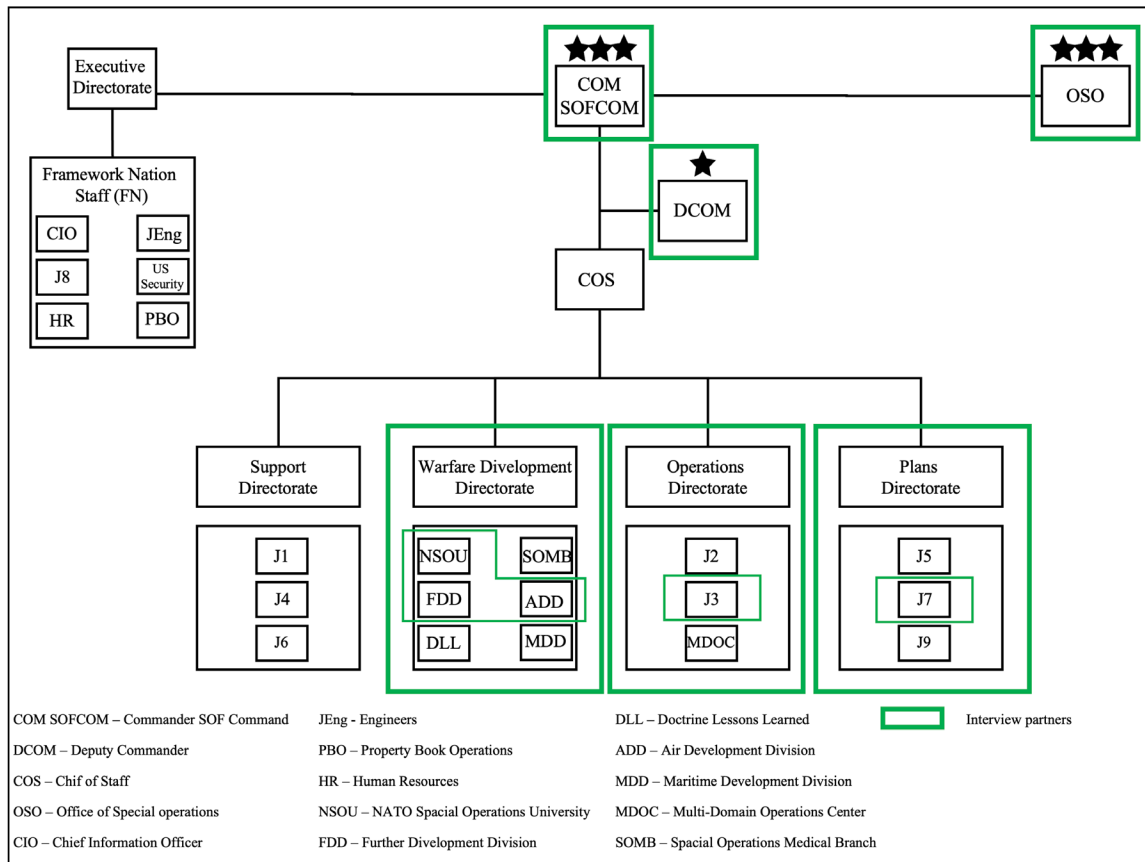


Figure 14. The Distribution of Interview Partners at the SOFCOM

1. Interview Principles and the Setup for Data Collection

The interview setup focused on three parts. Firstly, the interview covered an intuitive rather fundamental range by utilizing a closed-ended approach and harvesting binary responses and quantified hypotheses assessments. Then in the second part, it used a specific range of questions derived from the assumption and the argument, with the goal to harvest qualified responses and a range of quantified evaluations. Finally, the third section

of the interview utilizes two current OCO scenarios to assess cyber, space, and A-SOF interoperability from different SME perspectives and harvest binary responses, qualitative assessments, and quantified evaluations.

a. The first part, a closed-ended interview

The first part of the interviews focused on hypotheses H1 – H4. I instructed the interviewees to respond to closed-ended questions concerning the hypotheses statements by providing binary answers (yes or no), explaining their responses, and evaluating another question related to the hypotheses using semantic differential ranking.¹⁵² Table 3 depicts the approach and provides a qualitative clarification of how the thesis conducted the first part of the data collection through interviews with subject matter experts (SMEs).

¹⁵² David R. Heise, *The Semantic Differential and Attitude Research* (Chicago: Institute of General Medical Sciences of NIH, 1970).

Table 3. Qualitative Illustration of the Interview Part I: Closed-Ended Approach

Interview partner	Statements 1			Statement 2			Statement 3		
	H1: A-SOF lacks substantial knowledge about cyber and space to develop sustainable interoperability. H2: SOFCOM's organic training facility, NSOU, is of substantial importance in developing substantial knowledge for interoperability of A-SOF with Cyber and Space.			H3: SOFCOM is uniquely qualified to advance interoperability with cyber and space to enhance NATO's 360-degree approach.			H4: Integrating specific liaison elements enhances Space, Cyber, and A-SOF interoperability capabilities.		
	yes/no	reasoning	ranking	yes/no	reasoning	ranking	yes/no	reasoning	ranking
	yes=1 no=0	text for semantic analysis	1=low ranking 5=high ranking	yes=1 no=0	text for semantic analysis	1=low ranking 5=high ranking	yes=1 no=0	text for semantic analysis	1=low ranking 5=high ranking
ACO/SHAPE									
1									
2									
...									
ACT									
1									
...									
COE									
1									
...									
Academia									
1									
2									
...									
Economy									
1									
2									
	*	**	***	*	**	***	*	**	***
*	Tendency to a yes or to a no								
**	Reason for the absolute tendency								
***	How important it is to address and implement the topic derived from the statement(s).								

b. The second part, a structured interview with semantic differential ranking

The second part of the interviews focused on different perspectives of the interaction between cyber, space, and A-SOF. In the content, the questions resulted from doctrinal definitions, MDO considerations, and training and education. In this context, the thesis emphasized delving into the assumptions and arguments of the thesis, aiming to

capture comprehensive perspectives from SMEs and provide robust substantiation for both. The approach type is qualitatively explained with the Table 4 to set the stage for the follow-up analysis section, the interview firstly utilized open-ended questions useful for qualitative semantic network analysis. Secondly, the interview required the interviewees to quantitatively rank the facts of the answers in a semantic differential manner.

Table 4. Qualitative Illustration of the Interview Part II, Open-Ended Approach

Interview partner	Q1		...	Qn	
	*			*	
	reasoning	ranking		reasoning	ranking
	text for semantic analysis	1=low ranking 5=high ranking		text for semantic analysis	1=low ranking 5=high ranking
ACO/SHAPE					
1					
2					
...					
12					
13					
ACT					
1					
2					
3					
COE					
1					
2					
3					
Academia					
1					
2					
...					
7					
8					
Economy					
1					
2					
	**	***	...	**	***
*	See Appendix A. List of Interview questions and statements				
**	Reason for the answer				
***	How important it is to address and implement the topic derived from the question				

c. The third part, scenario-based interview

The interview concluded a scenario-based discussion along two scenarios. The interview utilized two scenarios that focused on two perspectives. The first scenario assumes that OCO will necessitate support from A-SOF involving Special Operations (SO) and/or space operations (SpSC) based on the starting point. The second scenario assumes and starting point that opportunities for A-SOF will occur through OCO, and NATO will coordinate and execute SO, with support from OCO and SpSC. To set the stage for the follow-up analysis section, the interview first utilized open-ended questions with an assessment focus on the feasibility, appropriateness, and utility of the scenarios, useful for qualitative semantic network analysis. Secondly, the interview required the interviewees to quantitatively rank the content of the answers, along the three assessment criteria, in a semantic differential manner. Table 5 illustrates the approach.

Table 5. Qualitative Illustration of the Interview Part III: Scenarios Discussion

Interview partner	Scenario 1				Scenario 2			
	A-SOF support				A-SOF is supported			
	OCO through SCEPVA is expected and space and A-SOF can coordinate and synchranize support to enhance the effects				OCO through SCEPVA and a window of oportunity is expected, where A-SOF can execute a SO with the support of space and cyber.			
	ranking	ranking	ranking	reason	ranking	ranking	ranking	reason
	Feasibility	Appropriateness	Realisticness		Feasibility	Appropriateness	Realisticness	
	1=low ranking 5=high ranking	1=low ranking 5=high ranking	1=low ranking 5=high ranking	text for semantic analysis	1=low ranking 5=high ranking	1=low ranking 5=high ranking	1=low ranking 5=high ranking	text for semantic analysis
ACO/SHAPE								
1								
2								
...								
ACT								
1								
2								
...								
COE								
1								
2								
...								
Academia								
1								
2								
...								
Economy								
1								
2								
	*	*	*	**	*	*	*	**
*	How feasible, appropriate and realistic is the scenario							
**	Reason for the answer							

B. DATA ANALYSIS

In the data analysis section of the thesis, the thesis uses two methods to test the four hypotheses (H1, H2, H3, and H4) and enable a focused evaluation. The first method involves quantitative analysis, which uses binary rankings for closed-ended statements (binary distribution analysis [BDA]) and semantically differentiated rankings for open-ended questions (semantic differential distribution analysis [SDDA]).¹⁵³ This analysis aims to create graphical representations of the percentage distribution of both BDA and SDDA, providing an initial quantitative perspective.

The second analysis method conducted a quantitative-qualitative semantic network Analysis (SNA).¹⁵⁴ Semantic network analysis is like social network analysis, except that with it, the nodes are words, terms, or concepts, and the ties between them capture some form of co-occurrence in a text, such as an interview, saying, or tweet.¹⁵⁵ It seeks to uncover a text's underlying semantic structure so that analysts can identify “higher-level units of meaning” or topics from the patterns of ties between terms, such as how they cluster together and which ones are more central.¹⁵⁶ This SNA methodology processes the documented responses from SMEs (see Appendix B. Question-Respondent Matrix from 1–300) and then analyzes it using community detection algorithms and centrality-based metrics. The objective is to identify central elements within the semantic network (SNEs) and interpret their significance concerning the research question (RQ).

Additionally, the SNA offers an opportunity for qualitative analysis. In this part, the thesis applies and demonstrates various semantic interpretations of the SNEs alongside their quantitative data. This approach provides a second perspective, enabling further

¹⁵³ Emde, “Open-Ended Questions in Web Surveys.”

¹⁵⁴ Drieger, “Semantic Network Analysis as a Method for Visual Text Analytics.”

¹⁵⁵ Elisa Bertino and Sorin Adam Matei, eds., *Roles, Trust, and Reputation in Social Media Knowledge Markets: Theory and Methods* (Cham, Switzerland: Springer, 2015), 81–89, <https://link.springer.com/book/10.1007/978-3-319-05467-4>.

¹⁵⁶ Mark Anthony Hoffman et al., “The (Protestant) Bible, the (Printed) Sermon, and the Word(s): The Semantic Structure of the Conformist and Dissenting Bible, 1660–1780,” *Poetics* 68 (2018): 89–103, <https://doi.org/10.7916/d8-ktex-m672>.

testing of the hypotheses and the development of a stance regarding the assumptions and statements.

1. Binary Distributions Analysis and Semantic Differentiation Distributions Analysis

The following section describes the quantitative part of the analysis. In this section, the thesis applies two different methods to quantitatively analyze the expertise from up to 26 interviews. The first type of method in the section is the binary approach, where the thesis illustrates experts' positive or negative tendencies by using closed-ended statements, such as hypotheses H1 – H4. A second type of method in the following section is the semantic differential ranking of open-ended questions, where the thesis illustrates a tendency expression, with 1 = low ranking and 5 = high ranking of answers.¹⁵⁷

The thesis divides the following sections of the quantitative analysis into three parts. Part I focuses on hypotheses H1, H2, H3, and H4. Part II focuses on six open-ended questions that highlight different facets of hypotheses H1, H2, H3, and H4 (see Table 6). Finally, Part III quantifies expert opinion based on two OCO scenarios (see Appendix A)

a. Quantitative Analysis Method Part I

This section quantifies and illustrates the results of the BDA (Figure 15, Figure 17, Figure 19, Figure 21) and SDDA (Figure 16, Figure 18, Figure 20, Figure 22). This section aims to test hypotheses H1, H2, H3, and H4 with the qualitative knowledge of a group of experts consisting of A-SOF, cyber, and space. The results represent the general distribution and tendency of the experts with regard to the topic of interoperability between A-SOF, cyber and space and the argument: “A-SOF as a warfighting element provide capabilities and structures in NFS and NCS to enable interoperability between A-SOF, Space, and Cyber, thus practically advancing the 360-degree approach and MDO capability and help achieve NATO’s strategic goal, but need additional adjustments.”

Figure 15 centers on hypotheses H1 and H2. The BDA focuses firstly on determining whether there is generally a knowledge gap between A-SOF, Cyber, and Space

¹⁵⁷ Emde, “Open-Ended Questions in Web Surveys,” chap. 5.

that makes practical implementation of interoperability difficult. The Thesis finds that the experts, with 96% ‘yes’, very consistently tend to confirm H1. On the other hand, the BDA finds the same result for H2. Most of the experts with 96% ‘yes’ tend to agree that SOFCOM’s organic training facility NSOU plays a substantial role in closing the mentioned knowledge gap.

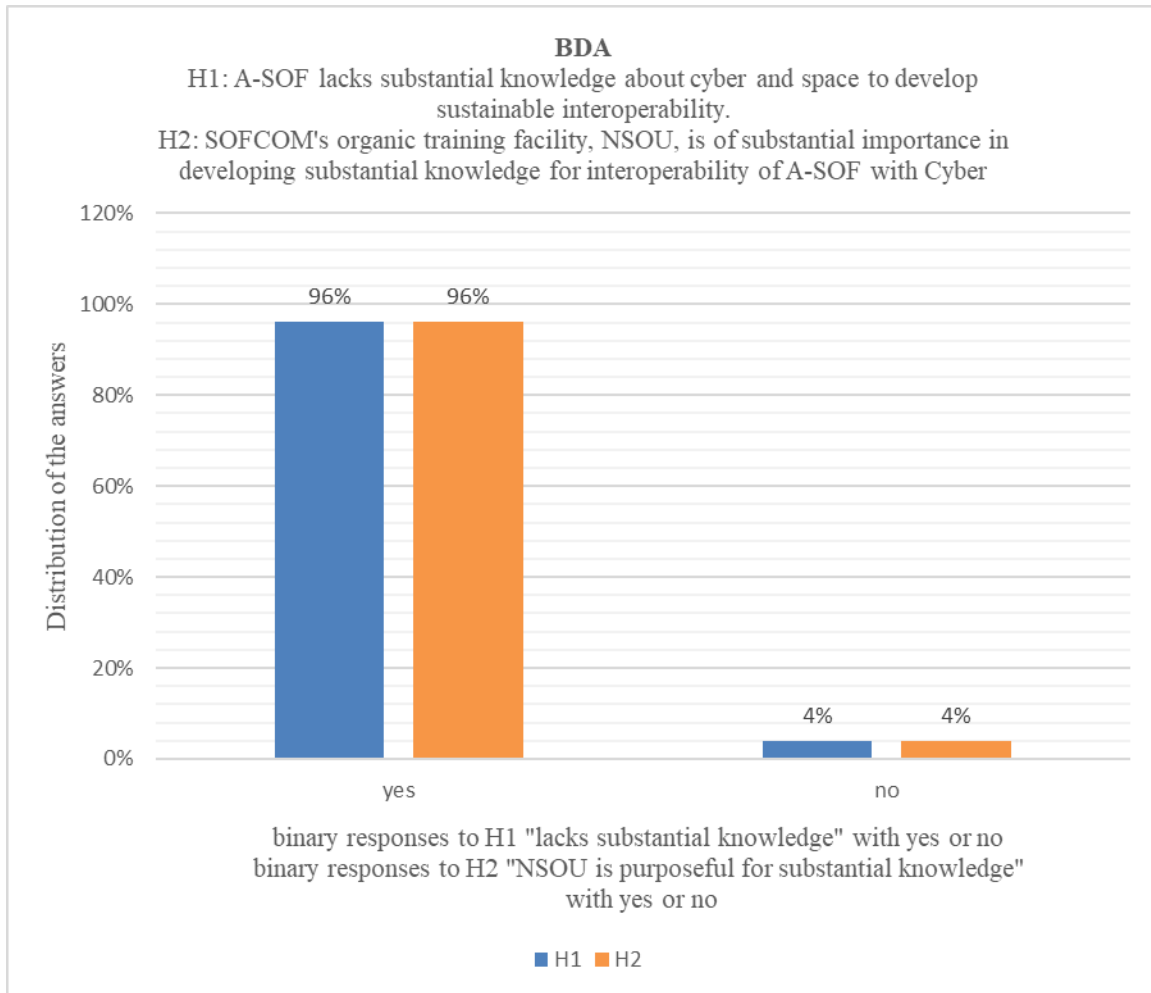


Figure 15. Substantial Knowledge and the Role of SOFCOM’s NSOU for Education

Figure 16 centers on hypotheses H1 and H2, too. This figure illustrates the results of the SDDA on H1 and H2. SDDA points out the importance of basic knowledge and the importance of organic educational institutions, such as the NSOU for SOFCOM and A-

SOF, in creating such knowledge. All the experts consider it important to acquire basic knowledge about other domains and also to utilize own training facilities such as NSOU for such knowledge transfer. A majority of 81% even consider these two aspects to be very important.

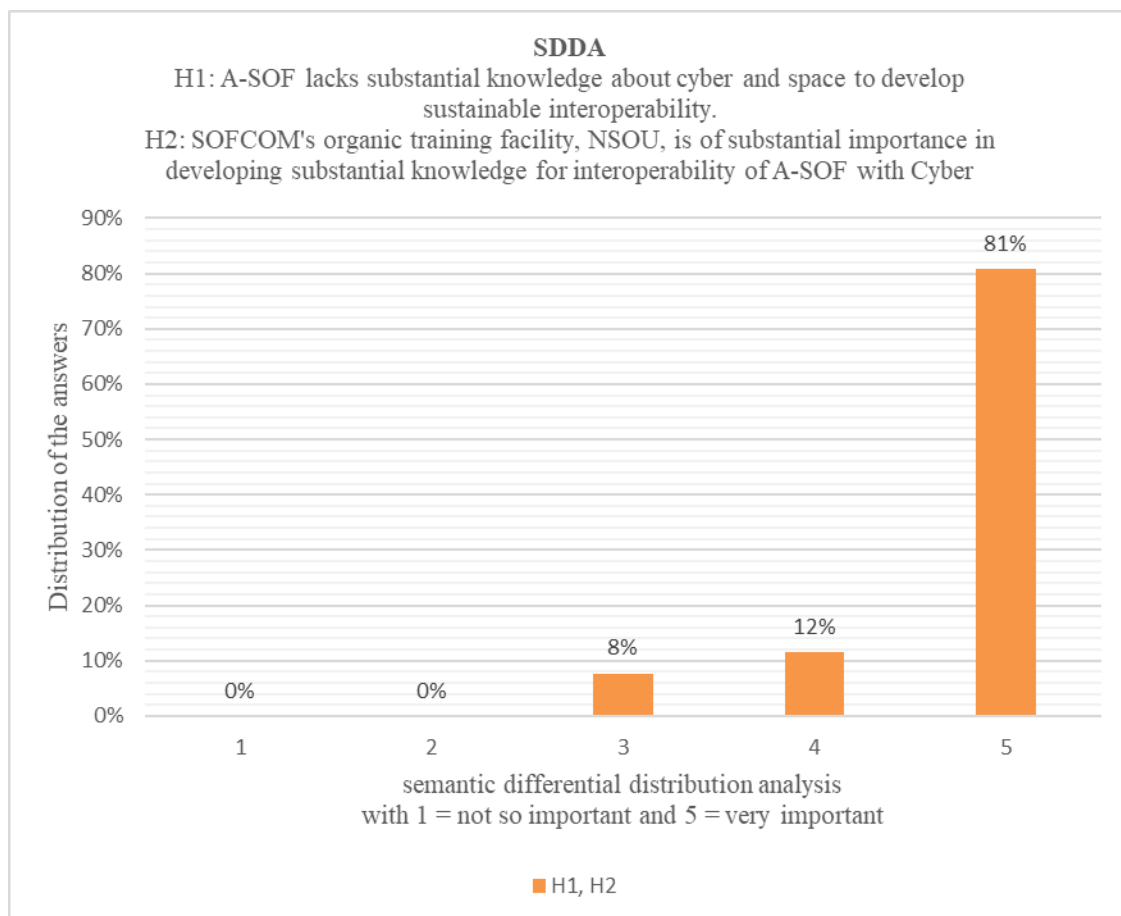


Figure 16. Importance of Basic Knowledge about each for A-SOF, Cyber, And Space.

Figure 17 centers on hypothesis H3. The BDA focuses on determining whether SOFCOM is uniquely qualified to advance interoperability with cyber and space to enhance NATO's 360-degree approach. The Thesis finds that the experts, with 100% 'yes', absolutely confirm H3. In the perspective of all interviewees, SOFCOM, with its structures

established and capabilities mapped, plays an essential and supporting role in pursuing NATO's goal of progressively achieving MDO or 360-degree approach.

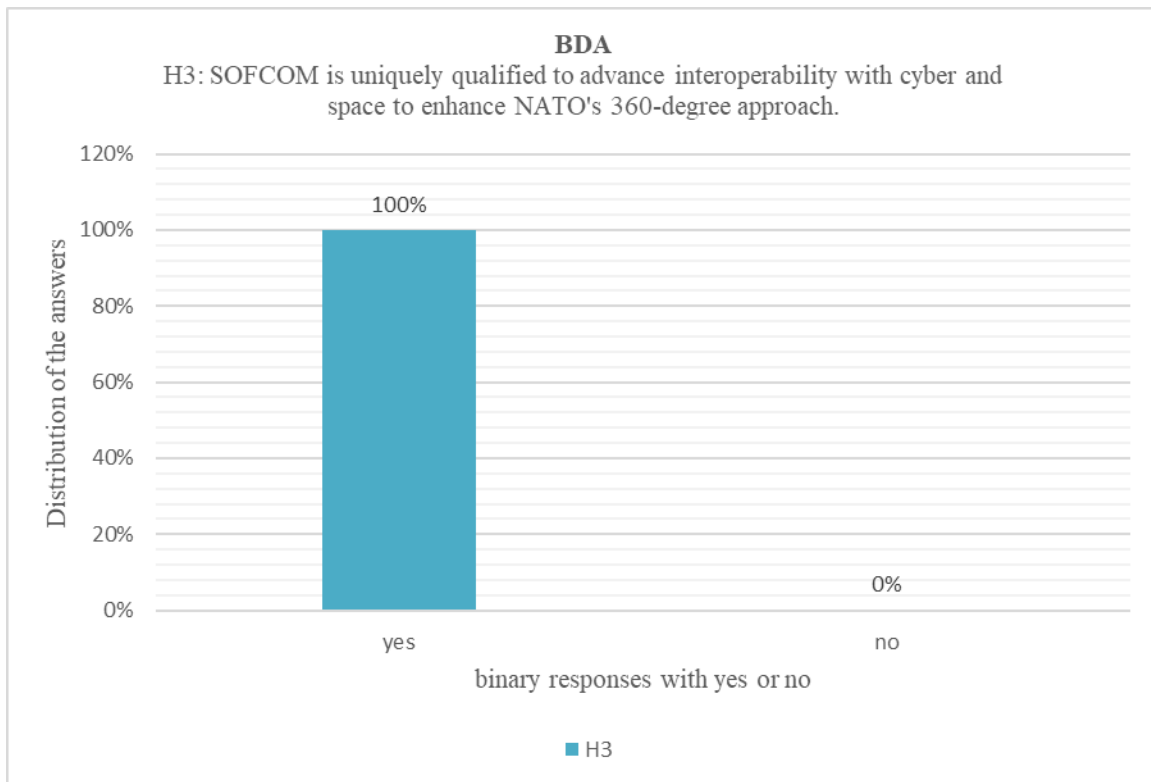


Figure 17. SOFCOM's Unique Qualification for Interoperability with Cyber, and Space

Figure 18 centers on the execution of SDDA on hypotheses H3. This figure illustrates the results of the SDDA. The section quantifies the distribution of expert evaluations on the question of, how qualified SOFCOM is to facilitate and enable the interoperability development process between A-SOF, cyber and space. The section assessed SOFCOM's MOU organizational structure, its establishment in the NCS as early as 2007, and the operational and strategic interfaces SOFCOM developed with other command entities since its establishment. All the experts consider SOFCOM as qualified for such goal. A majority of 69% even consider SOFCOM as very qualified to advance the interoperability between A-SOF, cyber and space.

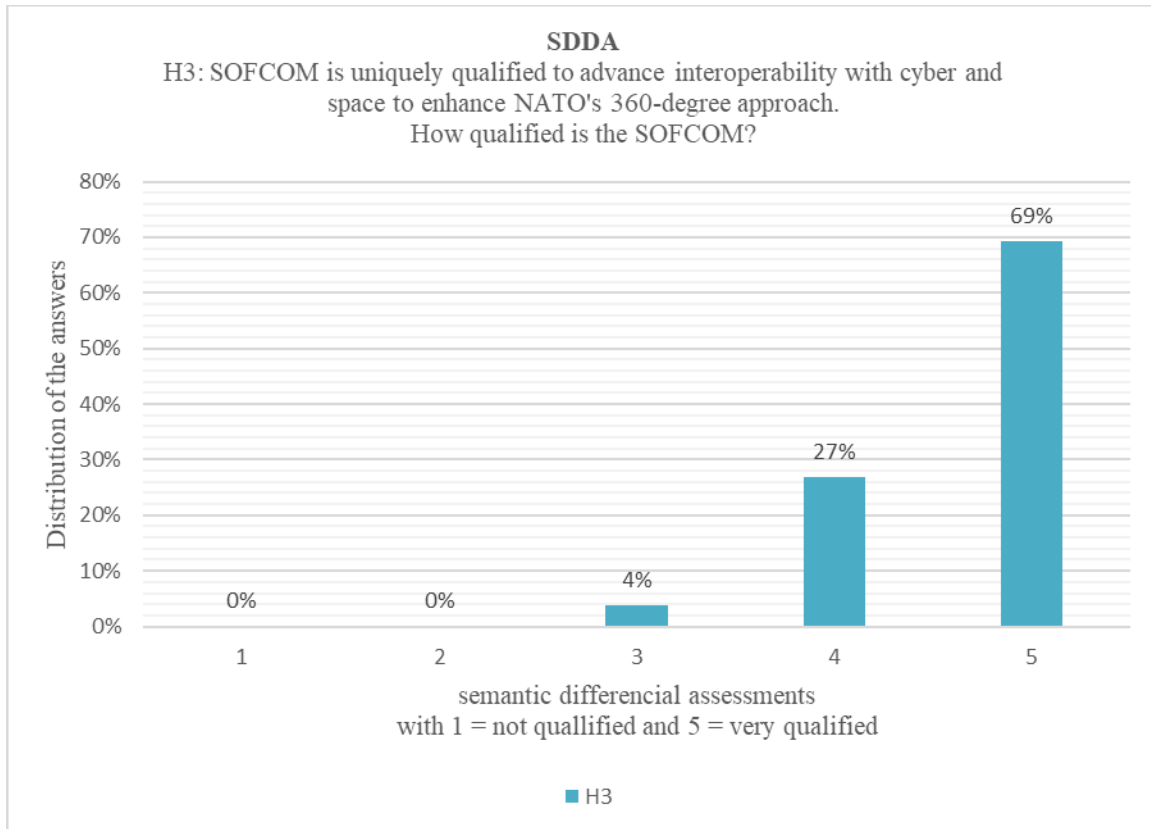


Figure 18. How qualified is SOFCOM to advance Interoperability with Cyber and Space

Figure 19 centers on hypothesis H4. The BDA focuses on statement, that integrating interoperability elements such as liaison elements, would enhance the interoperability development process between the operational layers of A-SOF with SOFCOM, cyber with CyOC, and space with SpCen. Figure 19 depicts the results, where 96% of respondents answered ‘yes,’ suggesting that experts perceive improvements through the sharing of liaison elements.

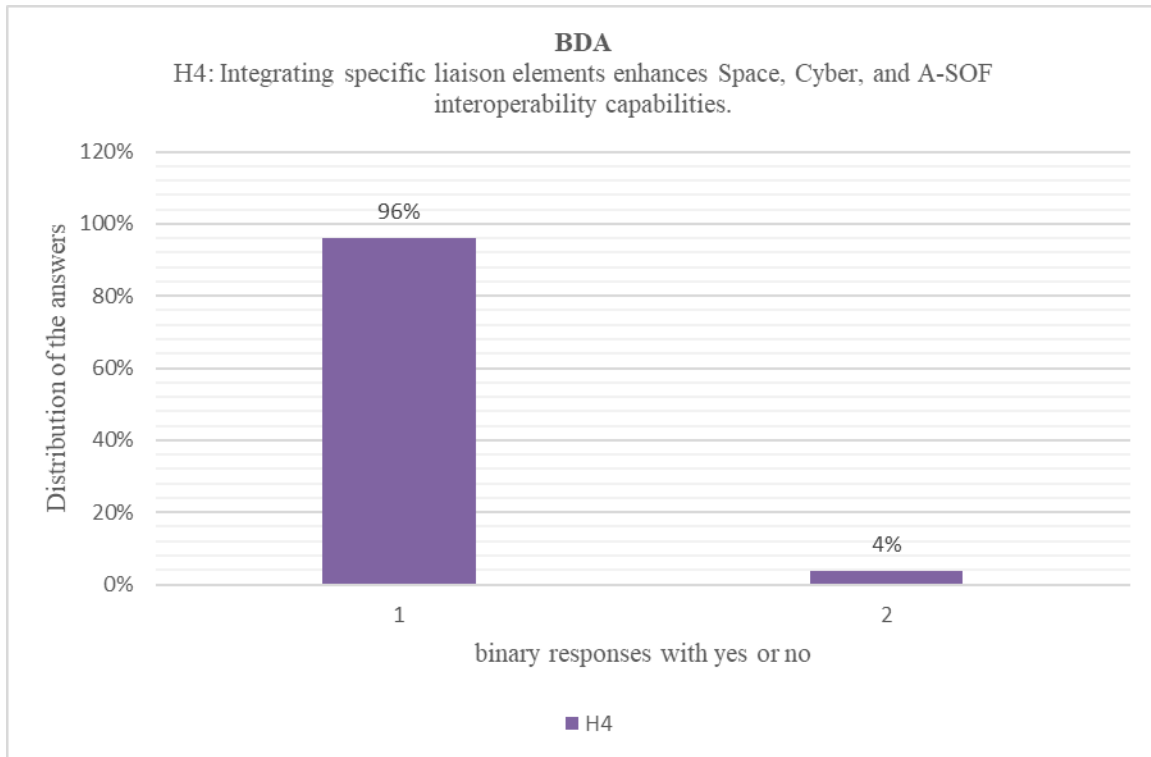


Figure 19. Integrating Specific Liaison Elements to Enhance Interoperability

Figure 20 illustrates the SDDA results on hypotheses H4 and quantifies the evaluation on the question, how big would an enhancement be by sharing and integrating liaison elements on the operational level between SOFCOM, CyOC and SpCen. The assessment focus was on SOFCOM's ability to interact with other entities by deploying liaison elements to communicate cross-domain awareness, synchronize capabilities, advise decision makers, coordinate demands and capacities and deconflict obstacles in all phases of operations. All the experts consider that approach as an enhancement for operational interoperability between A-SOF, cyber and space. A majority of 54% consider this approach a major enhancement.

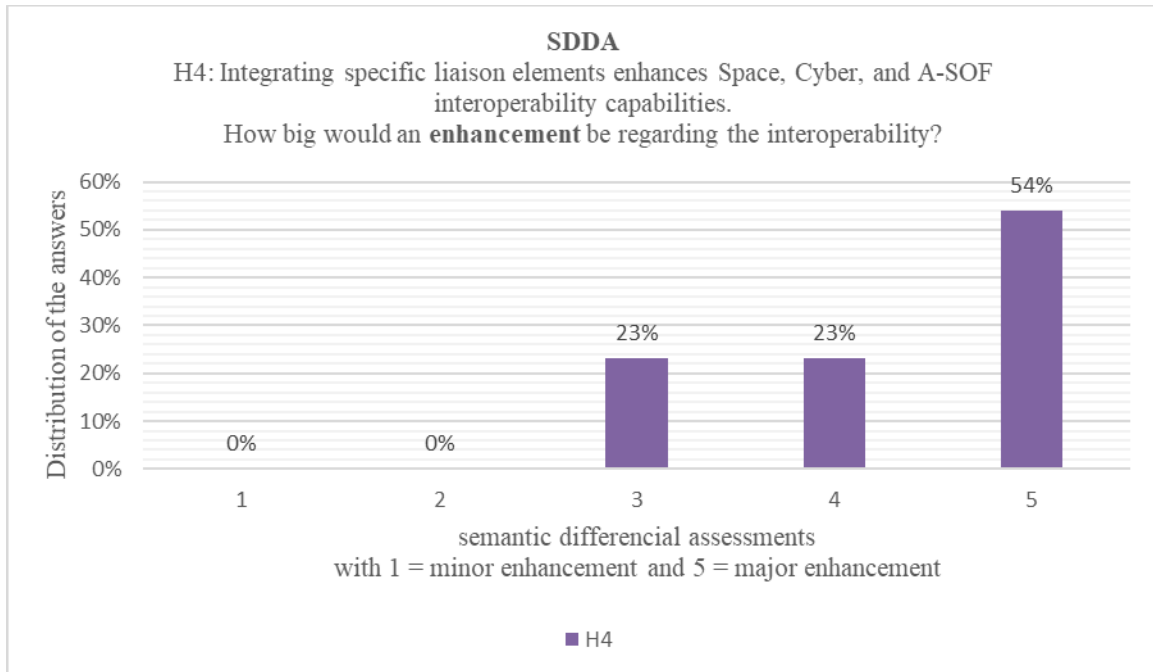


Figure 20. Liaison Elements Enhancing Interoperability between SOFCOM, Cyber, and Space

Figure 21 illustrates the comparison of the results from the BDA of all hypotheses. A large majority of the interviewees tend to a ‘yes’ and substantiate the content of the hypotheses H1, H2, H3, and H4.

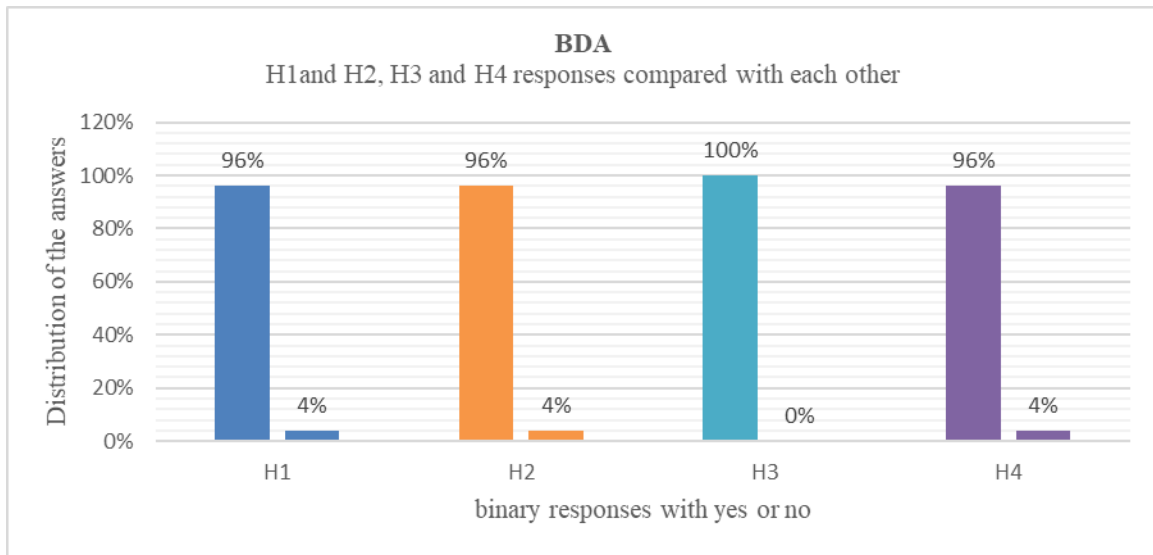


Figure 21. Binary Responses over H1, H2, H3, H4

Figure 22 illustrates the comparison of the results from the SDDA of all hypotheses. A large majority of the interviewees evaluate their responds with ‘5 = very high’, and substantiate the content of the hypotheses H1, H2, H3, and H4.

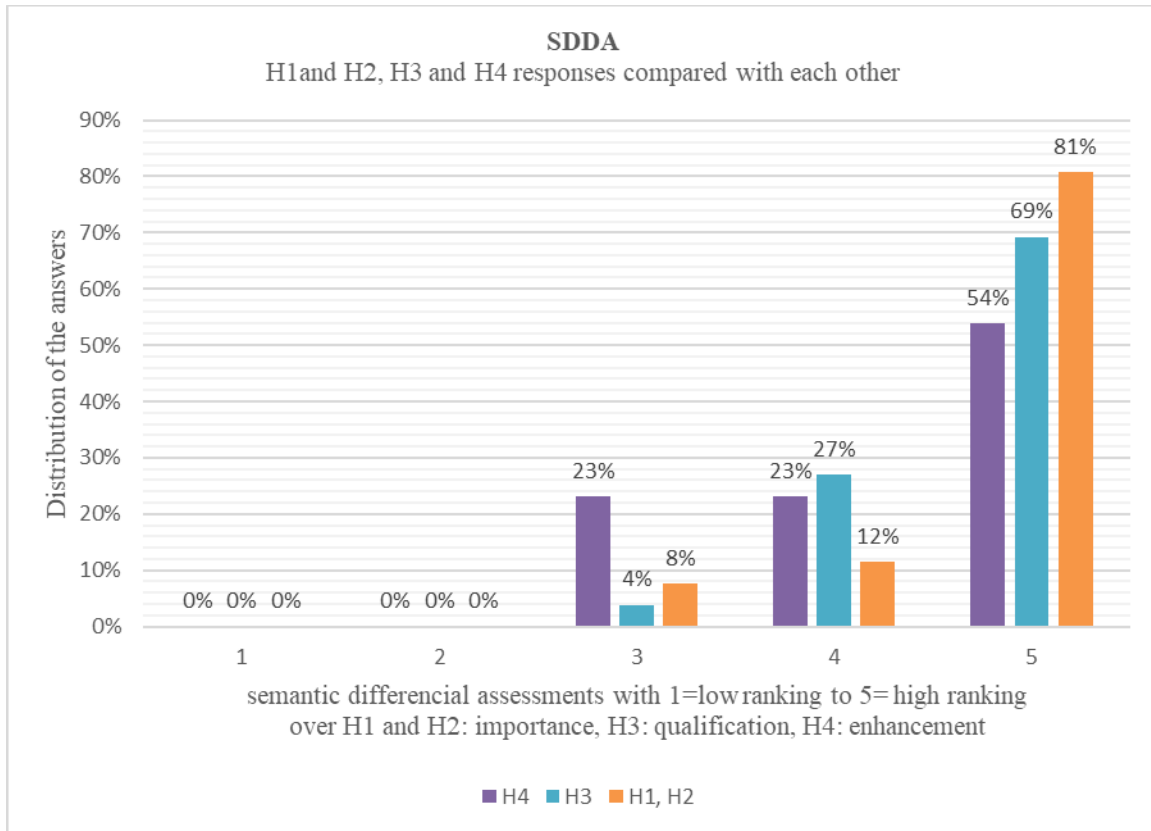


Figure 22. Semantic Differential Distribution analysis with 1 to 5 over H1, H2, H3, H4

b. Quantitative Analysis Method Interview Part II

This section quantifies and illustrates two areas. First, it illustrates the binary SME estimations (see Figure 23) considering SOFCOM as an MOU entity facing seven different challenges that typically distinguish a multinational alliance, such as NATO.¹⁵⁸ This quantification is essentially about capturing a binary tendency of SME experiences on whether an MOU organizational form can better overcome the typical seven challenges in comparison to an NFS organizational form (see Figure 23). In these results, the section notes that consistently most interviewees see advantages in the MOU form of organization to overcome challenges faster than in the NCCR. Such as that 50% of the interviewees who

¹⁵⁸ Jennifer D. P. Moroney et al., *Overcoming Barriers to Working with Highly Capable Allies and Partners in the Air, Space, and Cyber Domains* (Santa Monica, CA: RAND Corporation, 2023), https://www.rand.org/pubs/research_reports/RRA968-1.html.

see advantages more in the MOU organization to overcome bureaucratic challenges than with NFS.

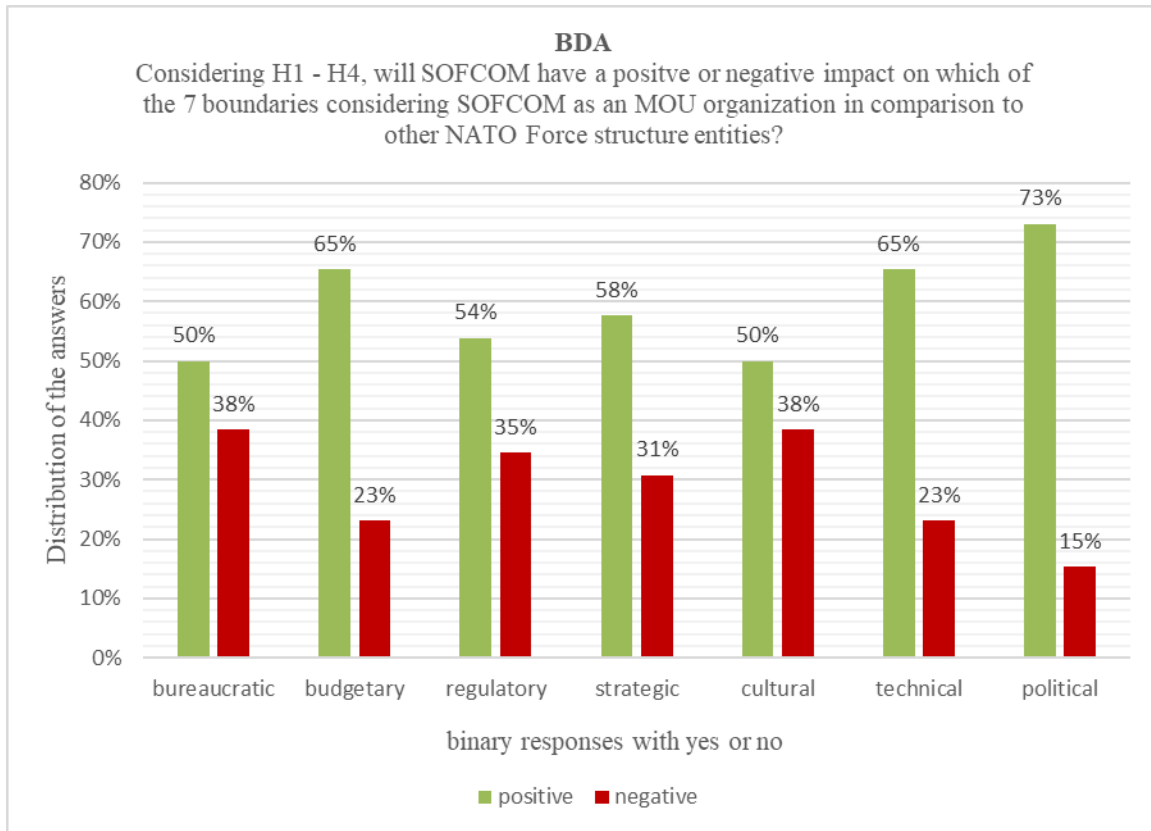


Figure 23. SOFCOM's Positive or Negative Impact on the 7 Challenges

In the second part, the section illustrates the distribution of SME assessments for a total of six open questions with an SCCA approach. Table 6 illustrates the questions and their respective relation to the hypotheses H1, H2, H3, and H4.

Table 6. Open-Ended Questions Q1 – Q6

Number	Questions	Affiliation
Q1	How relevant is the role of A-SOF as a war fighting element interacting with cyber and space regarding the 360-degree approach of NATO?	H4, H3
Q2	Considering Cyber, with its unique effect projections, how relevant is Cyber to enhance A-SOF cross-domain capabilities?	H4
Q3	Considering Space, with its unique support capabilities, how relevant is Space could a cross-domain enhancement be for SOFCOM including Space components?	H4
Q4	What is the role of SOFCOM as the main driver for integrating Cyber and Space in the A-SOF structure?	H3
Q5	How important are cyber and space capabilities in SOFCOM in enabling A-SOF to coordinate, synchronize, and establish education for knowledge sharing and awareness between the domains?	H1, H2, H4
Q6	Could NSOU take on a complementary role, first to specifically augment capability development for the Cyber, Space, and A-SOF triad, and second to achieve cooperation at the education level?	H1, H2

This section aims to use SCCA for further quantification of arguments to test hypotheses (H1-H4) and thereby substantiate the overall argument, *“A-SOF enhances capabilities and interoperability to cyber and space with established structures in NFS and NCS, thus supporting the 360-degree MDO approach capability, contributing to NATO’s strategic goals..”* Figure 24 shows the results of the analysis.

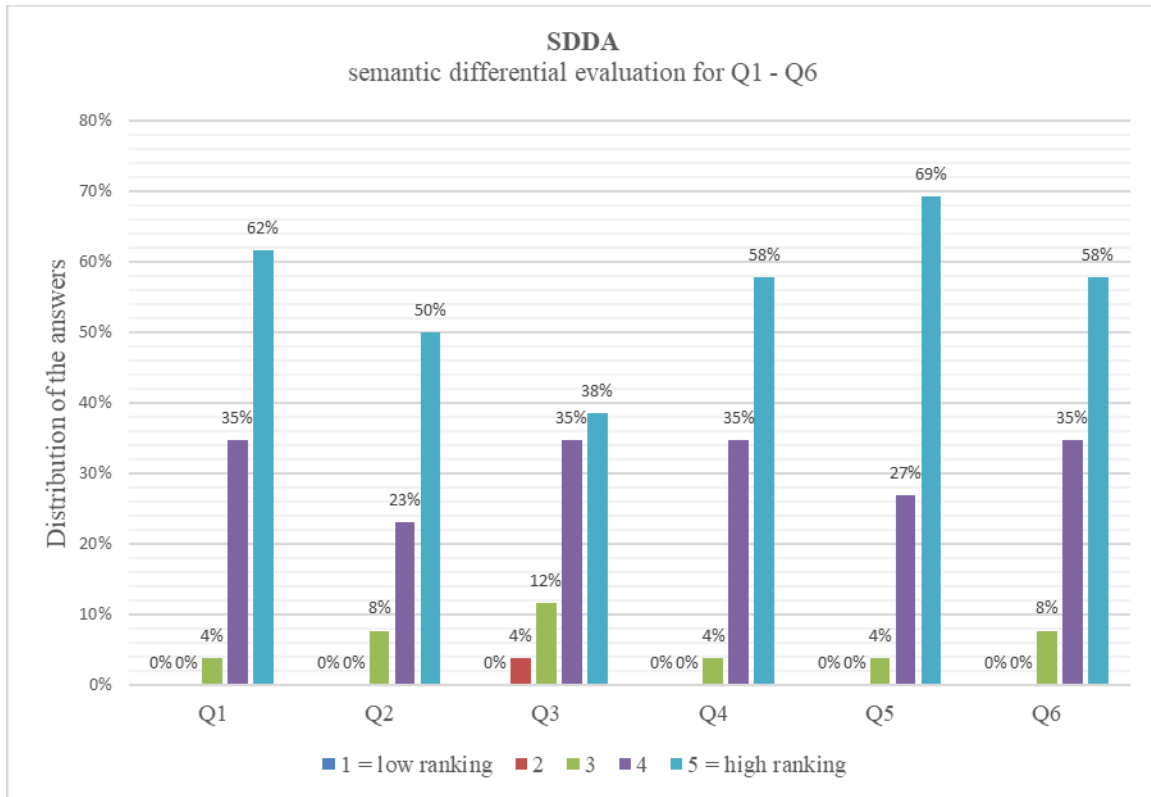


Figure 24. Distribution of the Semantic Differential Assessments with 1 to 5 to Q1–Q6

c. *Quantitative Analysis Method Interview Part III*

In the final section of the quantified analysis method, we consider two OCO scenarios generated by an FN mechanism (SCEPVA) that can be maximized either by Special Operations (SO) or by SpSC in the 360-degree approach. SOFCOM is currently investigating these scenarios as part of the ongoing development of MDOC, with the aim of integrating collaboration between SOFCOM and CyOC.¹⁵⁹ The section utilizes two OCO scenarios (see table) to semantically differentiate three different perspectives, Utility, Feasibility, and Appropriateness, and to illustrate the distributions of expertise ratings. Figure 25 illustrates the distribution of the semantic differential described above.

¹⁵⁹ Kaisler Alex, unpublished data gathered through expert interviews with CCD COE, July 1, 2023

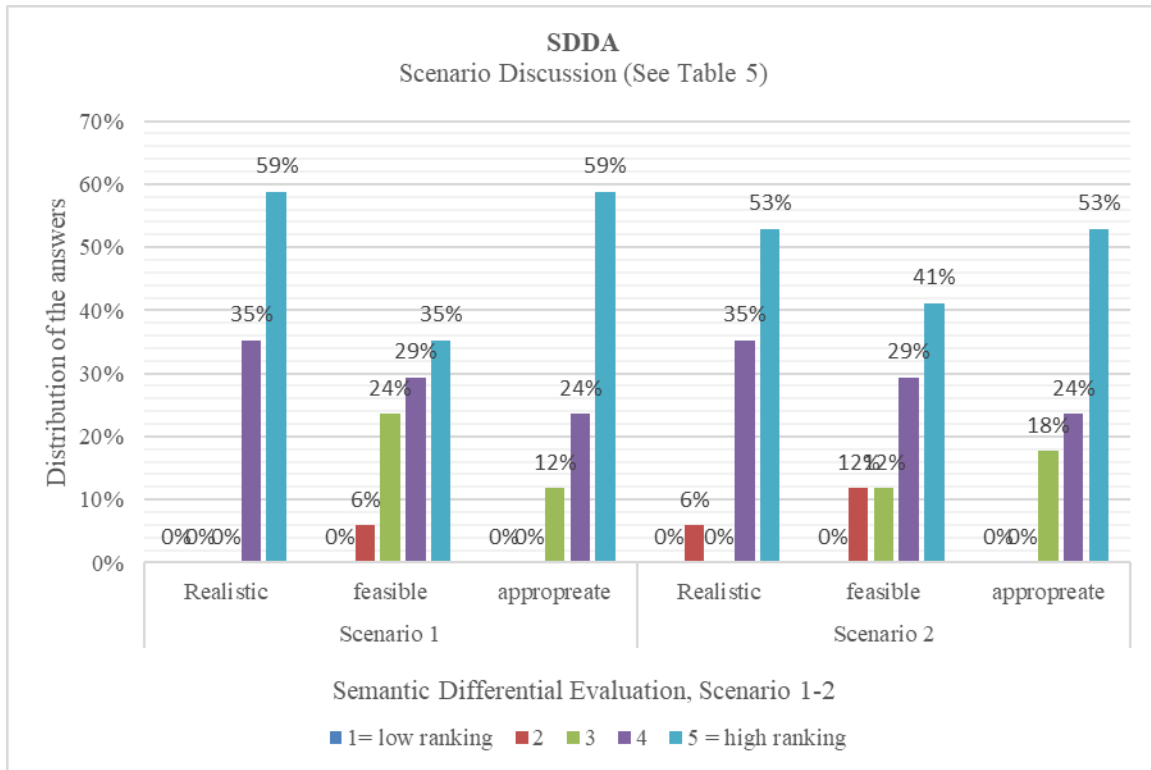


Figure 25. SME Assessments on OCO Scenarios 1–2

2. Semantic Network Analysis

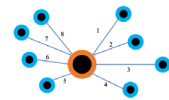
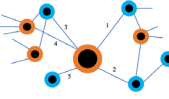
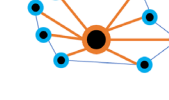
As part of the data collection (expert interviews), the thesis generated a complex SN by documenting and transcribing all SME responses as Table 4, Table 5, Table 6 emphasize.¹⁶⁰ The SN matrix thus provides the basis for the following section (see Appendix B. question-respondent matrix from 1 – 300). This section describes the second analysis part of the thesis research and includes SNA, which utilizes a quantitative-qualitative analysis approach.¹⁶¹ This section examines and illustrates, both the quantitative results, such as frequency-, distance-, and path-based centrality measures, and qualitative semantic interpretations of semantic power and centrality within the SN, as Table 7 shows.

¹⁶⁰ Alex Kaisler, “Semantic Network of Subject Matter Expertise on Allied Special Operations Forces, Cyber and Space,” excel, August 2023.

¹⁶¹ Drieger, “Semantic Network Analysis as a Method for Visual Text Analytics,” 4.

Specifically, the research presented below draws on four standard centrality measures: degree, eigenvector, closeness, and betweenness (see Table 7). With regards to SN, degree centrality identifies terms that frequently occur with other terms. It is not identical to word counts since it equals the number of ties a word has to other words. Nevertheless, the two often correlate highly with one another. Eigenvector centrality is similar to degree except that it weights each term’s score by the number of its neighbors’ ties. It identifies relatively well-connected terms tied to other well-connected terms. Words that score high in closeness do not necessarily have the most ties, but on average, they lie closer to other words in the network. Finally, betweenness centrality captures the extent to which a term lies on the shortest path between all other pairs of terms in a network. In social network analysis, we often view it as capturing a node’s brokerage potential. In this context, words with high scores in betweenness centrality are likely best understood as those contributing to holding the social network together..

Table 7. Quantitative and Qualitative Interpretation of Centrality Measures in Semantic Network Elements (SNE)¹⁶²

Methods	Quantity	Quality	Graphic
Frequency-based Measures: Degree Centrality (DC)	nodes most connected with other nodes.	Indirect influence or power; most known node, wide recognition	
Frequency-based Measures: Eigenvector Centrality	nodes most connected with other most connected nodes.	Indirect influence or power; pivotal nodes to understand the topic	
Distance-based Measures: Harmonic Closeness Centrality	nodes closest to all other nodes	Nodes with fast access to information or other nodes	
Path-based Measures: Betweenness Centrality	nodes in the best path to get to every other node	Nodes as semantic connectors, and group connectors.	

¹⁶² Adapted from: Sean F. Everton, “Social Network Analysis: Centrality & Prestige” (lecture, DA 4600: Disrupting Dark Networks, Naval Postgraduate School, Monterey, CA, September 2022.

In addition, this analysis utilizes the Spinglass community detection algorithm (SGA) to sort the semantic network into clusters of words or topic communities.¹⁶³ Spinglass is one of several community detection algorithms that sort nodes into separate communities or subclusters such that the density of ties within a community is greater than the density of ties between them. Analysts typically use modularity to determine which algorithm provides the best measure of fit or representation of community structure.¹⁶⁴ Modularity compares ties within and across communities to what one would expect in a random network of the size and having the same number of ties.¹⁶⁵ The higher the modularity score, the better the fit. Because the Spinglass algorithm provided the best fit, it is used here. Only after the preparation is complete does the thesis section apply the mentioned centrality measures to the isolated communities in order to quantitatively test the hypotheses.

a. Spinglass Communities

For analysis, the section uses first the SGA that breaks the SN down into more understandable sub-communities. As in social network analysis, this section examines the SN to determine important and central words or terms, enabling the thesis to test the hypotheses H1, H2, H3, and H4.¹⁶⁶ Using the SGA, the thesis has identified 25 subgroups or communities across the SN. The thesis then simplified the network by collapsing (shrinking) the network based on these 25 communities. When analysts collapse a network, they combine all the nodes (in this case, terms) that share a particular characteristic (in this case, membership in the same community) into a single “meta-node.” Figure 26 presents the individual steps of the collapsing process. As a result, one can recognize nodes of different sizes that describe a thematic community in the graph based on their topography

¹⁶³ Jörg Reichardt and Stefan Bornholdt, “Statistical Mechanics of Community Detection,” *Physical Review E* 74, no. 1 (July 2006): 1–14, <https://doi.org/10.1103/PhysRevE.74.016110>.

¹⁶⁴ M. E. J. Newman, “Modularity and Community Structure in Networks,” *Proceedings of the National Academy of Sciences* 103, no. 23 (2006): 77–82, <https://doi.org/10.1073/pnas.0601602103>.

¹⁶⁵ Daniel Cunningham, Sean Everton, and Philip Murphy, *Understanding Dark Networks, A Strategic Framework for the Use of Social Network Analysis* (Lanham, MD: Rowman & Littlefield, 2016), 128.

¹⁶⁶ Sean F. Everton, *Disrupting Dark Networks* (New York: Cambridge University Press, 2012).

(the more nodes and connections within the community, the larger the community node). Communities #14, #6 and #3 are the largest communities in the whole SN.

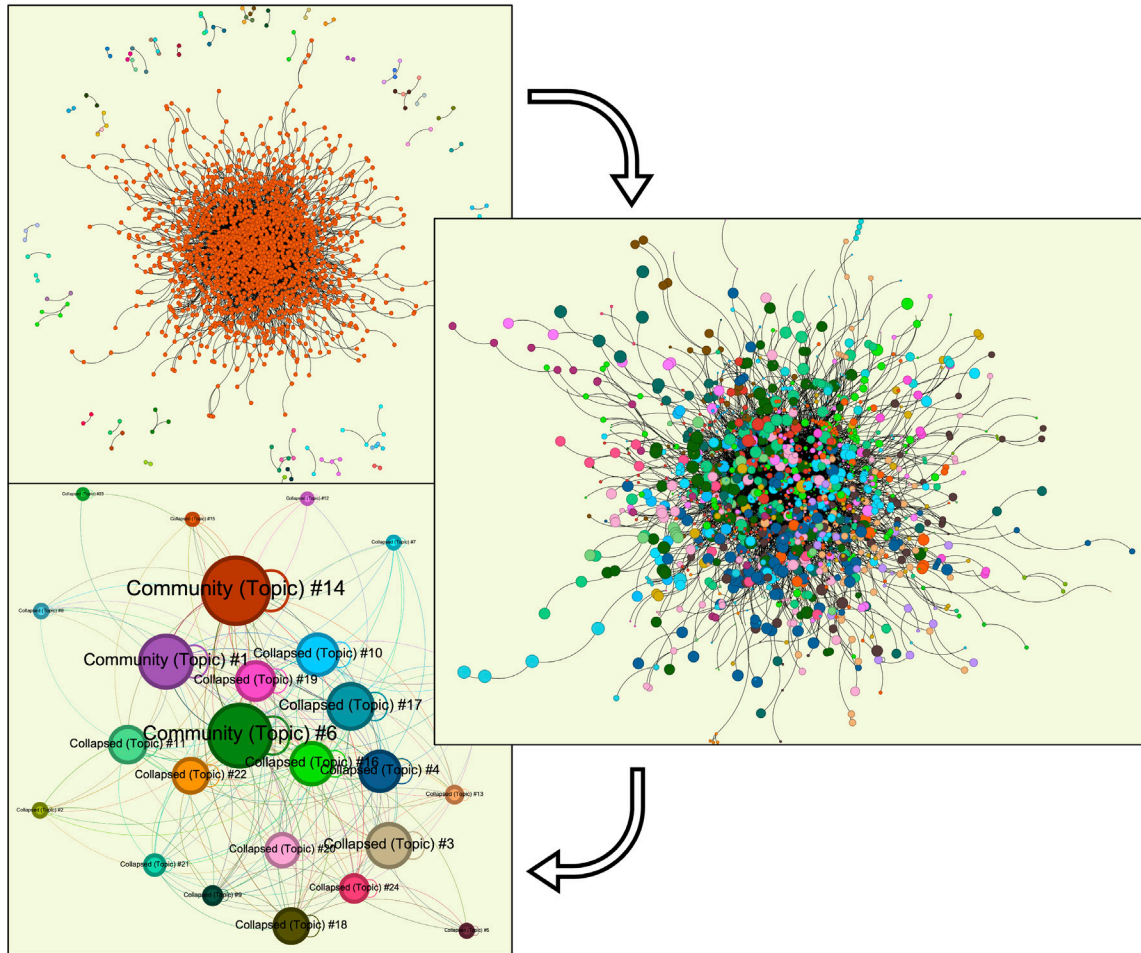


Figure 26. Utilizing the SNA on the entire SN and collapsing it into 25 Semantic Communities

b. Centrality Measurements Analysis

The second step applies the four different centrality measures discussed above to identify important and central nodes (words, terminologies) quantitatively from three perspectives (frequency-based, distance-based, path-based) and to place these nodes in a qualitative semantic context (influence, accessibility, connectivity position) to the

network.¹⁶⁷ This section aims to apply different centrality measurement methods to identify terms with high centrality in the SN. In the following paragraphs, the thesis presents the definitions of the centrality measures and the quantitative and qualitative results.

The first method to measure centrality is frequency-based measurement.¹⁶⁸ The simplest variant of this measurement method is the degree centrality. The degree centrality indicates the sum of all connections a node (i) has to other nodes (x_{ij}) in a network (n). This value one normalizes for comparability by dividing by the total number of nodes excluding the node itself ($n - 1$) in the network (see Figure 27).



Figure 27. Degree Centrality, Formula and a Qualitative Graphical Illustration

With this measurement method the results presented above shows the terms of the SN, which have a high recognition value by their connection network and in this way indirectly influence the network. It does not have to mean that such nodes have a high performance value as a result, because this measurement method is only concerned with the number of connections. An example of a node with a high degree centrality is a simple soldier who knows many other soldiers in a battalion. Such an actor has a high degree centrality and a high recognition value but does not have much power in the battalion.¹⁶⁹

¹⁶⁷ Cunningham, Everton, and Murphy, *Understanding Dark Networks*, 128.

¹⁶⁸ Stanley Wasserman and Katherine Faust, *Social Network Analysis: Methods and Applications* (New York: Cambridge University Press, 1994).

¹⁶⁹ Cunningham, Everton, and Murphy, *Understanding Dark Networks*, 143–48.

The eigenvector centrality is also a frequency-based centrality, but with a different focus. Here, the thesis applies a centrality algorithm based on the assumption that not only the number of connections is crucial, but rather the connection to other central nodes is more decisive. Thereby the eigenvector logarithm considers the most connections of a node (i) to other very connected nodes (x_j) in a SN denotes (see Figure 28).

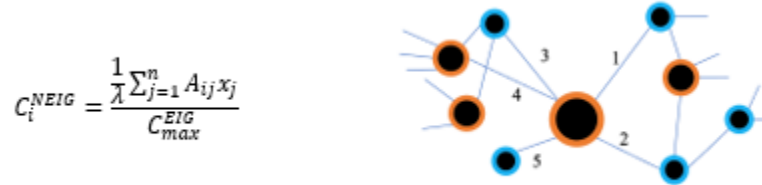


Figure 28. Eigenvector Centrality, Formula, and a Qualitative Graphical Illustration

Here the algorithm uses an adjacency matrix A to set the centrality of node (i) in proportion to its neighbors. Additionally, the algorithm uses the assumed eigenvalue λ . To normalize the eigenvector centrality, the algorithm uses the maximum percentage value of the eigenvector C_{max}^{EIG} . With this value, the thesis determines nodes in the SN that have the most connections to other very central nodes. Such nodes not only have a high recognition value, but also know a network and influence it. To remain in the already mentioned example pattern. Officers in a battalion may not have as many connections, but the connections they do have are powerful because they are connected to other very central positions.¹⁷⁰

Another centrality measurement technique is based on distance. HCC stands apart from frequency-based methods by emphasizing the relative length/distance of the paths between nodes as a critical factor in determining a node's centrality. HCC expresses that due to a relative closeness of a node to other nodes in the network, in terms of the path length that this node is distant from, gives the node a structural power in the network.

¹⁷⁰ Cunningham, Everton, and Murphy, 148.

HCC is calculated by summing the inverses of the geodesic distances (d) between a node and all other nodes in the network. The result is then normalized by dividing it by the total number of nodes in the network minus one ($n - 1$). Unlike the simple CC, this method also accounts for disconnected nodes in the network (see Figure 29).

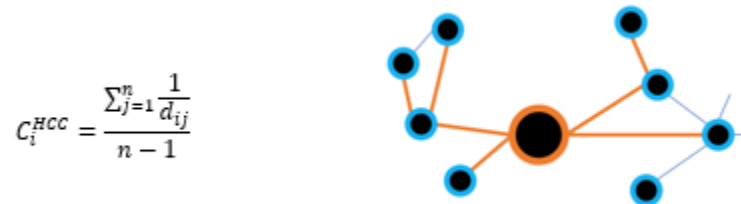


Figure 29. Harmonic Closeness Centrality, Formula and a Qualitative Graphical Illustration

A node with structural power has fast access within the network and represents the structure or the meaning of a network. In military structures, such positions are often professional, technical, and representative officer positions, such as the commander himself, but also logistics officers, technical officers, budget officers, etc. Words with structural power, often serve as central hubs, connecting various concepts and playing a crucial role in conveying relationships and hierarchies.¹⁷¹

The last measurement method that the thesis uses is the betweenness centrality, which is a path-based method. BC expresses that a node is central because it is on the shortest path between two other connected nodes in the network. The assumption is that a node has potential/connectivity power because it connects other possibly weakly connected nodes in the network through itself. Mathematically, the value of BS describes the number of time units that each node takes over a given node to every other node in the network. This implies that g_{ij} quantifies the count of geodesic paths from node i to node j , while g_{ikj} represents the number of geodesic paths from node i to node j passing through a specific intermediary node, k . We calculate the Betweenness Centrality (BC) by summing

¹⁷¹ Cunningham, Everton, and Murphy, 149–52.

the proportion between g_{ikj} and g_{ij} . Furthermore, the resulting value is normalized by dividing it by the constant value of the maximum potential number of node pairs that do not include node k (see Figure 30).



Figure 30. Betweenness Centrality, Formula and a Qualitative Graphical Illustration

A node with a potential/connectivity power describes a connector, such as a senior enlisted leader within a military unit, who has the potential to connect elements. In a semantic network, words with potential connection power are those that play a role in linking and connecting various concepts or nodes within the network. These words often serve as bridges, connectors, or transitions between related ideas.¹⁷²

c. *Preparation of the SN and its decomposition for further analysis*

In the first step of SNA, the thesis conducted the SGA by communities to test the hypotheses and help substantiate the assumption and statement. Using the Gephi social network analysis package, the analysis section can isolate and graph the three dominant communities #14, 6, and 1, as Figure 26 illustrates.¹⁷³ In a subsequent step, the K-Core topology filter refines this cohort of three communities into a 6-core cluster, where each node has at least six connections to every other node within this cluster. This process isolates and identifies the dominant nucleus within the three communities. Figure 31

¹⁷² Cunningham, Everton, and Murphy, 153.

¹⁷³ Mathieu Bastian, Sebastien Heymann, and Mathieu Jacomy, “Gephi: An Open Source Software for Exploring and Manipulating Networks,” *Proceedings of the International AAAI Conference on Web and Social Media* 3, no. 1 (2009): 361–62, <https://doi.org/10.1609/icwsm.v3i1.13937>.

graphically represents the nucleus and displays the most central terms in the three communities.

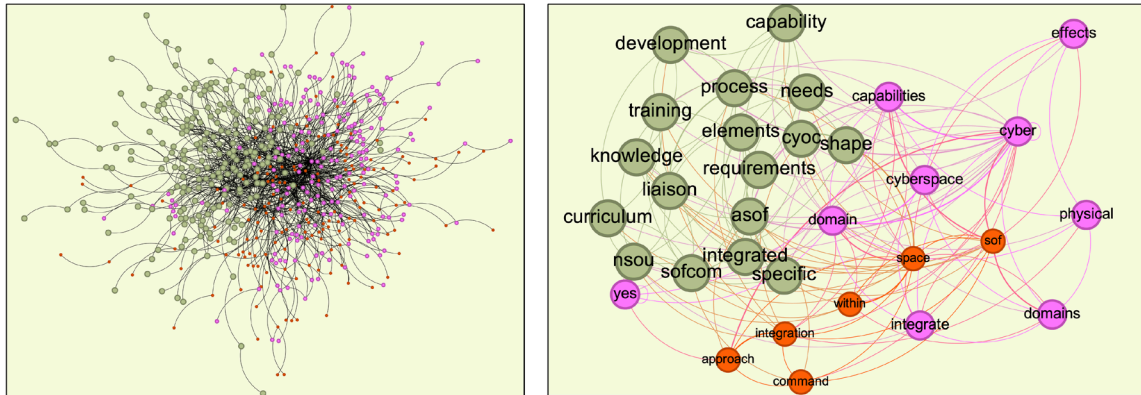


Figure 31. Left: 3 Largest Communities with 579 Nodes and 1145 Edges; Right: 3 Largest Communities shrunk to 6-Core Nucleus Cluster

To quantitatively substantiate the graphical findings quantitatively, the section now applies the centrality measures and summarizes them in Table 8. It presents the ten top-ranked terms in the three communities according to degree-, closeness-, betweenness-, and eigenvector centrality.

Table 8. Centrality Results of the 3 Largest Communities

	Degree Centrality (DC)		Harmonic Closeness Centrality (HCC)		Betweenness Centrality (BC)		Eigenvector Centrality (EC)	
1	cyber	0.173	cyber	0.903	cyber	0.292	cyber	1.000
2	space	0.131	space	0.839	space	0.189	sof	0.712
3	sof	0.104	sof	0.758	domain	0.154	space	0.697
4	domain	0.069	domain	0.726	sof	0.091	capabilities	0.458
5	nsou	0.067	nsou	0.710	nsou	0.081	domain	0.432
6	capabilities	0.066	capabilities	0.694	sofcom	0.080	integration	0.402
7	sofcom	0.059	sofcom	0.694	capabilities	0.073	training	0.393
8	integration	0.059	integration	0.694	integration	0.066	sofcom	0.379
9	asof	0.057	asof	0.677	specific	0.062	nsou	0.359
10	process	0.057	process	0.677	process	0.058	asof	0.347

Figure 32 compares the betweenness centrality of the 6-core with the results of the community detection algorithm SGA 6-core from Figure 31. In the following sections, the

thesis, examines the SGA's three dominant communities using the same approach as this section has done. In this way, the sections will present graphical and quantitative results derived from the centrality measurements.

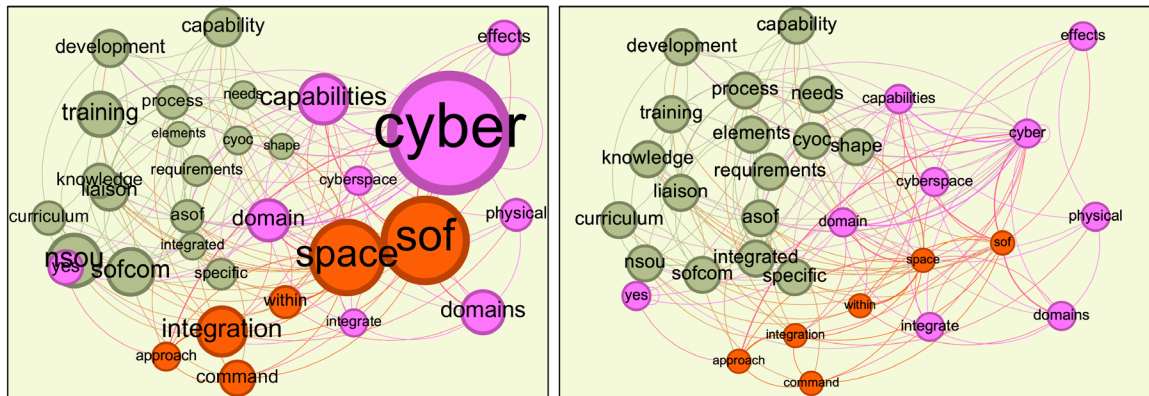
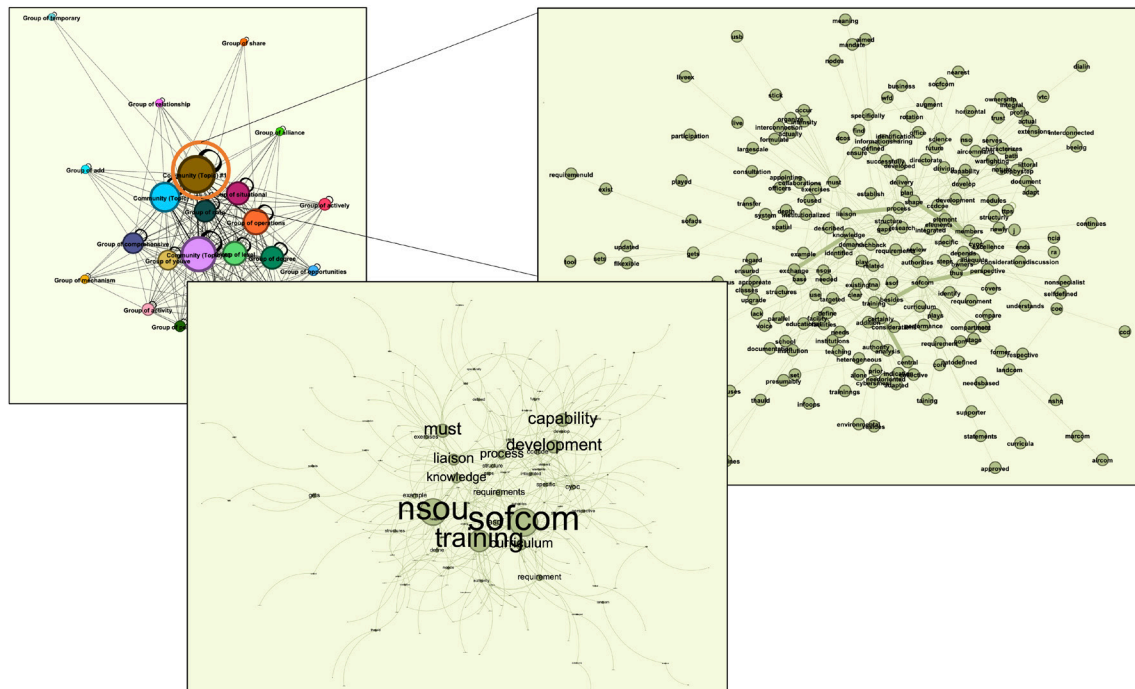


Figure 32. Right: 6-core Nucleus Cluster scaled by SGA; Left: 6-core Nucleus Cluster Scaled by BC.

d. *Analysis of Community #14*

Based on the section before, Figure 33 presents the steps of isolating the largest community. The SNA detects a community consisting of 214 nodes and 374 edges. One can observe that this community strongly communicates around the terms SOFCOM-Training-NSOU. Other prominent keywords like development, must, liaison, capability, knowledge, process, and curriculum stand out.



Top Right: Isolated Community #14 with SGA with 216 Nodes and 374 Edges; Bottom: Isolated Community #14 scaled with BC

Figure 33. Top Left: Collapsed 25 Communities

To quantitatively substantiate the graphical findings quantitatively, the section now applies the centrality measures and summarizes them in Table 9. It presents the ten top-ranked terms in the community #14 according to degree, closeness, betweenness, and eigenvector centrality. The Thesis notes and confirms that the terms SOFCOM, Training, and NSOU are centrally dominant in Community #14, and the terms that the table presents in positions 4 – 10 also have very central values.

Table 9. Centrality Results of the Community #14 within the SN

		Degree Centrality (DC)		Harmonic Closeness Centrality (HCC)		Betweenness Centrality (BC)		Eigenvector Centrality (EC)
1	training	0.140	sofcom	0.504	sofcom	0.242	training	1.000
2	sofcom	0.121	training	0.490	nsou	0.230	sofcom	0.937
3	nsou	0.098	nsou	0.490	training	0.188	nsou	0.798
4	development	0.093	curriculum	0.440	must	0.117	liaison	0.539
5	capability	0.088	development	0.439	development	0.115	development	0.525
6	liaison	0.084	liaison	0.433	capability	0.113	curriculum	0.524
7	must	0.070	process	0.429	liaison	0.097	asof	0.448
8	knowledge	0.070	knowledge	0.424	curriculum	0.092	process	0.443
9	curriculum	0.070	must	0.422	knowledge	0.084	requirements	0.435
10	asof	0.065	capability	0.421	process	0.082	knowledge	0.430

Finally, the section illustrates the centrality results in Table 9 graphically in Figure 34. The section shows exemplarily the 4-core nucleus clusters of Community #14 on which the SNA applies the BC. This figure substantiates the centrality of the terms SOFCOM, training, and NSOU and graphically illustrates the interrelation of key terms such as development, must, liaison, curriculum, capability, etc.

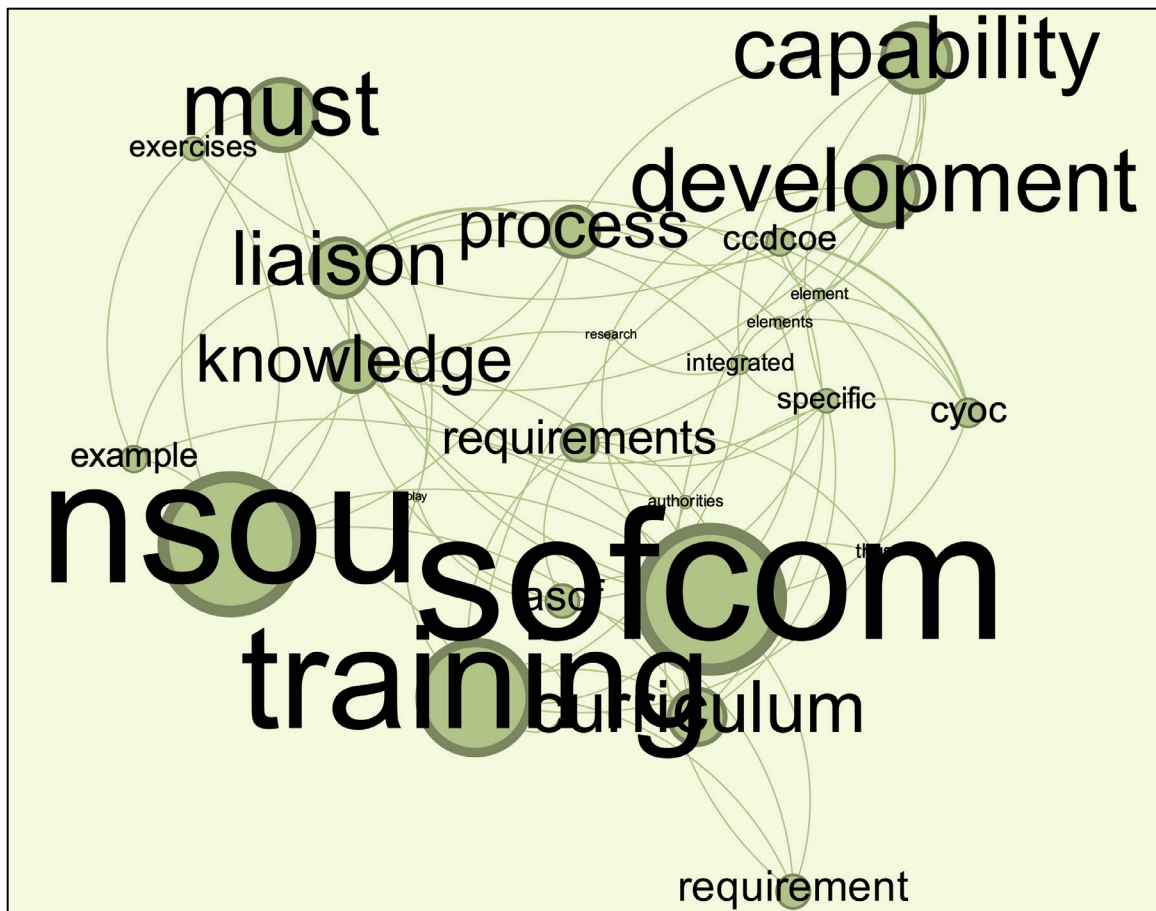
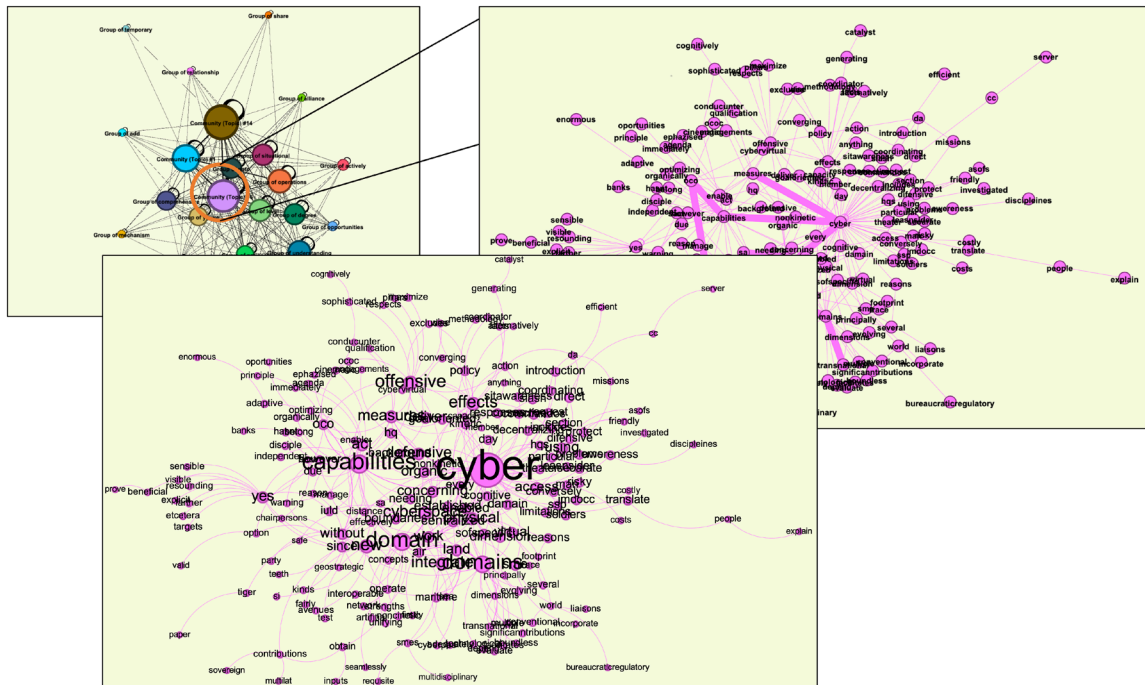


Figure 34. Community #14 4-Core Cluster, Scaled with BC

e. Analysis of Community #6

Further on, Figure 35 presents the steps of isolating the Community #6. The SNA detects a community consisting of 200 nodes and 308 edges. The thesis recognizes that this community communicates strongly around the term Cyber. Other central keywords, such as domain, yes, offensive, effects, and new stand out and build visual clusters.



Top Right: Isolated Community #6 with SGA with 200 Nodes and 308 Edges; Bottom: Isolated Community #6 scaled with BC

Figure 35. Top Left: Collapsed 25 Communities

To substantiate the graphical findings quantitatively, the section now applies the centrality measures and summarizes them in Table 10. It presents the ten top-ranked terms in community #6 according to degree, closeness, betweenness, and eigenvector centrality. The Thesis notes and confirms that the term Cyber is centrally dominant in Community #6 and the terms that the table presents in positions 4 – 10 also have very central values.

Table 10. Centrality Results of the Community #6 within the SN

	Degree Centrality (DC)	Harmonic Closeness Centrality (HCC)	Betweenness Centrality (BC)	Eigenvector Centrality (EC)				
1	cyber	0.327	cyber	0.621	cyber	0.548	cyber	1.000
2	domains	0.131	capabilities	0.508	capabilities	0.178	capabilities	0.432
3	capabilities	0.126	domain	0.493	domains	0.166	domain	0.399
4	domain	0.111	domains	0.490	domain	0.149	domains	0.379
5	yes	0.080	offensive	0.457	yes	0.095	offensive	0.281
6	offensive	0.075	new	0.451	effects	0.092	new	0.260
7	effects	0.075	effects	0.444	offensive	0.089	effects	0.244
8	physical	0.065	physical	0.431	physical	0.085	cyberspace	0.235
9	cyberspace	0.060	cyberspace	0.430	new	0.065	integrate	0.223
10	without	0.055	integrate	0.430	cyberspace	0.065	physical	0.209

Finally, the section illustrates the centrality results in Table 10 graphically in Figure 36 the section shows exemplarily the 4-core nucleus clusters of Community #6 on which the SNA applies the BC. This figure substantiates the centrality of the term Cyber and further emphasizes other interrelated key terms such as capabilities, domain physical, yes, offensive, effects, etc.

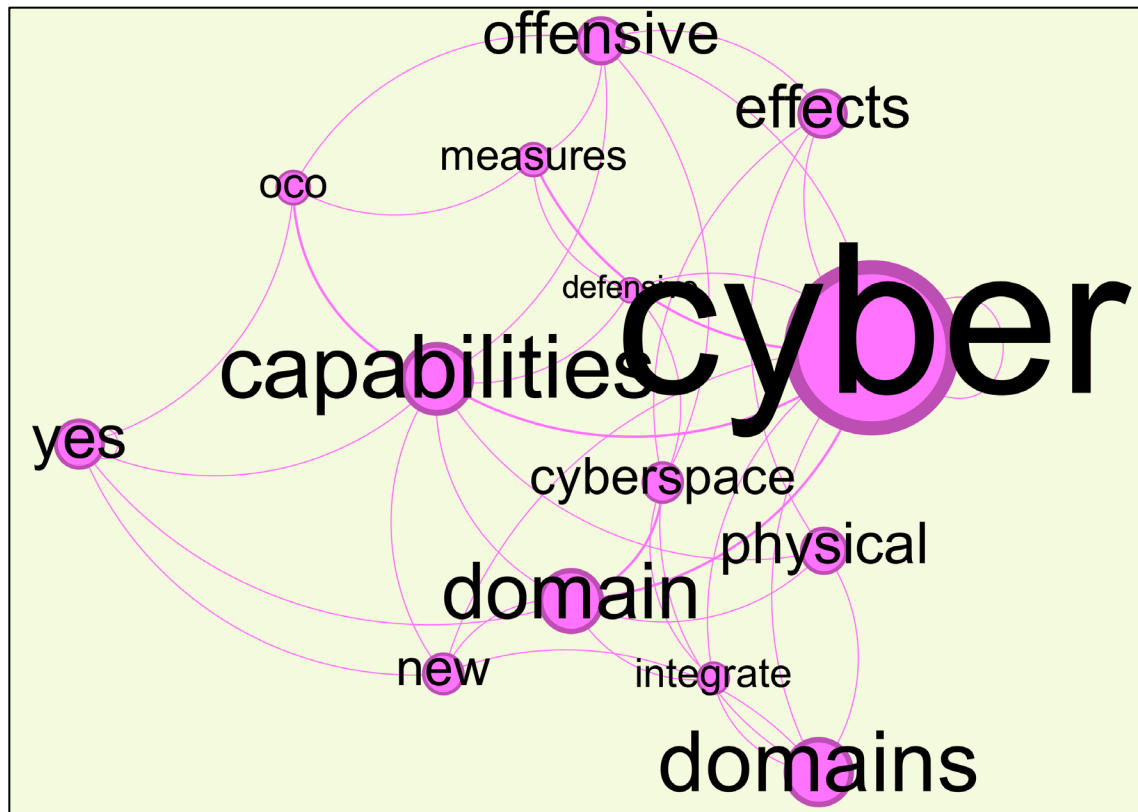
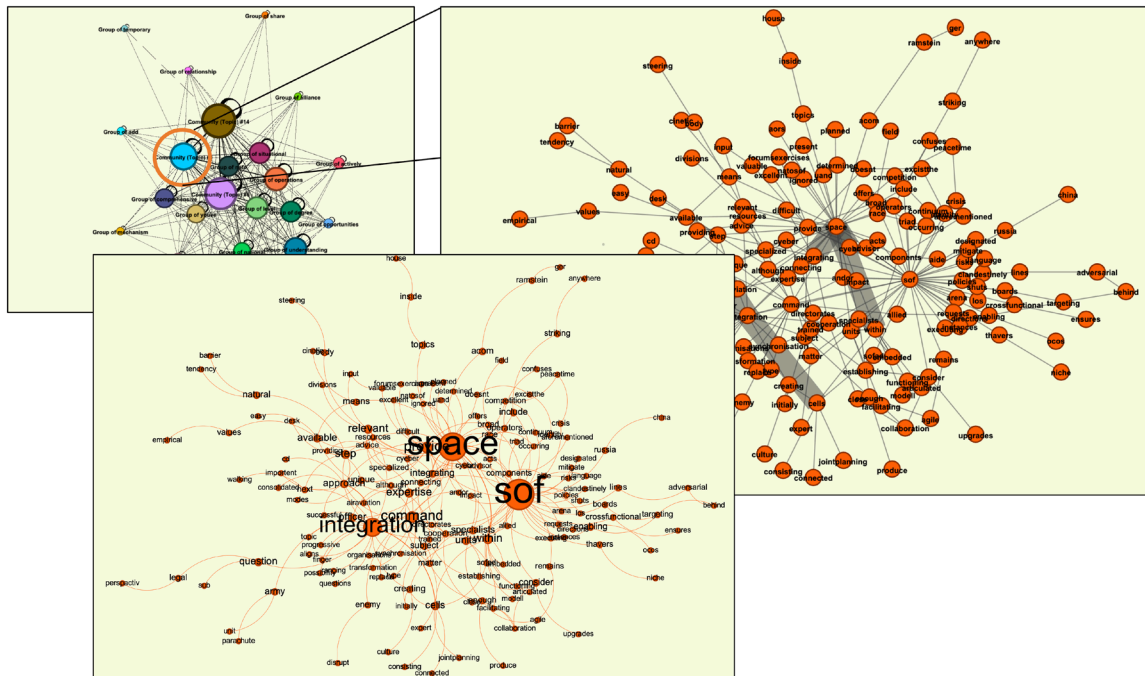


Figure 36. Community #6 4-Core Cluster scaled with BC

f. Analysis of Community #1

Last, the section examines community #1. Figure 37 presents the steps of isolating the Community #1. The Community #1 consists of 163 nodes and 233 edges. The section illuminates that the semantic community interacts with the words Space and SOF. SOF – Space builds a center of gravity and other strong interconnected terms such as integration, command, cyber, expertise, provide, relevant, etc., surround it.



Top Right: Isolated Community #1 with SGA with 163 Nodes and 233 Edges; Bottom: Isolated Community #1 scaled with BC

Figure 37. Collapsed 25 Communities

Also, in the last section of the SNA with community #1, the intention is to confirm the graphical results with quantitative applications. The thesis utilizes the centrality measures and summarizes the results in Table 11. It presents the ten top-ranked terms in community #1 according to degree, closeness, betweenness, and eigenvector centrality. The table notes and confirms that the terms SOF and Space are centrally dominant in Community #1 and build the center of gravity. The terms that the table presents in positions 3 – 10 also have very central values.

Table 11. Centrality Results of the Community #1 within the SN

	Degree Centrality (DC)	Harmonic Closeness Centrality (HCC)	Betweenness Centrality (BC)	Eigenvector Centrality (EC)
1	sof 0.278	sof 0.591	sof 0.471	sof 1.000
2	space 0.222	space 0.570	space 0.424	space 0.897
3	integration 0.136	integration 0.510	integration 0.242	integration 0.551
4	provide 0.086	command 0.463	command 0.103	command 0.411
5	command 0.080	provide 0.453	provide 0.099	provide 0.384
6	within 0.062	expertise 0.434	within 0.060	within 0.318
7	approach 0.049	within 0.434	expertise 0.055	integrating 0.309
8	integrating 0.043	units 0.422	step 0.054	expertise 0.300
9	step 0.043	integrating 0.419	relevant 0.052	cyber 0.291
10	cells 0.043	specialists 0.412	cells 0.471	units 0.276

In conclusion, Figure 38 graphically represents the centrality results from Table 11. Specifically, it provides a visual depiction of the 3-Core nucleus clusters within Community #1, demonstrating the application of BC. This visual representation reinforces the importance of the terms ‘Space’ and ‘SOF’ within this Community. Furthermore, the figure underscores their interconnectedness with other key terms, including integration, Cyber, command, provide, relevant, etc.

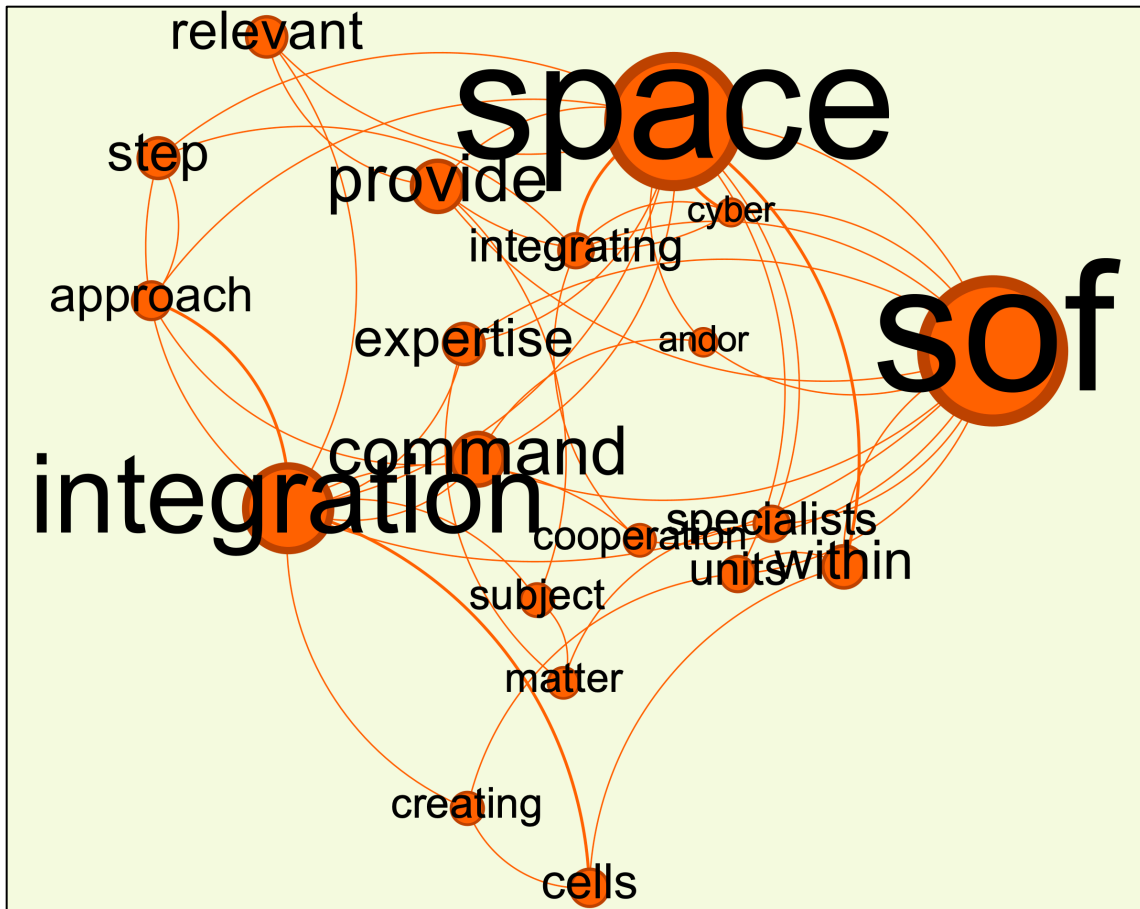


Figure 38. Community #1 3-Core Cluster Scaled with BC

This chapter provides a summary of the data collection process employed in the thesis, which included expert interviews. The thesis employed two distinct analysis approaches to test hypotheses H1, H2, H3, and H4. The first analysis method involved the use of BDA and SDDA for quantitative analysis. The second approach employed a hybrid method, combining SNA with qualitative elements. In the subsequent chapter, the thesis will evaluate the analysis results and present the key findings.

THIS PAGE INTENTIONALLY LEFT BLANK

V. ASSESSMENT AND FINDINGS

In the previous chapter, the thesis conducted an evaluation using BDA, SDDA, and SNA. The comprehensive assessment unequivocally confirms the validity of hypotheses H1, H2, H3, and H4.

H1: A-SOF lacks significant expertise in cyber and space domains, hindering the development of sustainable interoperability.

H2: SOFCOM's integral training facility, NSOU, holds significant importance in cultivating fundamental and supplementary knowledge for achieving interoperability with Cyber and Space.

H3: SOFCOM is uniquely qualified to advance interoperability with cyber and space to enhance NATO's 360-degree approach.

H4: Integrating specific liaison elements enhances Space, Cyber, and A-SOF interoperability capabilities.

As a result, the thesis asserts the correctness of the underlying research assumption, *“NATO's strategic goal, to evolve modern warfare from JO to MDO as a 360-degree approach, directly relates to cyber and space domains and their interoperability with other domains and warfighting elements.”* Simultaneously, the contention (research statement) that, *“A-SOF enhances capabilities and interoperability to cyber and space with established structures in NFS and NCS, thus supporting the 360-degree MDO approach capability, contributing to NATO's strategic goals.”* stands as a critical component for a conclusive response to the research question in the recommendations.

A. DISTRIBUTIONS ANALYSIS ASSESSMENT

This section reveals that both distributional analysis methods, BDA and SDDA, provide robust support for hypotheses H1, H2, H3, and H4. All four hypotheses are conclusively affirmed, with clear to overwhelming majorities based on expert binary ratings. Moreover, the section addresses the open-ended questions linked to these hypotheses with high semantic differentiation ratings. The scenario section of the interviews is also clear and supports the hypotheses with both analyses. As a result, the test culminated in a resounding confirmation of the hypotheses.

1. Binary Distribution Analysis Assessment

Utilizing BDA, Figure 39 presents a graphical summary of expert binary assessments. Figure 39 illustrates that a significant majority of interviewees 97% unequivocally endorse the hypotheses. Additionally, the experts lend their support with 59% average to the assertion that SOFCOM's specificity as a MOU organization equips it to effectively address challenges in a superior manner compared to other organizations.

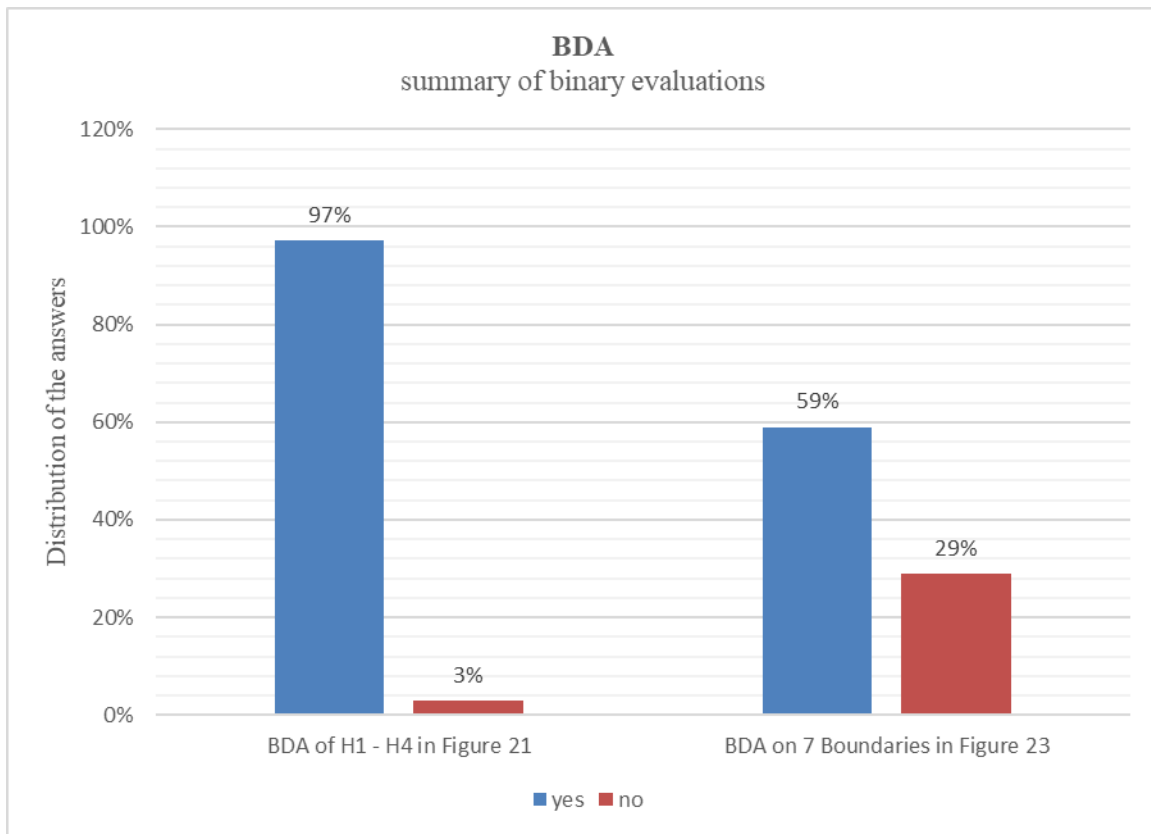


Figure 39. Summary of the Results from the BDA of the Interviews with Experts

In the left distribution diagram of Figure 39, this section evaluates, in summary, several key findings in relation to the four hypotheses. First, it identifies a knowledge gap that exists between A-SOF and cyber, and space domains, hindering the development of practical solutions for improved interoperability. Second, it highlights the central role played by SOFCOM's organic training facility NSOU in closing this knowledge gap.

Third, it emphasizes that SOFCOM possesses unique qualifications for enhancing interoperability between A-SOF and the cyber and space domains, thanks to its doctrinal and structural advantages. Fourth, it underscores the importance of interoperability elements such as liaison, planning, and advisory functions in tangibly improving collaboration between A-SOF, Cyber, and Space.

In the right-hand distribution diagram of Figure 39, the section assesses that SOFCOM, in its capacity as an MOU organization, is better suited than other NFS organizations to advance NATO's goal of evolving modern warfare from JO to MDO incrementally. The distribution of responses by the majority that boundaries, as described by Moroney, can particularly affect an alliance such as NATO, and political intentions and strategic goals/objectives can be significantly slowed down and sometimes not implemented at all.¹⁷⁴ This outcome not only supports Hypothesis 3 but also emphasizes the unique role of SOFCOM within the NFS framework.

2. Semantic Differentiation Distribution Analysis Assessment

Applying SDDA, this section of the thesis provides a visual summary of the semantic assessments. As depicted in Figure 40, a clear majority of interviewees strongly support hypotheses H1, H2, H3, and H4, leading to further findings supporting the thesis's research argument, mentioned above. The histograms within Figure 40 reveal that 68% of respondents rate the hypotheses with a semantic value of 5, signifying the highest degree of value. Likewise, questions Q1 – Q6 are also assigned a value of 5, indicating their high value. Lastly, the experts assess both scenarios with a 50% consensus, assigning a semantic highest value of 5 for appropriateness, realism, and feasibility.

¹⁷⁴ Moroney et al., *Overcoming Barriers to Working with Highly Capable Allies*.

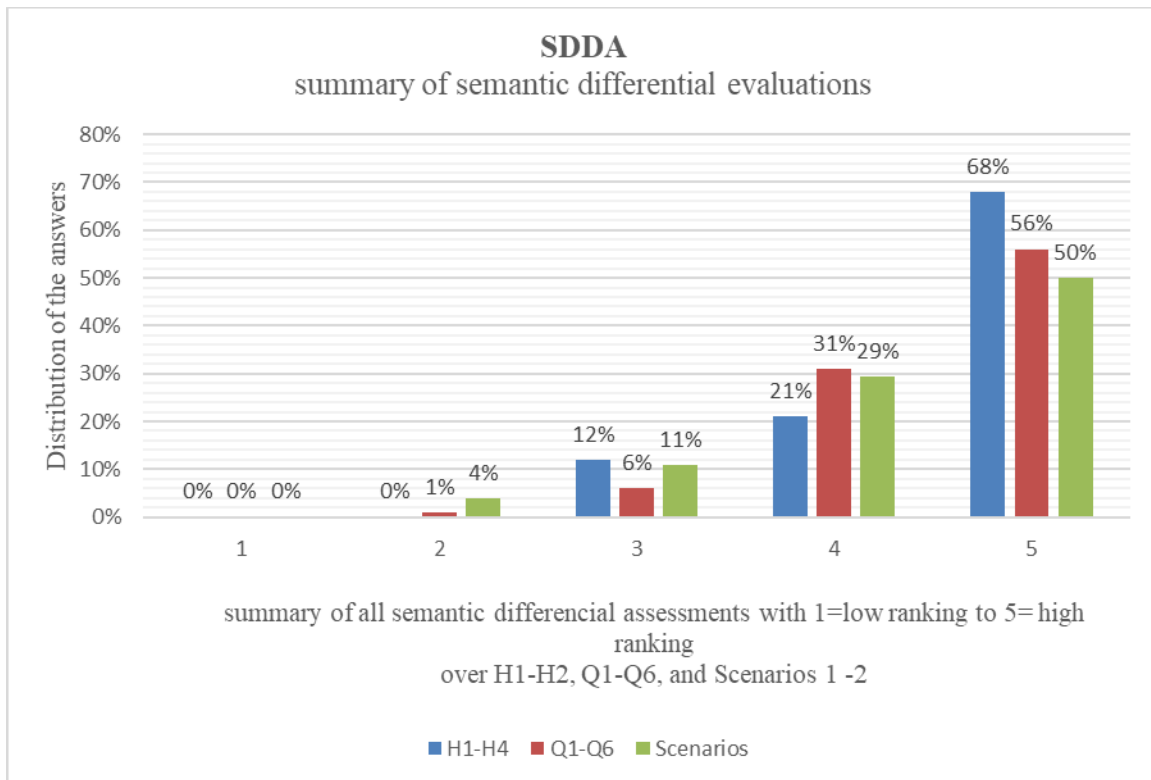


Figure 40. Summary of the Results from the SDDA of the Interviews with Experts

This section yields further findings from the SDDA. First and foremost, it becomes evident that achieving a MDO capability in alignment with NATO’s objectives necessitates significant enhancements in A-SOF. These enhancements include the integration of robust interoperability measures with the cyber and space domains, harnessing the offensive capabilities of the cyber domain, and leveraging specialized support capabilities within the space domain through SpSC. Secondly, SOFCOM emerges as a key facility within A-SOF, possessing both advantages and essential structural capabilities that enable the consistent integration of cyber and space capabilities with A-SOF. This integration not only fortifies A-SOF but also contributes to NATO’s overarching development objectives, as articulated in the research assumption at the beginning of the chapter. Third, experts recognize A-SOF’s distinct qualifications. Leveraging the organizational structures of SOFCOM and drawing upon A-SOF’s valuable lessons from joint NATO deployments, SOFCOM can strategically develop a synchronization, communication, and information-sharing

platform. This platform serves to bridge the operational command levels of SOFCOM, the CyOC, and the SpCen. Through this initiative, A-SOF not only cultivates robust interoperability but also fosters cross-domain awareness and coherence within the Cyber and Space domains. Finally, fourth, experts underscore the importance of a more complementary role for NSOU within the interoperability framework. This role includes offering a coordinated curriculum and establishing an academic network focused on cyber and space, thereby enriching the knowledge base and resources essential for these domains.

B. SEMANTIC NETWORK ANALYSIS ASSESSMENT

This section describes the assessments that the thesis draws after conducting the SNA. In general, the SNA detects three dominant communities and supports hypotheses H1, H2, H3, and H4 both quantitatively with results on centrality measurements, and qualitatively through graphical representations and semantic interpretations. With the evaluation of the SNA, the thesis provides a total of three findings for community #14, two findings for community #6, and ZX assessments for community # 1.

1. Assessments for Community #14

In the first community, the centrality values from Table 9 indicate strong support for hypotheses H1 and H2, surpassing the average. Notably, the organic training facility “NSOU,” the operational command “SOFCOM,” and the field of action “Training” emerge as central concepts in addressing the issue of improving interoperability between A-SOF, Cyber, and Space. The concept of “Training,” with an EC value of $C_i^{NEIG} = 1.00$, stands out as the term interconnected with all other crucial and highly connected terms and concepts. This topic complex holds significant recognition within SOFCOM’s broader social network and exerts a considerable influence across the 25 communities.

The key finding from this assessment is that, for SOFCOM, “NSOU” should play a central role in developing solutions for enhanced collaboration in education and training with the Cyber and Space domains (see Figure 41). This finding supports strongly H1: **“A-SOF lacks significant expertise in cyber and space domains, hindering the development of sustainable interoperability .”** and H2: **“SOFCOM’s organic training**

facility, NSOU, is of substantial importance in developing basic and complementary knowledge for interoperability with Cyber and Space.”

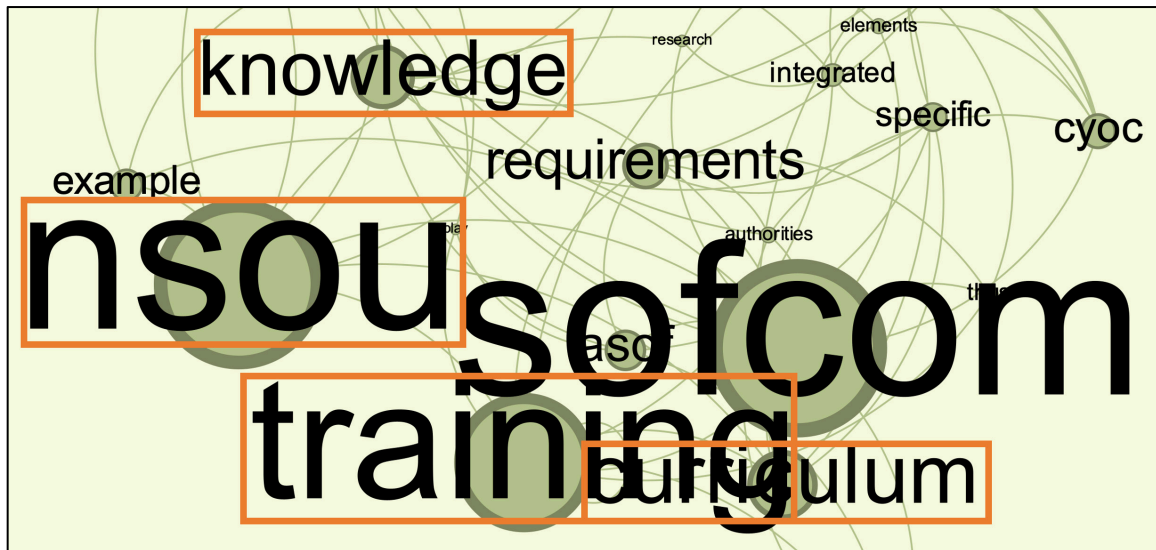


Figure 41. Education, as a Key finding for Interoperability

Secondly, the term “liaison” holds a central position in the social network of Community #14, reinforcing hypotheses H3 and H4 and underscoring the significance of interconnectivity, particularly for the A-SOF. “Liaison” stands out with a high HCC value of $C_i^{NHCC} = 0.433$ and an EC value of $C_i^{NEIG} = 0.539$ in the analysis. This term acts as a hub, offering crucial access to information, with its high HCC value amplifying its structural power. The A-SOF’s ability to work with established liaison elements is instrumental in implementing NATO’s 360-degree approach effectively. As the A-SOF operates with liaison elements aligned with their capability profile, SOFCOM uniquely positions itself to contribute a liaison-based approach, enhancing interoperability with the CyOC and the SpCen.

This assessment leads to the second key finding: the exchange of interoperability elements, such as cross-domain awareness (communication, cooperation development, synchronization, etc.), supports the development of improved interoperability between A-SOF, Cyber, and Space, contributing to NATO’s 360-degree approach (see Figure 42).

This finding strongly supports H4: **“Integrating specific liaison elements enhances Space, Cyber, and A-SOF interoperability capabilities.”**

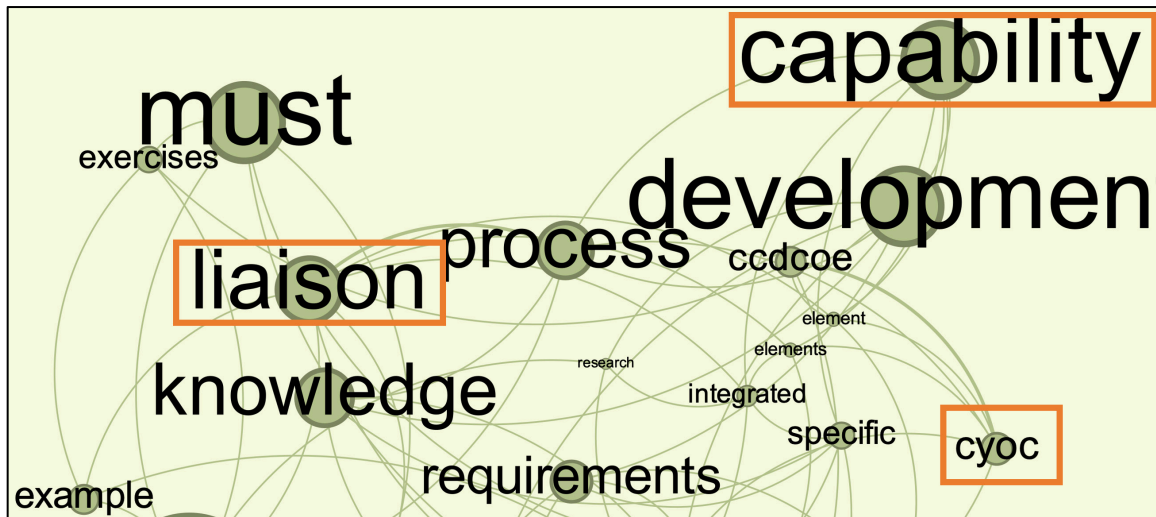


Figure 42. Liaison Elements for Better Interoperability

Thirdly, the term “must” holds a central position within the community #14 as well. It embodies a strong sense of obligation, necessity, and requirement, signifying a firm commitment by Community #14 across the entire network of 25 communities. With HCC values of $C_i^{NHCC} = 0.422$ and BCC of $C_i^{NEIG} = 0.539$, this term wields structural and connective power, offering access and facilitating connections among concepts and other terms. Interpretively, Community #14, alongside its central concepts and institutions, such as SOFCOM, NSOU, and key capabilities like liaison, assumes highly obligating roles within the topic complex related to the RQ and throughout the entire social network.

This assessment leads to the third key finding, emphasizing that **“SOFCOM must take an active and committed role in shaping and improving interoperability with cyber and space”** (see Figure 43).



Figure 43. SOFCOM's Role and Positioning toward Integration Efforts.

2. Assessments for Community #6

The evaluation of the analysis results of Community #6 provides information on how A-SOF integrates the cyber component in answering the RQ. The evaluation opens terms and concepts that serve as findings and that A-SOF must address in order to answer the RQ in a goal-oriented manner and in accordance with the NATO guidelines of the 360-degree approach.

Community #6 also yields clear results from the analysis. As shown in Table 10, the term “cyber” emerges as the most central term within Community #6. In the 4-core nucleus cluster, terms such as “capabilities,” “offensive,” “effects,” and “OCO” gravitate around “Cyber.” Cyber, both as a domain and a platform for unique capabilities, assumes a pivotal role for A-SOF, particularly regarding its offensive capabilities within NATO’s 360-degree MDO approach and the RQ-related component of how A-SOF can collaborate

with the cyber domain. To exemplify the assessment for the offensive interpretation of the cyber domain for the RQ, this section shows that the term “offensive” scores an HCC value of $C_i^{NHCC} = 0.457$ and the term ‘effect’ scores an HCC value of $C_i^{NHCC} = 0.444$. The term “offensive” and “effects” bestowing structural power upon Community #6 and serving as a gateway to other concepts and terms across all 25 communities within the social network especial for SOFCOM and Space and the communities #14 and #1.

The initial assessment of Community #6 leads to an important finding (see Figure 44): **“Cybers OCO offer a promising avenue for achieving MDO-oriented interoperability with A-SOF.”**

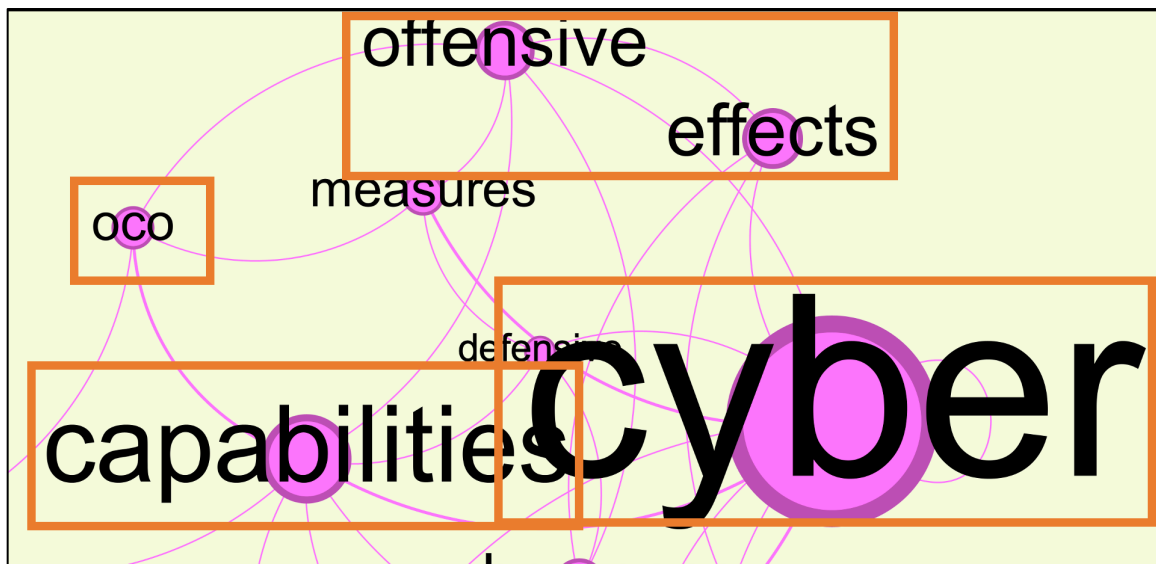


Figure 44. Cyber and its Offensive Effects as Structural Power Components for Better Interoperability

Secondly, the term ‘yes’ occupies a central position within Community #6. “Yes” establishes numerous connections with other terms and acts as a crucial connector among the various elements in the network. Although it scores relatively low with a DC value of $C_i^{NDC} = 0.08$ and a BC value of $C_i^{NBC} = 0.095$. Yet, it still secures a spot among the top-five terms within Community #6, underscoring its role in facilitating connections across the network with recognition and connection power.

Linguistically, “yes” signifies agreement, approval, consent, or confirmation. In this position, it serves as a connective power, fostering ties between different concepts and terms. From an interpretive standpoint, Community #6, with Cyber as its focal point, aligns with and affirms the research assumption, which asserts, “NATO’s strategic goal, to evolve modern warfare from JO to MDO as a 360-degree MDO approach, directly relates to cyber and space domains and their interoperability with other domains and warfighting elements.” Additionally, the research statement that *“A-SOF enhances capabilities and interoperability to cyber and space with established structures in NFS and NCS, thus supporting the 360-degree MDO approach capability, contributing to NATO’s strategic goals”* is confirmed.

This assessment strengthens the key finding in community #6, emphasizing that **“Cybers OCO offer a promising avenue for achieving MDO-oriented interoperability with A-SOF.”**

3. Assessments for Community #1

The evaluation of Community #1 offers valuable insights, particularly regarding the key terms “SOF,” “Space,” and “Integration.” Community #1’s evaluation supports hypothesis H3, which claims that A-SOF’s SOFCOM is uniquely qualified to enhance interoperability between A-SOF SOF as a warfighting element and functional domain, and cyber and space, with the SOF and space components. Additionally, the term “Integration” provides substantial support for both hypothesis H4, which emphasizes the sharing of interoperability elements to enhance overall interoperability and the core statement of the thesis. An analysis of Table 11 reveals that “SOF” and “Space” serve as the central focal points within Community #1. The term ‘Integration’ complements these central concepts with significant values: $C_i^{NHCC} = 0.51$, a BC value of $C_i^{NBC} = 0.242$, and EC value of $C_i^{NEC} = 0.242$. These values, especially the high structural power (HCC) and influence power (EC) of the term ‘Integration,’ highlight that Space, with its unique support capabilities via SpSC, aligns seamlessly with SOF in the context of NATO’s 360-degree approach, creating a cohesive connection within the entire social network (SN). Other

central terms such as “relevant,” “provide,” “expertise,” “specialists,” and “cooperation” support the integration idea of SOF and Space with their central values.

The first finding from Community #1 affirms that **“A-SOF, a warfighting element, fosters interoperability, particularly with Space entities, driving integration”** (see Figure 45).

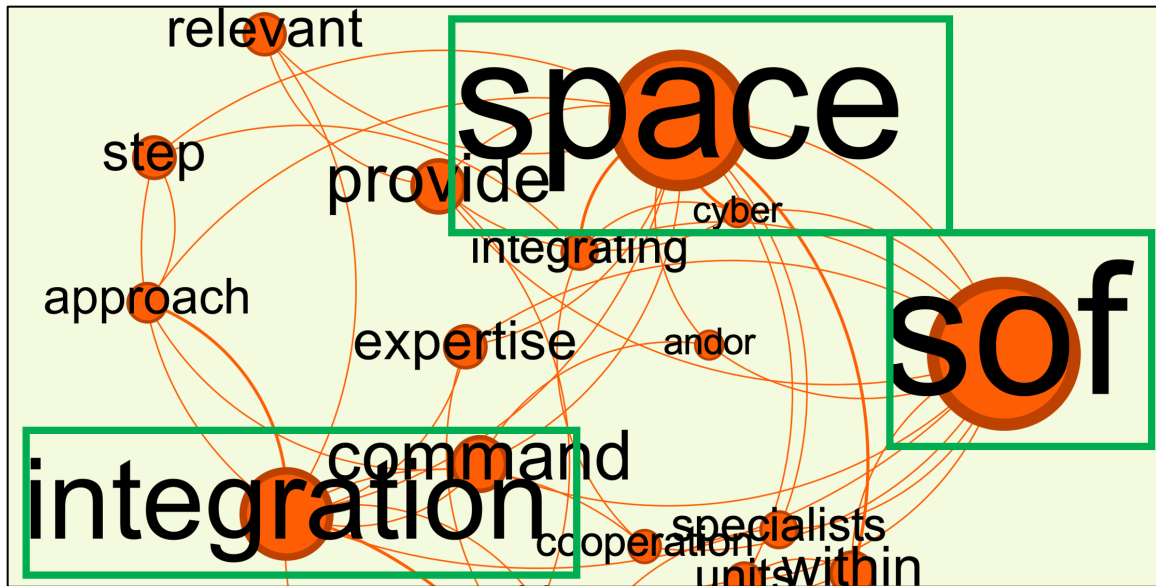


Figure 45. Space, SOF and Integration, the Central Components within Community #1

The 3-core nucleus cluster of community #1 presents the word “within” as a central preposition of the network. As with the terms “must” and “yes” before, which interpreted the sections in the respective other community evaluations, the thesis evaluates the centrality values of the preposition with HCC $C_i^{NHCC} = 0.434$ and with EC $C_i^{NEC} = 0.318$ and interprets them in consideration of the topic of examination. In this context the term “within” denotes the idea that the terms “Space,” “SOF” and “integration” occur within the specific context of the research statement ***“A-SOF enhances capabilities and interoperability to cyber and space with established structures in NFS and NCS, thus supporting the 360-degree MDO approach capability, contributing to NATO’s strategic goals.”***

This assessment highlights further support the key finding in Community #1, underscoring that, **“A-SOF, a warfighting element, fosters interoperability, particularly with Space entities, driving integration.”**

C. SUMMARY OF THE ASSESSMENTS OF THE ANALYSES

The thesis assessed two different analysis methods. In the first part of the evaluation, the thesis focused on the two distribution analyses BDA and SDDA. In this assessment, most experts confirmed hypotheses H1, H2, H3, and H4. In the second part of the chapter, the thesis shifted its focus to SNA. Here, the results not only confirmed the four hypotheses H1, H2, H3, and H4 but also yielded three additional findings. These seven over all findings (see Table 12). will guide the thesis in developing the recommendations and consistently answering the RQ.

Table 12. Main Findings derived from the Assessment Process

#	Findings
F1	H1: A-SOF lacks significant expertise in cyber and space domains, hindering the development of sustainable interoperability .
F2	H2: SOFCOM's integral training facility, NSOU, holds significant importance in cultivating fundamental and supplementary knowledge for achieving interoperability with Cyber and Space.
F3	H3: SOFCOM is uniquely qualified to advance interoperability with cyber and space to enhance NATO's 360-degree approach
F4	H4: Integrating specific liaison elements enhances space, cyber, and A-SOF interoperability capabilities
F5	SOFCOM must take an active and committed role in shaping and improving interoperability with cyber and space
F6	Cybers OCO offer a promising avenue for achieving MDO-oriented interoperability with A-SOF
F7	A-SOF, a warfighting element, fosters interoperability, particularly with space entities, driving integration.

The final chapter contains a summary of all the steps the thesis has taken. The chapter will then connect the seven key findings to the RQ and a presentation of recommendations, which the thesis concluded in this chapter in Table 12 will follow. Finally, an outlook and suggestion of how A-SOF and other entities can utilize the analysis method of SNA for other research projects will conclude.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION WITH FINDINGS, RECOMMENDATIONS AND OUTLOOK

A. REVIEW OF THE RESEARCH DEVELOPMENT AND APPROACH

The research question RQ in this thesis emerged from NATO's strategic reorientation, aimed at adapting to the changing nature of warfare from JO to MDO, following NATO's 360-degree approach. This study addresses the RQ over the course of six chapters. To highlight the significance of a multi-domain approach involving A-SOF, cyber, and space capabilities, the thesis draws upon a historical example: the Russian cyber-attack on ViaSat, which marked the first strike in the conflict with Ukraine. This example underscores the vital role of these domains in modern warfare and their interaction. Notably, the attack failed due to the absence of the Russian SOF to sustain the initial successes achieved through Russian OCO.

Based on an in-depth literature review, the thesis developed the research assumption that *“NATO's strategic goal, to evolve modern warfare from JO to MDO as a 360-degree approach, directly relates to cyber and space domains and their interoperability with other domains and warfighting elements.”* From that standpoint the thesis derived the research statement: *“A-SOF enhances capabilities and interoperability to cyber and space with established structures in NFS and NCS, thus supporting the 360-degree MDO approach capability, contributing to NATO's strategic goals.”* These two building blocks enabled the thesis to develop four hypotheses, tested to answer the research and analysis chapter's research question. To conduct the research, the thesis collected the necessary data by interviewing experts from the A-SOF, cyber, and space domains.

The thesis tested the hypotheses with the help of two quantitative analysis methods BDA, SDDA and a hybrid method of SNA. All analysis approaches provided reliable quantitative and qualitative results, which the thesis then assessed in detail in the evaluation and findings chapter. The evaluation very clearly confirmed all four hypotheses and established a further three findings. Based on these products, it is possible for the thesis to develop specific recommendations in this chapter and to address these recommendations to the decision-makers. In the findings section, the thesis articulates the key findings

derived from testing the hypotheses. The findings serve as an instrument to develop recommendations to answer the RQ.

B. MAIN FINDINGS

The primary findings of this thesis encompass Hypotheses H1, H2, H3, and H4, all of which have yielded positive results. The thesis outlines all the key findings F1 – F7, that emerged from the research and that Table 12 summarizes.

Firstly, the results consistently confirm the validity of H1, which posits that “A-SOF lacks significant expertise in cyber and space domains, hindering the development of sustainable interoperability.” The research indicates a lack of comprehensive understanding within the A-SOF community regarding these emerging domains and their operational principles. Experts concur that acquiring knowledge about cyber and space is essential before A-SOF can effectively engage in cooperative efforts and establish interoperable capabilities. This aligns with Blessing, Elgin, Ewers-Peters, and Tiderman’s assertion that a successful strategy hinges on understanding one’s operational environment and capabilities.¹⁷⁵ This observation is particularly pertinent at the operational level for A-SOF. Consequently, the thesis contends that SOFCOM, as the requirements authority, should identify this knowledge gap, address training needs, and allocate resources to bridge this crucial knowledge deficiency.

Secondly, the results and evaluations from the BDA, SDDA, and SNA consistently affirm the validity of H2, which states that “SOFCOM’s organic training facility, NSOU, plays a vital role in cultivating the essential knowledge required for A-SOF’s interoperability with Cyber and Space domains.” NSOU, as SOFCOM’s organic training facility, seeks to enhance MDO capabilities within NATO’s core education and training activities by implementing targeted cross-domain education and training. This would significantly contribute to the readiness of the NCS and NFS, ultimately leading to an enhancement in Alliance LOA.¹⁷⁶ Experts within the A-SOF community, from the new

¹⁷⁵ Blessing et al., “New Decade, New Challenges, and New Opportunities,” 2.

¹⁷⁶ Supreme Allied Commander, Europe and Supreme Allied Commander, Transformation, *Bi-SC Education and Individual Training*, 8.

domains of cyber and space, but also science and the economy, confirm that NSOU is in many ways particularly qualified to play a leading role in shaping the contribution that this section illustrates. On the one hand, COM SOFCOM, as the A-SOF requirement authority, has full command (FULLCOM) over NSOU and has an immediate and direct influence on its design and actions.¹⁷⁷ On the other hand, the USA organizes NSOU as an FN under the MOU, providing the school with flexibility and speed for development measures, although it is not part of the NFS. Regardless of the organizational form, NSOU is certified and accredited by NATO so that NSOU can offer content and a curriculum coordinated with NATO requirements to allies.¹⁷⁸ As SOFCOM's organic training facility, NSOU possesses the capacity to promptly and directly implement SOFCOM's requirements for A-SOF via a tailored curriculum. Additionally, SOFCOM can expedite the provision of financial, personnel, and infrastructure resources to facilitate efficient the training and education.

Thirdly, the research findings strongly validate the accuracy of H3, which posits that SOFCOM is uniquely qualified to promote interoperability with cyber and space domains, thus enhancing NATO's 360-degree approach. Since its establishment as a MOU in 2010, SOFCOM has consistently served as a pivotal strategic and operational command hub. It offers strategic advice, enables A-SOF development, and coordinates A-SOF activities. As a hybrid MOU/NFS organization with 13 years of operational experience and a proven track record in handling sensitive classifications and national caveats, SOFCOM possesses the established structures and characteristics necessary to advance NATO's transition from JO to MDO and a 360-degree approach. In that regard, Moon's assertion that A-SOF has functioned as an innovation engine for adapting to challenging scenarios since NATO's inception is entirely applicable to SOFCOM.¹⁷⁹ This underscores SOFCOM's unique role in addressing the RQ.

Fourthly, H4, which asserts that "Integrating specific liaison elements enhances Space, Cyber, and A-SOF interoperability capabilities," aligns with the results of the

¹⁷⁷ NATO Standardization Office, *Allied Joint Doctrine*, 118.

¹⁷⁸ NATO Special Operations Headquarters, *NATO Special Operations School Course Catalogue 2022–2023*, 4–5.

¹⁷⁹ Moon, *NATO Special Operations Forces in the Modern Security Environment*.

interview research. A strategic approach involving targeted interoperability elements at the operational command level, facilitated by SOFCOM's MDOC, Cyber's CyOC, and Space's SpCen, can significantly enhance synchronization among independent domain activities, foster cross-domain awareness, and pinpoint cross-domain support requirements in alignment with the principles of MDO and NATO's 360-degree approach. As emphasized by Lewis, an actor can most effectively realize the strategic value and success perspective of cyber and space domains when they complement kinetic elements.¹⁸⁰ Therefore, operational command elements such as SOFCOM must champion and promote the exchange of liaison between domains, as advocated in this thesis. The exchange of liaison elements among operational commands advances interoperability. It supports the complementary roles of cyber and space during strategic competition, the gray phases of evolving threats and crises, and particularly in the kinetic phases of warfare.

In addition to the key findings supporting the positively tested H1, H2, H3, and H4, the thesis derives three extended findings that result primarily from the SNA evaluation and complement H1, H2, H3, and H4.

The fifth overarching finding (F5) underscores the importance of "SOFCOM's active and committed role in developing enhanced interoperability with cyber and space domains." The research affirms that A-SOF, in conjunction with SOFCOM, possesses both structural and conceptual advantages that align with NATO's objective of advancing the Alliance towards MDO capability, leading to the modernization and improvement of allied LOAs. Structurally, SOFCOM, as a MOU organization distinct from the NFS, offers greater flexibility and adaptability, specifically suited for addressing the challenges posed by cyber and space interoperability and 360 degree-approach of NATO. Conceptually, A-SOF has operated within a sensitive environment for over a decade, demonstrating a deep understanding of classification issues and national caveats. To drive improved interoperability, SOFCOM must play a central role in fostering collaboration across A-SOF, cyber, and space disciplines, ensuring consistent communication of A-SOF's intent. In this effort, SOFCOM should realign and adapt its core mission to "enable A-SOF

¹⁸⁰ Lewis, *Cyber War and Ukraine*, 8.

development,” to be closely congruent with NATO’s MDO enhancement goal. The communication effort adopted by the U.S. ARSOF in their 2030 strategy for transforming ARSOF, particularly regarding cooperation with cyber and space within LOE #1, can serve as a progressive and exemplary model for enhancing communication and collaboration.¹⁸¹

The research has revealed the sixth finding F6: “OCO offer a promising avenue for achieving MDO-oriented interoperability with A-SOF.” OCOs within NATO are subject to stringent central control and national constraints. Presently, NATO can only indirectly generate offensive cyber effects within the cyberspace domain through SCEPVA process (refer to section III.A.3). Given the complexity and sensitivity of this level of operational activity within NATO, A-SOF presents a suitable partner for interoperability. A-SOF has a synchronization and communication platform through the SOFCOM operational command, which is an ideal conduit for synchronizing and facilitating sensitive and, at times, unilateral cooperation for A-SOF-cyber operations. This collaboration also paves the way for cross-domain support and aligns well with MDO-oriented developments. Offensive cyber effects represent a sensitive area for NATO and are therefore a challenge in dealing with NATO’s MDO ambitions. Despite these limitations, cyber with OCO must align with MDO requirements and enable synchronization interfaces to other disciplines. Interoperability between the cyber domain’s CyOC and A-SOF’s SOFCOM at the operational level would close this capability gap. SOFCOM is the only command in NATO structures that can interoperable address the challenges described by Goździewicz that arise from indirect offensive cyber activities with SCEPVA without compromising sensitivity.¹⁸²

From the research, the thesis derived the seventh finding F7 with: “A-SOF as a warfighting element, provides a suitable structure to facilitate interoperability efforts with the Space domain and thereby offer Space and its SpSC capabilities at operational level interoperability intersections with and to the A-SOF discipline.” Space is the youngest of the five domains and is similar in organization and structure to the cyber domain. Nations

¹⁸¹ U.S. Army Special Operations Command, *Army Special Operations Forces Strategy*, 12.

¹⁸² Goździewicz, “Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA).”

provide space capabilities to NATO and space activities are subject to classifications and national caveats. At the same time, both space and cyber must align with NATO's MDO intentions and seek avenues of interoperability as a core component and enabler for MDO development of the Allied LOA. The ACT invests in conceptual and, above all, technically supported further developments for NATO's MDO capability, such as the Agile Multi-Domain C2 Model NATO SAS 143 of the International Command and Control Institute. In addition to these efforts, Space still has the need to design practical and operational level interoperability and MDO capabilities. A-SOF's SOFCOM provides Space with an excellent construct and hub for operational interoperability. The research demonstrates, and experts confirm, that achieving interoperability of space capabilities can be accomplished through collaboration with SOFCOM to advance MDO developments.

In the research, the thesis has yielded the seventh finding F7: "A-SOF, as a warfighting element, offers an effective framework to enhance interoperability with the Space domain, thus enabling the integration of Space and its Special Space Capabilities (SpSC) at an operational level, intersecting with and complementing the A-SOF discipline." Space, the newest of the five domains, shares organizational and structural similarities with the cyber domain. Various nations contribute their space capabilities to NATO, with these activities being subject to classifications and national caveats. Moreover, both the space and cyber domains must align with NATO's MDO objectives, emphasizing the importance of interoperability as a central element and enabler for the development of the Allied LOA. ACT is committed to advancing NATO's MDO capabilities through both conceptual and technical support. For instance, initiatives like the Agile Multi-Domain Command and Control (MDCC) Model, NATO SAS 143, from the International Command and Control Institute (IC2I), exemplify this dedication.¹⁸³

Furthermore, the Space domain still requires practical solutions to achieve operational-level interoperability and MDO capabilities. A-SOF's SOFCOM offers an ideal foundation and central hub for achieving operational interoperability. The research,

¹⁸³ International Command and Control Institute (IC2I), "Agile Multi-Domain C2," 2.

confirms that cooperation with SOFCOM is instrumental in advancing MDO developments and achieving interoperability for space capabilities.

C. RECOMMENDATIONS

Three recommendations emerge from the analysis and evaluation of the thesis findings. These areas are suggested as potential pathways to further explore and address findings F1 to F7, ultimately responding to the RQ: ***“Given that there is a politically initiated adaptation process in NATO aiming at a 360-degree approach against hybrid threat scenarios and with a requirement of a direct dependency between Cyber, Space, and MDO capabilities, how can A-SOF contribute to this process and evolve better interoperability between A-SOF, Cyber, and Space?.”***

The initial component of the three proposed recommendations focuses on the research question from a broader standpoint. A-SOF requires a comprehensive strategy to consistently align the entire A-SOF community toward improved interoperability with cyber and space domains. Simultaneously, it necessitates proactive communication of its intentions openly and transparently to other disciplines. The second element within the framework of these recommendations centers on the role of the NSOU as the key supporting entity for the A-SOF strategy, aimed at enhancing interoperability with the cyber and space domains, and delineates its potential to fulfill this role effectively. Finally, the thesis presents a third recommendation, introducing a specific approach. This approach outlines how SOFCOM can proactively shape and advance operational-level interoperability. It can do so by deploying dedicated liaison elements, including cyber and space liaison elements. These elements are instrumental in implementing an exchange and interoperability culture, serving as a common ground for synchronizing, enabling, and developing. Emphasizing the crucial nature of closely coordinating all three components in terms of sequence and timing is essential, with each building upon the other (see Figure 46).

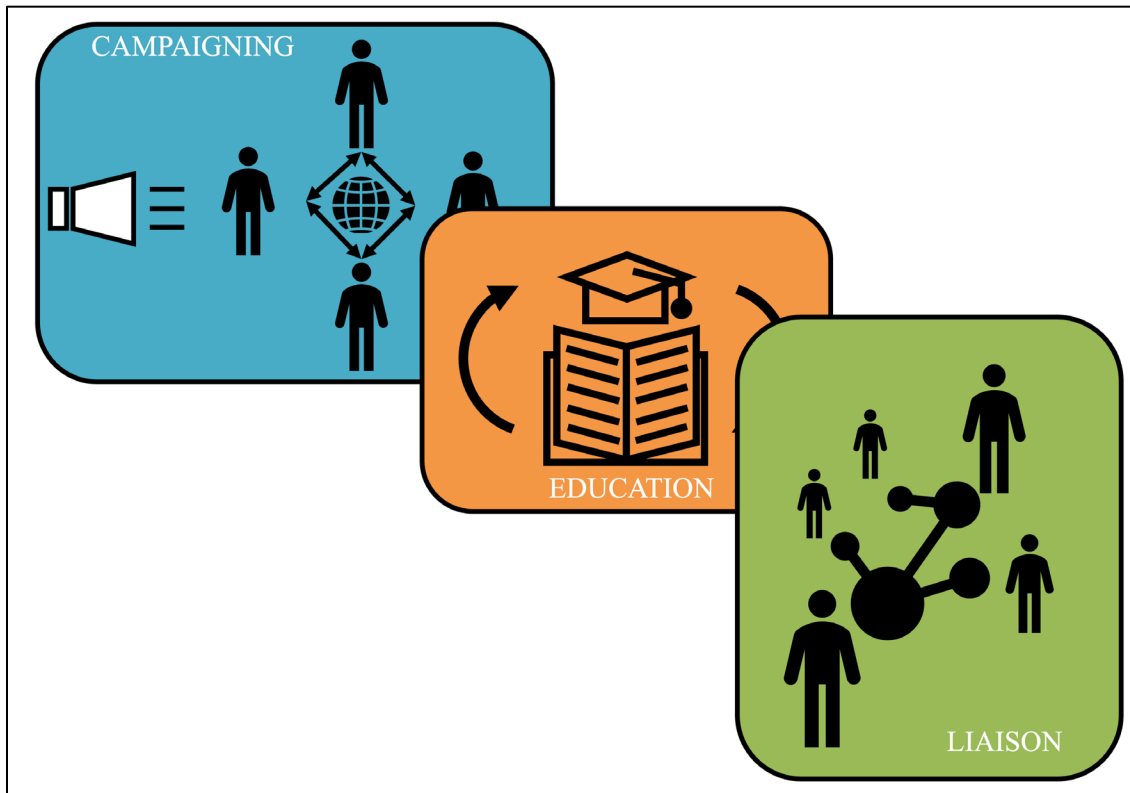


Figure 46. Three Main Recommendations to address the Research Question

1. A-SOF Strategy 2030 as a Communications Campaign

The Space-Cyber-SOF Triad describes an interdependent and mutually supporting relationship between cyberspace, space, and SOF. Special operations often rely upon the information advantage provided by cyberspace and space capabilities to see, sense, and stimulate to influence relevant populations or strike deep into the physical nodes of an adversary’s system and assess the results.

—LTG Braga, U.S. ARSOF Strategy 2030: Means/Capabilities and Resources, 2023¹⁸⁴

With the H4 findings highlighting that “SOFCOM is uniquely qualified to advance interoperability with cyber and space, enhancing NATO’s 360-degree approach,” SOFCOM serves a pivotal in addressing the research question (RQ). Implementing a consistent strategy “A-SOF Strategy 2030” underscores SOFCOM’s commitment.

¹⁸⁴ U.S. Army Special Operations Command, *Army Special Operations Forces Strategy*, 12.

SOFCOM should communicate the strategy transparently and proactively within the A-SOF community and across the new cyber and space domains. This approach by SOFCOM can reinforce by specific measures, substantiating its significant contribution. Moreover, by monitoring the process, SOFCOM will benefit itself and play a crucial role in advancing NATO's capabilities.

For example, the USASOC maintains consistent communication with the "US ARSOF Strategy 2030" paper, which outlines the strategic direction for United States Army Special Operations Forces (USARSOF) until 2030. Within this strategy, the leadership delineates strategic goals, the methodologies to achieve them, and the required resources.

Promoting interoperability with cyber and space assets plays a central role in ARSOF's pursuit of strategic objectives related to modernization, enhancement, and positioning. The strategy paper contributes to the thesis topic in two significant ways. Firstly, it serves as a guiding compass for the entire USARSOF community, providing a clear path for their actions. Secondly, it fosters external communication and creates a positive gravitational pull, strengthening connections between USARSOF, U.S. Army Cyber Command (ARCYBER), and U.S. Army Space and Missile Defense Command (USASMDC).¹⁸⁵ SOFCOM has the capabilities and the structure to develop a future strategy and utilize these two advantages in interoperability development with cyber and space.

a. A-SOF Strategy 2030

SOFCOM should adopt a parallel approach by strategically aligning itself with the NATO 2022 Strategic Concept and creating and releasing a strategy paper to yield the positive outcomes mentioned above and tie the A-SOF to NATO cyber and space domains. SOFCOM must initiate and consistently execute this process, considering the unique challenges posed by a multinational alliance with distinct structures, dependencies, and subordination relationships, which may differ from those of USASOC. Despite these

¹⁸⁵ U.S. Army Special Operations Command, *Army Special Operations Forces Strategy*.

differences, the shared objective remains the development of special forces in alignment with their respective strategies. Within this strategy document, SOFCOM should explicitly incorporate ‘Interoperability with Cyber and Space’ as a pivotal and integral element of A-SOF’s strategic trajectory, seamlessly integrating it into SOFCOM’s overarching intent.

Initially, by releasing a strategy paper, “A-SOF Strategy 2030,” SOFCOM should aim to communicate a unified message to all NATO Allies. This strategic document, aligned with SOFCOM’s mission, should offer a clear and compelling vision to the A-SOF community, catalyzing positive transformations in developing national SOF, cyber, and space capabilities within the framework of A-SOF. To underscore the significance of this concept, the thesis uses the history of SOFCOM as a prime example. McRaven’s “The Theory of SOF” played a pivotal role in the evolving understanding of SOF. Over time, this understanding was communicated consistently and transformed into the foundational comprehension of A-SOF and its categorization within NATO today.¹⁸⁶ This evolution ultimately led to the establishment of a strategic command, SOFCOM, which delineated tasks for A-SOF encompassing MA, DA, and SR.¹⁸⁷

This established the foundation for the shared core competence of A-SOF, a capability now acknowledged by all SOF units within NATO and considered crucial at the national level. Beyond these core competencies, the interoperability approach to cyber and space capabilities, which NATO considers essential requirements for MDO, must undergo a similar process of recognition and integration as MA, DA and SR. A cohesive strategy is essential to drive the necessary adaptation, both within NATO and at the national level. SOFCOM must include in the strategy itself aspects of consistent alignment of the A-SOF community and define pull factors for attracting the cyber and space disciplines. The goal for SOFCOM must be for the NATO community to affiliate SOFCOM with this strategy.

SOFCOM, in its leadership, structure, and organization, can develop a strategy for A-SOF, ensuring its accessibility to all Allied nations. This involves creating a sustained media presence on the subject, establishing, and maintaining liaisons with cyber and space

¹⁸⁶ McRaven, “The Theory of Special Operations,” 3.

¹⁸⁷ NATO Standardization Office, *Allied Joint Doctrine for Special Operations*, 7.

entities, and fostering a training strand through NSOU. The foundational elements of this strategy, including the SOFCOM mission, the LOO (Advise, Enable, Synchronize, Empower), the LOE (1a, 1b, ..., 4c), and the end state, can be derived from the existing NATO strategy. SOFCOM must adapt these pillars to align with Strategy 2022 and refine them to meet a restated end state. Crucially, the strategy should be available internally for the A-SOF community and transparently communicated to the broader community through various media channels. Figure 47 provides an outline and example of how SOFCOM can evolve the cornerstones of the strategy.

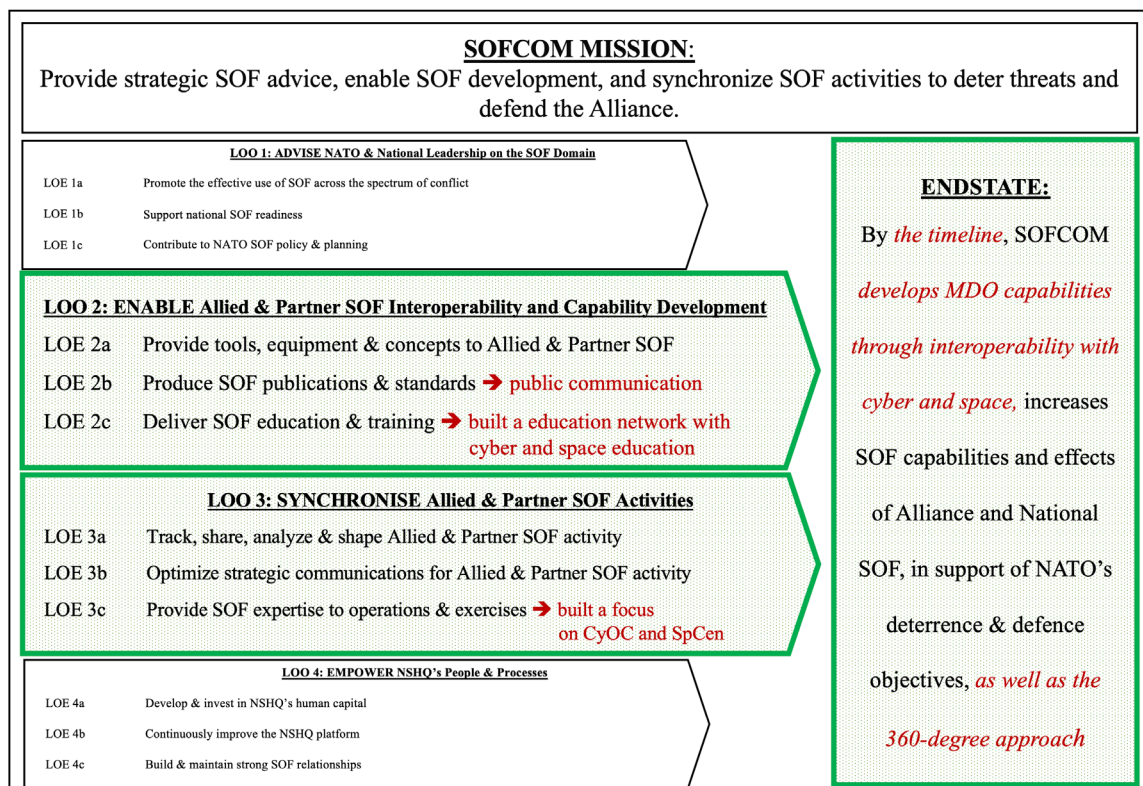


Figure 47. Consistent Communication Campaign derived from an “A-SOF Strategy 2030”¹⁸⁸

¹⁸⁸ Adapted from Allied Special Operations Forces Command, “NSHQ’s 2-Year Strategic Approach (2022-24),” 1.

The Warfare Development Directorate possesses the requisite authority and resources to develop the “A-SOF Strategy 2030,” publish it in the interest of SOFCOM, and oversee associated measures. Devoting significant energy and resources to this initiative is crucial for SOFCOM, as it establishes a structural framework for the interoperability process. Transparent strategic communication is integral to ensuring this process’s sustainable and effective commencement.

The next two sections outline two specific packages of measures as recommendations two and three. On the one hand, these measures are core components of the proposed A-SOF Strategy 2030. On the other hand, both provide practical interoperability measures in addition to the strategic cornerstones that the first section has set.

2. NSOU: Short and Long-Term Education Packages

My vision for NSOU is to remain the crossroads of NATO special operations forces (SOF) and a gathering place for the Alliance’s best and brightest to learn, share, and teach. NSOU is committed to leading the Alliance in SOF education and the development of the most important weapon NATO has—our minds.

—LTG Antonio Fletcher, Commander Allied-Special Operations Command,
Welcome to the 2023–2024 Academic Year 2023¹⁸⁹

To foster the evolution of interoperability with cyber and space, SOFCOM’s NSOU is integral. Acknowledging F1’s observation that “A-SOF lacks significant expertise in cyber and space domains, hindering the development of sustainable interoperability,” SOFCOM must develop a well-defined, coordinated, and targeted knowledge base within LOO 2’s “Enabling” axis (refer to Figure 47). NSOU has the competence and qualified means to generate very fast and short-term adaptation measures in the curriculum. At the same time, NSOU can evolve sustainable training programs, supported by providing resources (e.g., along defined authority requirements derived from a consistent strategy “A-SOF Strategy 2030”). This strategic foundation will pave the way for subsequent targeted development measures across the remaining LOO axes.

¹⁸⁹ Adapted from: Allied Special Operations Forces Command, “NSHQ’s 2-Year Strategic Approach (2022-24)” (Mons, Belgium: SOFCOM, 2022), 1.

Like SOFCOM, NSOU is an MOU organization with the USA as FN. This form of organization gives NSOU great flexibility and allows it to find solutions unbureaucratically and implement measures more quickly than NFS institutions. Simultaneously, the ACT accredits NSOU, ensuring high-quality training aligning with NATO standards as per the NATO Training Directive.¹⁹⁰ With these characteristics, NSOU is in a key position to evolve a form of training for A-SOF that plays an important complementary role to cyber and space-specific training. NSOU should not only focus its own A-SOF community on MDO development but also train cyber and space specialists in A-SOF cross-domain awareness and thus create a training network.

NSOU, subordinate to the Warfare Development Directorate, has the available resources to set up NSOU Research Center to a MDO Capability Group. This group must then evolve short-term as well as sustainable and long-term training packages through a TRA and TNA process with experts from cyber and space.¹⁹¹

a. Short-term curriculum adaptation

NSOU and the branches responsible for education and training play a crucial role in identifying gaps during course execution through immediate evaluation process using After Action Reports (AAR) and utilizing Post Course Reviews (PCR) as part of the NATO System Approach to Training (NATO SAT). Course Directors can then direct contractors to address these gaps promptly to improve the course quality.

Consider the Special Operations Component Command (SOCC) Planner course for a practical illustration. This training involves specialists teaching cross-domain or cross-discipline awareness blocks in various disciplines, a crucial aspect for planner trainees to understand and synchronize within the planning process. For example, utilizing AAR analysis, the SOCC Planner Course Director might identify a gap in cyber and space cross-domain awareness. Here, the Operational Studies Branch can elaborate with the course

¹⁹⁰ Supreme Allied Commander, Europe and Supreme Allied Commander, Transformation, *Bi-SC Education and Individual Training*.

¹⁹¹ Supreme Allied Commander, Europe and Supreme Allied Commander, Transformation, chaps. 5–9.

delivery contractor a feasible cyber and space awareness block, seamlessly integrating it into the course. Although this method has initial limitations, it allows for immediate implementation between identifying a gap in an AAR after completing a course and the next course iteration.

If the contractual framework with training providers contains persistent gaps, NSOU can devise a short-term solution within months. Additionally, should adaptation measures align with the defense budget, NSOU retains the flexibility to adjust course content within the annual quality management process, implementing an enhanced course the following year. Steering this process towards MDO development and the promotion of cyber and space interoperability is the focused role of the NSOU Research Center.

b. Long-term education program

In the long term, NSOU must academically map the evolutionary development of warfare from JO to MDO capability and provide an academic perspective for a sustainable A-SOF MDO transformation with cyber and space. The structure of NSOU establishes a robust foundation within the Operations Studies Branch for the holistic development of a Multi-Domain Operations Studies Branch. This initiative aims to advance interoperability with cyber and space academically. By doing so, NSOU could significantly enhance and fundamentally initiate an interoperability process, aligning with the insights derived from findings F1 and F2. The successful execution of this measure necessitates clear prioritization by the requirement authority, and SOFCOM must actively support it with essential resources, including budget, personnel, and infrastructure.

With backing from the NSOU Research Center and under the guidance of the Warfare Development Directorate, NSOU is committed to embracing a comprehensive global programming approach (see Figure 48). This approach is pivotal in discerning a long-term and sustainable curriculum and training plan tailored for A-SOF, cyber, and space personnel. In the NATO Global Programming method described above (Figure 48), the requirements authority (COM SOFCOM) can systematically define performance gaps through the Strategic Training Plan (STP) and the Training Requirements Analysis (TRA), synchronizing them with the cyber and space requirements authorities in SHAPE. In the subsequent process,

SMEs, utilizing the Training Needs Analysis (TNA) and the NATO SAT method, can actively define the Performance Objectives (PO). Following the establishment of PO, NSOU can assemble a sustainable training package and adjust its structure to align with the MDO transformation, demonstrating high adaptability and building up synergies with cyber and space.

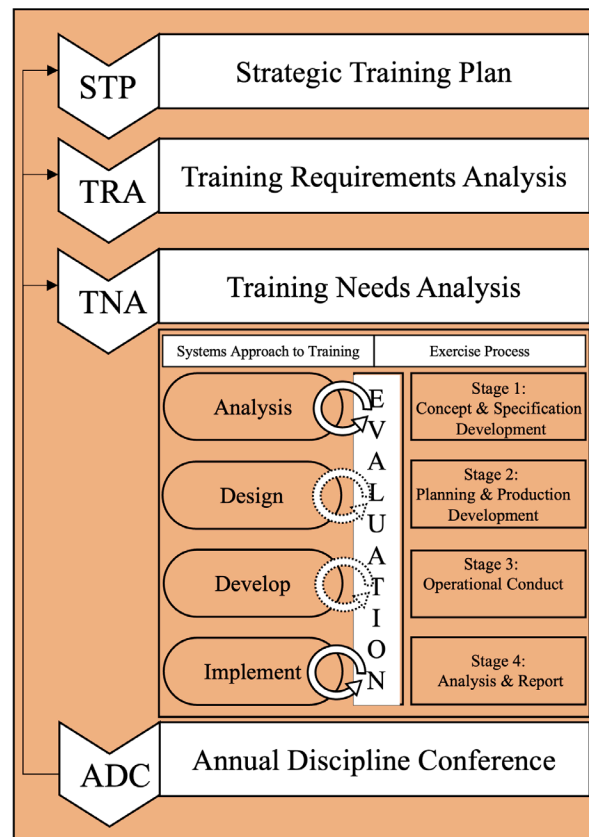


Figure 48. Global Programming – Development Methodology¹⁹²

NSOU and SOFCOM have the necessary structures and capabilities to support and advance the MDO transformation process in a focused manner and in the interest of the A-SOF mission to Advise, Enable, Synchronize, and Empower A-SOF. With the transformation of the current Operations Studies Branch to a Multi-Domain Operations

¹⁹² Adapted from Supreme Allied Commander, Europe and Supreme Allied Commander, Transformation, 25.

Studies Branch, NSOU would create an operational training demand for cyber and space in the A-SOF community. This demand would in turn attract training suppliers and civilian expertise providers to NSOU, who in turn would evolve innovative training contents in competition and thus also contribute to shaping the NATO MDO transformation.

3. Interoperability Elements

SOFCOM can evolve multi-level interconnectivity to link the operational levels of SOFCOM, Cyber Directorate, and AIRCOM in the manner of MDO transformation and NATO's 360-degree approach. In the interest of LOO 3 "Synchronization, Monitoring and Sharing," SOFCOM could share A-SOF and cyber activities and synchronize space support in a cross-domain liaison approach. This liaison approach unfolds in three stages.

Initially in the first stage, SOFCOM should promptly assign small liaison elements to the CyOC in the Cyber Directorate and the SpCen in AIRCOM at a working level to immediately generate situational and cross-domain awareness. This approach directly facilitates tangible learning experiences between A-SOF and the Cyber and Space domains. Beyond the previously noted effects, the liaison elements would yield valuable insights that NSOU could incorporate into the NATO SAT process, thereby contributing to targeted training development. Moreover, viewed through the lens of the A-SOF Strategy 2030, these elements would signal cooperation to the cyber and space domains, making interoperability more practical and appealing.

In the second, more advanced phase, the operational command elements of SOFCOM, the Cyber Directorate, and AIRCOM, as mentioned in the preceding section, would exchange specialized and specifically trained interoperability elements. SOFCOM and the other two operational command levels are to undertake this evolutionary step only after developing and implementing a cross-domain training framework at NSOU. The liaison elements, equipped with PR, can mutually support and benefit from each other across the LOO spectrum (Advise, Enable, Synchronize, and Empower). These liaison elements with PR would then simultaneously flow into the national SOF, cyber, and space structures and strengthen the alliance in the manner of LOO 4 "Empower" and promote additional knowledge exchange.

In the final long-term stage, planning elements like the Special Operations Space and Cyber Integration Cell (SOSCIC) in all planning departments of all operational Commands can expand the planning efforts of the respective commands in the cross-domain. SOFCOM, as the A-SOF Requirement Authority can only generate planning, liaison, and advisory elements to improve the interoperability of A-SOF, Cyber, and Space if it lays the foundations with a consistent strategy and a targeted cross-domain training platform in NSOU.

The three sections of the recommendations illustrated three coordinated options for action, all of which incorporated aspects of the key findings F1 – F7 and showed one way in which the thesis could answer the RQ *“Given that there is a politically initiated adaptation process in NATO aiming at a 360-degree approach against hybrid threat scenarios and with a requirement of a direct dependency between Cyber, Space, and MDO capabilities, how can A-SOF contribute to this process and evolve better interoperability between A-SOF, Cyber, and Space?”* The thesis recommends that SOFCOM evolve a consistent strategy that directs the A-SOF community in the interoperability transformation direction. Under this strategy umbrella, the thesis proposes to evolve a cross-domain training framework with and through NSOU to develop the technical substance and PR necessary for targeted interoperability. Accompanying the training framework, the thesis proposes to implement interoperability elements in a multi-stage approach for practical implementation at the operational command level.

D. WAY AHEAD

My team and I try to review SOF-specific literature, papers, articles, projects, and theses to capture essences and ideas, but we can’t keep up. If anyone has ideas on how to make it faster and more effective, I’m all ears.

—LTG Braga, Naval Postgraduate School, 26 Oct. 2023¹⁹³

The thesis yielded a wealth of intriguing findings within a robust subject area, unveiling numerous research opportunities. Looking ahead, it aims to accentuate a

¹⁹³ Jonathan P. Braga, “Command and Leadership” (lecture, Naval Postgraduate School, Monterey, CA, October 26, 2023).

particularly promising facet of the analytical framework employed, underscoring its potential. Utilizing Social Network Analysis (SNA), the thesis effectively scrutinized both the qualitative and quantitative data extracted from the interviews. Leveraging a community detection algorithm and semantic centrality measurements, it visually and quantitatively mapped semantic relationships. Remarkably, this method unequivocally validated the hypotheses tested in both BDA and SDDA.

In the contemporary landscape, decision-makers grapple with the formidable task of sifting through vast amounts of data prior to formulating decisions or undergoing cognitive processes. The thesis advocates for the SNA approach as a viable method for conducting comparative analysis and systematically dissecting extensive semantic data to extract core themes and cognitive patterns. This methodology stands to aid decision-makers in semantically navigating extensive literature, identifying pivotal topics, and ultimately fostering more informed decision-making.

To illustrate how senior leadership might leverage SNA in the future, the thesis examines the application within SOFCOM through the envisioned strategy “A-SOF Strategy 2030.” Following the publication of this strategy, SOFCOM can harness SNA to scrutinize its strategic communications across various mediums like articles, directives, and theses, and within the targeted cyber and space community. This analysis aims to determine whether SOFCOM achieves the desired impact or if it needs further corrective measures. By employing SNA, a quantitative and semantic comparison of internal communications can ascertain their potential effectiveness. This methodology provides a means to gauge the impact of communication strategies. Demonstrated as an additional tool for analyzing semantic datasets, it merits consideration for its potential as a component in the leadership process.

APPENDIX A. LIST OF INTERVIEW QUESTIONS AND STATEMENTS

Hypotheses H1, H2, H3, H4 and open-ended questions

1. H1: A-SOF lacks significant expertise in cyber and space domains, hindering the development of sustainable interoperability.
2. H2: SOFCOM's integral training facility, NSOU, holds significant importance in cultivating fundamental and supplementary knowledge for achieving interoperability with Cyber and Space.
3. H3: SOFCOM is uniquely qualified to advance interoperability with cyber and space to enhance NATO's 360-degree approach.
4. H4: Integrating specific liaison elements enhances Space, Cyber, and A-SOF interoperability capabilities
5. How Cyber and Space as military domains can be considered? What is special unique, and what is different from other domains?
6. How can SOF be considered a functional domain/warfighting element, and which role does it have while considering Cyber and Space?
7. How relevant is the role of A-SOF regarding the 360-degree approach of NATO?

Doctrinal definitions and MDO considerations

8. A comprehensive and systemic understanding of the IE (Information Environment) is required to identify opportunities and risks resulting from A-SOF actions effectively.
9. What structural adaptation steps do you see for the SOFCOM, Cyber, as a competence component of the IE, and space as a multiple enabler, being able to consider IE for A-SOF activities holistically?
10. How is structural/organizational interoperability for SOFCOM to include the component Space and Cyber needed?
11. Are there other A-SOF entities besides SOFCOM within the NFS that could also develop and drive the Cyber, Space, and A-SOF fusion?
12. From an organization perspective, which relevance has a command such as SOFCOM when there is a discourse about interoperability with Cyber, Space is so enhanced?
13. What is the role of SOFCOM as the main driver for integrating Cyber and Space in the A-SOF structure?
14. How important are cyber and space capabilities in SOFCOM in enabling A-SOF to coordinate, synchronize, and establish education for knowledge sharing and awareness between the domains?
15. The SOFCOM is organized through different directorates. Cyber and Space offer cross-domain capabilities and could enable and enhance SOFCOM in other areas. Consider the different directorates of SOFCOM and assign cyber capabilities to each that would strengthen the areas and which capabilities should be provided.

Education and Training

16. Facilities such as CCDCOE, NSO, NDC NCIA, and SpCOE are NATO infrastructures that provide allies and partners with a wide variety of training to develop cyber and space capabilities.
17. Could NSOU take on a complementary role, first to specifically augment capability development for the Cyber, Space, and A-SOF triad, and second to achieve cooperation at the education level?
18. Would such an alignment be purposeful and support the MDO and Interoperability efforts?
19. Due to the abstract nature of Cyber and Space, A-SOF lacks a fundamental understanding at the operational and highest tactical levels.
20. Would be the use of SOFCOM training facility NSOU appropriate/advantageous, first, to fill this lack of understanding at the operational-strategic levels by integrating SOF-specific cyber and space topics into the curriculum and, second, to support the interoperability of the three domains?
21. How can understanding Cyber and Space be improved?
22. How important is mapping cyber and space-specific topics in NSOU's curriculum?
23. How could NSOU develop and integrate Cyber and Space into its curriculum? How long does it usually take to define a need or a gap to develop and incorporate a new educational topic to close it?
24. Which advantages or disadvantages do you see if A-SOF develops its organic capabilities and provides its training in NSOU?
25. Which boundaries exist regarding enhancing Cyber and Space capabilities in SOFCOM?

Scenarios

A-SOF and Space enable and support OCO to enhance cyber effects:

An offensive cyber effect could be expected to occur due to SCEPVA. However, conditionally, there is physical support by SOF and support through the Space required (Space capabilities, Space products, Space Services) to guarantee and maximize the intended Cyber effect.

26. For such a scenario, would it be beneficial to have space and A-SOF elements in the CyOC that could specifically assess the requirement and understand the language of cyber and enable cross-domain synchronization and coordination?
27. Is such a scenario realistic?
28. Is such a scenario appropriate?
29. Is such a scenario feasible?
30. Is that a pragmatic step toward MDO?

A-SOF is enabled and supported by OCO and Space capabilities:

An offensive cyber effect could be expected to occur due to SCEPVA. However, it can be determined that the generated effect provides A-SOF as a warfighting element with a window of opportunity, and space could support and enable both in all phases with space products and space Services.

31. For such a scenario, would it be beneficial to have space and A-SOF elements in the CyOC that could specifically assess the upcoming cyber effect, detect and evaluate a window of opportunity, and enable cross-domain synchronization and coordination?
32. Is such a scenario realistic?
33. Is such a scenario appropriate?
34. Is such a scenario feasible?
35. Is that a pragmatic step toward MDO?

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. QUESTION-RESPONDENT MATRIX FROM 1 – 300¹⁹⁴

Sort Key	New Label	New Question	Original Question	Respondent	Response
1	1H1R1	1	H1	1	what I saw from the exercises at least, communication is one basic human communication is one key words, how they communicate with each other. Second, key word perhaps is capability awareness. What capabilities discipline can offer so that the soft side can use this information in their planning? I think this is very important. Third keyword perhaps is, well, this relates to technology but sorry, the capability but technology as well. What technology we have in the cyber side. That's a soft can, for example, use or integrate into their practices. So technology, communication, basic communication, maybe methods of communication, how we communicate? And also capability awareness. All three domains are very different in nature / capability and disciplines awareness / Cyber and Space are very technical driven / The effects and capabilities of Cyber and Space are invisible and difficult to understand, the effects and capabilities of SOF are kinetic.
2	1H1R2	1	H1	2	How SOF operates is mysterious and often highly classified / Space and Cyber are new Domains with very specific requirements / Cyber is a artificial Domain and Space and Cyber are both transnational domains / fast evolving domains / there is a lack of understanding how to utilize the domains and how to utilize the capabilities Yes. Basically, I think that the other components still don't know exactly how, you know, it's best to use the cyber capabilities. And probably this is not the only sub question but more wider problem. Maybe in some ways, maybe your mechanic in some ways.
3	1H1R3	1	H1	3	SOFCOM recognizes the critical need for a comprehensive understanding of cyber and space domains at the operational and highest tactical levels. To address this, we are actively considering integrating SOF-specific cyber and space topics into the curriculum of our training facility, the NSOU. This initiative aims to fill the existing gaps in understanding and promote interoperability among the triad of cyber, space, and Allied-SOF. By advancing the fusion of these domains through education, we can strengthen our capabilities and better meet the challenges of modern military campaigning.
4	1H1R4	1	H1	4	The appropriateness and sufficiency of the NSOU (SOFCOM and the School) facilities for education in cyber and space domains depend on various factors. The NSOU can integrate SOF-specific cyber topics inside the core curriculum, such as SOCC Planning and JOC/AOC. While specific cyber/ space courses are not inside the current course catalogue, it is a topic of interest for the NSOU Research Centre (NRC).
...	...	...	...	...	...
300	15E2R20	15	E2	20	Such kind of scenario seems very risky. Cyber effects can be planned and prepared, but if (out of a sudden) a system gets updated or disconnected, they cannot be delivered. If SOF already deployed and on the way to the area of operations but the cyber effect fails, they are at a high risk. I cannot imagine how to calculate such kind of risk and how to plan/conduct a joint operation with such uncertainty. There is a need to coordinate cyber effects with kinetic effects (we have seen this during the Ukraine war. It makes no sense to destroy communication infrastructure (5G) if you need it for your own C2). This might be an area where NATO has a capability cap regarding planning, supporting and executing SOF operations supported by cyberspace.

¹⁹⁴ Kaisler, "Semantic Network of Subject Matter Expertise."

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Allied Special Operations Forces Command. “Allied Special Operations Forces Command (SOFCOM).” Mons, Belgium: Allied Special Operations Forces Command, August 23, 2023.
- . “NATO Special Operations University: The Crossroads of NATO SOF.” NATO Special Operations University, 2023. <https://www.nshq.nato.int/nsou>.
- . “NSHQ’s 2-Year Strategic Approach (2022-24).” Mons, Belgium: SOFCOM, 2022.
- Bastian, Mathieu, Sebastien Heymann, and Mathieu Jacomy. “Gephi: An Open Source Software for Exploring and Manipulating Networks.” *Proceedings of the International AAAI Conference on Web and Social Media* 3, no. 1 (2009): 361–62. <https://doi.org/10.1609/icwsm.v3i1.13937>.
- Beaurpere, Will and Ned Marsh. “Space, Cyber, and Special Operations: An Influence Triad for Global Campaigning.” Modern War Institute, June 9, 2022. <https://mwi.usma.edu/space-cyber-and-special-operations-an-influence-triad-for-global-campaigning/>.
- Bertino, Elisa, and Sorin Adam Matei, eds. *Roles, Trust, and Reputation in Social Media Knowledge Markets: Theory and Methods*. Cham, Switzerland: Springer, 2015. <https://link.springer.com/book/10.1007/978-3-319-05467-4>.
- Blessing, Jason, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, and Rakel Tideman. “New Decade, New Challenges, and New Opportunities: The Way Ahead to NATO 2030.” In *NATO 2030: Towards a New Strategic Concept and Beyond*, edited by Jason Blessing, Katherine Kjellström Elgin, and Nele Marianne Ewers-Peters, 1–22. Washington, DC: Johns Hopkins University, 2021. <https://sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>.
- Bornemann, J. “Final Decision on MC 0437/2 Special Operations Policy.” Brussels: North Atlantic Military Committee, 2011.
- Boschetti, Nicolò, Nathaniel Gordon, and Gregory Falco. “Space Cybersecurity Lessons Learned from the Viasat Cyberattack.” In *AIAA Ascend 2022*. Las Vegas, NV: American Institute of Aeronautics and Astronautics, Inc., 2022. <https://doi.org/10.2514/6.2022-4380>.
- Brown, Gerald G., Robert F. Dell, Heath Holtz, and Alexandra M. Newman. “How U.S. Air Force Space Command Optimizes Long-Term Investment in Space Systems.” *Interfaces* 33, no. 4 (2003): 1–14. <https://doi.org/10.1287/inte.33.4.1.16369>.

- Cooperative Cyber Defence Centre of Excellence. “About Us.” Accessed February 26, 2023. <https://ccdcoe.org/about-us/>.
- Cunningham, Daniel, Sean Everton, and Philip Murphy. *Understanding Dark Networks, A Strategic Framework for the Use of Social Network Analysis*. Lanham, MD: Rowman & Littlefield, 2016.
- Department of Defence. *North Atlantic Treaty Organization (NATO) Special Operations Headquarters (NSHQ)*. DOD Directive 3801.02. Washington, DC: Department of Defense, 2019. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/380102p.pdf?ver=2019-05-28-134326-997>.
- Department of Defense. “Combatant Commands,” 2023. <https://www.defense.gov/About/Combatant-Commands/>.
- Drieger, Philipp. “Semantic Network Analysis as a Method for Visual Text Analytics.” *Procedia – Social and Behavioral Sciences* 79 (June 2013): 4–17. <https://doi.org/10.1016/j.sbspro.2013.05.053>.
- Duggan, Patrick Michael. “Strategic Development of Special Warfare in Cyberspace.” *Joint Force Quarterly: JFQ*, no. 79 (2015): 46–53.
- Emde, Matthias. “Open-Ended Questions in Web Surveys – Using Visual and Adaptive Questionnaire Design to Improve Narrative Responses.” PhD diss., Technical University Darmstadt, 2014. <http://tuprints.ulb.tu-darmstadt.de/id/eprint/4219>.
- Ertan, A., K. Floyd, P. Pernik, and T. Stevens, eds. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. Tallinn, Estonia: NATO CCDCOE Publications, 2020.
- European Space Policy Institute. “The War in Ukraine and the European Space Sector.” ESPI Briefs No. 57. Vienna, Austria: European Space Policy Institute, May 2022.
- Everton, Sean F. *Disrupting Dark Networks*. New York: Cambridge University Press, 2012.
- . “Social Network Analysis Network Topography.” Presented at the DA 4600: Disrupting Dark Networks, lecture, Monterey, CA, September 14, 2022.
- Gouré, Daniel. *A Competitive Strategy to Counter Russian Aggression against NATO*. Arlington, VA: Lexington Institute, 2018. <https://www.lexingtoninstitute.org/competitive-strategy-counter-russian-aggression-nato/>.
- Goździewicz, Wiesław. “Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA).” *Cyber Defense Magazine*, November 2019. <https://www.cyberdefensemagazine.com/sovereign-cyber/>.

- Gresham, John D. “Interview with Adm. William H. McRaven, USN, Commander, U.S. Special Operations Command.” Defense Media Network, June 29, 2012. <https://www.defensemedianetwork.com/stories/interview-adm-william-h-mcraven-usn-commander-u-s-special-operations-command/2/>.
- Heise, David R. *The Semantic Differential and Attitude Research*. Chicago: Institute of General Medical Sciences of NIH, 1970.
- Hoffman, Mark Anthony, Jean-Philippe Cointet, Philipp Soeren Brandt, Newton Key, and Peter Shawn Bearman. “The (Protestant) Bible, the (Printed) Sermon, and the Word(s): The Semantic Structure of the Conformist and Dissenting Bible, 1660–1780.” *Poetics* 68 (2018): 89–103. <https://doi.org/10.7916/d8-ktex-m672>.
- Hooren, Jonas van. “The Imperative Symbiotic Relationship between SOF and Cyber: How Dutch Special Operation Forces Can Support Cyber Operations.” Master’s thesis, Naval Postgraduate School, 2019. <http://hdl.handle.net/10945/64086>.
- International Command and Control Institute (IC2I). “Agile Multi-Domain C2.” In *23rd ICCRTS*. Pensacola, FL: International Command and Control Institute, 2018.
- Jasper, Scott. *Russian Cyber Operations: Coding the Boundaries of Conflict*. Washington, DC: Georgetown University Press, 2020.
- Jensen, Mikkel Storm. “Five Good Reasons for NATO’s Pragmatic Approach to Offensive Cyberspace Operations.” *Defence Studies* 22, no. 3 (2022): 464–88. <https://doi.org/10.1080/14702436.2022.2080661>.
- Johnson, Kaitlyn. “NATO in Space.” In *NATO 2030: Towards a New Strategic Concept and Beyond*, edited by Jason Blessing, Katherine Kjellström Elgin, and Nele Marianne Ewers-Peters, 235–59. Washington, DC: Johns Hopkins University, 2021. <https://sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>.
- Joint Chiefs of Staff. *Competition Continuum*. Joint Doctrine Note 1–19. Washington, DC: Joint Chiefs of Staff, 2019.
- . Joint Publication 1 Volume 1 Joint Warfighting. Washington, DC: Joint Chiefs of Staff.
- . *Space Operations*. Joint Publication 3-14. Washington, DC: Department of Defense, 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14Ch1.pdf.
- Lewis, James A. *The Role of Offensive Cyber Operations in NATO’s Collective Defence*. Tallinn Paper No. 8. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015. https://ccdcoe.org/uploads/2018/10/TP_08_2015_0.pdf.

- Lewis, James Andrew. *Cyber War and Ukraine*. Washington, DC: Center of Strategic and International Studies, 2022. <https://www.csis.org/analysis/cyber-war-and-ukraine>.
- Lilly, Bilyana, Kenneth Geers, Greg Rattray, and Robert Koch. “Business@War: The IT Companies Helping to Defend Ukraine.” In *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, 71–83. Tallinn, Estonia: CyCon, 2023. <https://doi.org/10.23919/CyCon58705.2023.10181980>.
- Maness, Ryan C., Benjamin M. Jensen, and Brandon Valeriano. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford, UK: Oxford University Press, 2018.
- McCoy, Kelly. “The Road to Multi-Domain Battle: An Origin Story.” Modern War Institute, October 27, 2017. <https://mwi.westpoint.edu/road-multi-domain-battle-origin-story/>.
- McRaven, William H. “The Theory of Special Operations.” Master’s thesis, Naval Postgraduate School, 1993. <https://hdl.handle.net/10945/14838>.
- Moon, Madeleine. *NATO Special Operations Forces in the Modern Security Environment*. Brussels: NATO Parliamentary Assembly, 2018. <https://www.nato-pa.int/document/2018-special-operations-forces-moon-report-169-dscfc-18-e-rev1-fin>.
- Moore, Daniel. *Offensive Cyber Operations: Understanding Intangible Warfare*. Oxford, UK: Oxford University Press, 2021.
- Moroney, Jennifer D. P., Stephanie Pezard, David E. Thaler, Gene Germanovich, Beth Grill, Bruce McClintock, Karen Schwindt, Mary Kate Adgie, Anika Binnendijk, and Kevin J. Connolly. *Overcoming Barriers to Working with Highly Capable Allies and Partners in the Air, Space, and Cyber Domains*. Santa Monica, CA: RAND Corporation, 2023. https://www.rand.org/pubs/research_reports/RR968-1.html.
- Mueller, Grace B., Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias. *Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures*, 2023. <https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war>.
- Nakasone, Paul M. “A Cyber Force for Persistent Operations.” *Joint Force Quarterly*, no. 92 (2019): 10–14.
- NATO. “Allied Command Transformation.” NATO What We do, May 4, 2023. https://www.nato.int/cps/en/natohq/topics_52092.htm.
- . *Brussels Summit Declaration*. Brussels: NATO Public Diplomacy, 2018.

- . “Foreign Ministers Take Decisions to Adapt NATO, Recognize Space as an Operational Domain.” NATO News, November 20, 2019. https://www.nato.int/cps/en/natohq/news_171028.htm.
- . Framework Mechanism for the Integration of Sovereign Cyber Effects Provided Voluntarily by Allies into Alliance Operations and Missions. MCM-0112–2018. Brussels: NATO, 2018.
- . “London Declaration Issued by NATO Heads of State and Government (2019).” NATO Official Texts, July 1, 2022. https://www.nato.int/cps/en/natohq/official_texts_171584.htm.
- . *NATO 2022 Strategic Concept*. Brussels: NATO, 2022. <https://www.nato.int/strategic-concept/#StrategicConcept>.
- . “NATO-Accredited Centres of Excellence, 2023 Catalogue.” Norfolk, Virginia, USA, Allied Command Transformation, 2023. https://www.act.nato.int/wp-content/uploads/2023/05/COE_CATALOG_DEC_2022_LR.pdf
- . “NATO Cyber Defence.” Brussels: NATO Public Diplomacy Division, April 2021. www.nato.int.
- . “NATO Response Force.” NATO What We do, July 27, 2022. https://www.nato.int/cps/en/natohq/topics_49755.htm.
- . “NATO’s Overarching Space Policy.” NATO Official Texts, January 17, 2022. https://www.nato.int/cps/en/natohq/official_texts_190862.htm.
- . “Riga Summit Declaration.” NATO Official Texts, July 6, 2022. https://www.nato.int/cps/en/natohq/official_texts_37920.htm.
- . “Warsaw Summit Communiqué.” NATO Official Texts, July 9, 2016. https://www.nato.int/cps/en/natohq/official_texts_133169.htm.
- NATO Communications and Information Agency. “NCI Agency.” Accessed August 16, 2023. <https://www.ncia.nato.int/what-we-do/nci-academy.html>.
- NATO Defense College. “NATO Defense College Mission,” January 1, 2022. <https://www.ndc.nato.int/about/organization.php?icode=23>.
- NATO HQ. “NATO Communications and Information Agency (NCI Agency).” NATO, April 4, 2022. https://www.nato.int/cps/en/natohq/topics_69332.htm.
- NATO HQ Allied Air Command. “We Coordinate NATO Space Matters.” NATO Space Centre, 2023. <https://ac.nato.int/missions/we-coordinate-nato-space-matters>.

- NATO Space Center of Excellence. “NATO Space Center of Excellence Home.” Accessed August 29, 2023. <https://www.space-coe.org>.
- NATO Space Centre of Excellence. “NATO Space Center of Excellence Organisation.” Accessed August 31, 2023. <https://www.space-coe.org/organisation>.
- NATO Special Operations Headquarters. *Comprehensive Defence Handbook—Vol I*. Edition A Version 1. Mons, Belgium: NATO Special Operations Headquarters, 2020. <https://www.nshq.nato.int/library>.
- . *NATO Special Operations School Course Catalogue 2022–2023*. Mons, Belgium: NATO Special Operations Headquarters, 2022.
- . *NATO Special Operations University Course Catalogue 2023–2024*. Mons, Belgium: NATO Special Operations Headquarters, 2023.
- NATO Standardization Office. *Allied Joint Doctrine*. Edition F Version 1. NATO Standard AJP-01. Brussels: NATO Standardization Office, 2022. <https://www.cimic-coe.org/resources/external-publications/ajp-01-edf-v1-f.pdf>.
- . *Allied Joint Doctrine for Air and Space Operations*. AJP 3.3. Brussels: NATO Standardization Office, 2016.
- . *Allied Joint Doctrine for Communication and Information Systems*. AJP-6. Brussels: NATO Standardization Office, 2017. https://www.coemed.org/files/stanags/01_AJP/AJP-6_EDA_V1_E_2525.pdf.
- . *Allied Joint Doctrine for Cyberspace Operations*. AJP-3.20. Brussels: NATO Standardization Office, 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.
- . *Allied Joint Doctrine for Electronic Warfare*. AJP 3.6. Brussels: NATO Standardization Office, 2020.
- . *Allied Joint Doctrine for Joint Targeting*. AJP-3.9. Brussels: NATO Standardization Office, 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1033306/AJP-3.9_EDB_V1_E.pdf.
- . *Allied Joint Doctrine for Special Operations*. NATO Standard AJP-3.5. Brussels: NATO Standardization Office, 2019.
- . *Allied Joint Doctrine for the Conduct of Operations*. NATO Standard AJP-3. Brussels: NATO Standardization Office, 2019.

- . *Task Verbs for Use in Planning and the Dissemination of Orders*. STANAG 2287 Lo (edition 1). Brussels: NATO Standardization Agency, 2006.
- Newman, M. E. J. “Modularity and Community Structure in Networks.” *Proceedings of the National Academy of Sciences* 103, no. 23 (2006): 8577–82. <https://doi.org/10.1073/pnas.0601602103>.
- North Atlantic Military Committee. *NATO Military Policy for Information Operations MC 0422/6*. Brussels: North Atlantic Military Committee, 2019.
- . *Policy on Space Support in NATO Operations*. MC 0670. Brussels: North Atlantic Military Committee, 2018.
- NSHQ. “Allied Special Operations Forces Command (SOFCOM)” Accessed August 23, 2023. <https://www.nshq.nato.int/>.
- NSHQ Public Affairs Office. “NATO Special Operations Senior Leaders Convene in Slovakia.” NATO Special Operations News, May 5, 2023. https://portal.nshq.nato.int/home/sofad_conf_role_of_sof_and_collective_defence.
- Reichardt, Jörg, and Stefan Bornholdt. “Statistical Mechanics of Community Detection.” *Physical Review E* 74, no. 1 (July 2006): 1–14. <https://doi.org/10.1103/PhysRevE.74.016110>.
- Remuss, Nina-Louisa. “NATO and Space: Why Is Space Relevant for NATO?” *ESPI Perspectives*, no. 40 (October 2010): 1–9.
- Reynolds, Jeffrey. “NATO Multi-Domain Operations: Adapting beyond Joint Doctrine.” *The Three Swords*, no. 38 (2022): 25–29.
- Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, UK: Cambridge University Press, 2017.
- SHAPE. *Allied Command Operations Forces Standards Volume X: Special Operations Forces*. Mons, Belgium: SHAPE, 2018.
- Stoltenberg, Jens. “Press Conference by NATO Secretary General Jens Stoltenberg Following the Meeting of the North Atlantic Council at the Level of Foreign Ministers.” NATO Press Conferences, November 20, 2019. http://www.nato.int/cps/fr/natohq/opinions_171022.htm.
- Sukhankin, Sergey. “Russian Special Operations Forces: Image Versus Substance.” *Eurasia Daily Monitor* 16, no. 43 (March 27, 2019): 1–4.

- Supreme Allied Commander, Europe and Supreme Allied Commander, Transformation. *Bi-SC Education and Individual Training*. Directive (E&ITD) 075–007. Mons, Belgium: Supreme Allied Commander, Europe and Supreme Allied Commander, Transformation, 2015.
- Tuinman, Joost Martijn, and Matthias Johann Schwarzbauer. “The Strategic Utility of SOF in Great Power Competition: A NATO Perspective.” Master’s thesis, Naval Postgraduate School, 2022. <https://hdl.handle.net/10945/71557>.
- UK Ministry of Defence. *Cyber Primer*. London: UK Ministry of Defence, 2022. <https://www.gov.uk/government/publications/cyber-primer>.
- United Nations Office for Outer Space Affairs. “2222 (XXI). Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies.” Committee on the Peaceful Uses of Outer Space – Meeting Schedule for 2023, June 31, 2023. <https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html>.
- U.S. Army Special Operations Command. *Army Special Operations Forces Strategy*. Fort Bragg, NC: U.S. Army Special Operations Command, 2023. https://www.soc.mil/temp-pages/strategy/ARSOF_STRATEGY_2030.pdf.
- U.S. Cyber Command. *Achieve and Maintain Cyberspace Superiority*. Fort George G. Meade, MD: U.S. Cyber Command, 2018. <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf>.
- U.S. Space Force. *Operations: Doctrine for Space Forces*. Space Doctrine Note. Washington, DC: Headquarters, United States Space Force, 2022. <https://media.defense.gov/2022/Feb/02/2002931717/-1/-1/0/SDN%20OPERATIONS%2025%20JANUARY%202022.PDF>.
- Wasserman, Stanley, and Katherine Faust. *Social Network Analysis: Methods and Applications*. New York: Cambridge University Press, 1994.
- Wendt, Eric P. “Comprehensive Defense, a Whole-of-Society Approach via Irregular Forces.” *Special Warfare* 34, no. 2 (June 2021): 2–13.

INITIAL DISTRIBUTION LIST

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



DUDLEY KNOX LIBRARY

NAVAL POSTGRADUATE SCHOOL

WWW.NPS.EDU

WHERE SCIENCE MEETS THE ART OF WARFARE