A Discourse in Conflict:

Resolving the Definitional Uncertainty of Cyber War

A thesis presented in partial fulfilment for the requirements for the degree of

Master of Arts

in

Defence and Security Studies

at Massey University, Albany, New Zealand

Dan Hughes

2017

Abstract

Since emerging in academic literature in the 1990s, definitions of 'cyber war' and cyber warfare' have been notably inconsistent. There has been no research that examines these inconsistencies and whether they can be resolved. Using the methodology of discourse analysis, this thesis addresses this research need.

Analysis has identified that the study of cyber war and cyber warfare is inherently inter-disciplinary. The most prominent academic disciplines contributing definitions are Strategic Studies, Security Studies, Information and Communications Technology, Law, and Military Studies. Despite the apparent definitional uncertainty, most researchers do not offer formal definitions of cyber war or cyber warfare. Moreover, there is little evidentiary basis in literature to distinguish between cyber war and cyber warfare.

Proximate analysis of definitions of cyber war and cyber warfare suggests a high level of inconsistency between dozens of definitions. However, through deeper analysis of both the relationships between definitions and their underlying structure, this thesis demonstrates that (a) the relationships between definitions can be represented hierarchically, through a *discourse hierarchy of definitions*; and (b) all definitions share a common underlying structure, accessible through the application of a *structural definition model*. Crucially, analysis of definitions via these constructs allows a *foundational definition of cyber war and cyber warfare* to be identified. Concomitantly, use of the model identifies the areas of greatest inter-definitional inconsistency and the implications thereof and contributes to the construction of a *taxonomy of definitions* of cyber war and cyber warfare. Considered holistically, these research outputs allow for significant resolution of the inconsistency between definitions. Moreover, these outputs provide a basis for the emergence of dominant functional definitions that may aid in the development of policy, strategy, and doctrine.

The research conducted in this thesis contributed to the following publications:

Hughes, D., & Colarik, A. M. (2016). Predicting the Proliferation of Cyber Weapons into Small States. *In Joint Forces Quarterly 83, Fourth Quarter 2016* (pp. 19-26). NDU Press.

Hughes, D., & Colarik, A. (2016). Small State Acquisition of Offensive Cyberwarfare Capabilities: Towards Building an Analytical Framework. *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).* Vol. 9650 (pp. 166 - 179).

Hughes, D. (In Press). Archer's Stakes in Cyberspace: Methods to Analyze Force Advantage. In Prunckun, H. (Ed.) *Cyber Weaponry: Issues and Implications of Digital Arms*. Springer

Hughes, D., & Colarik, A. (In Press). A Hierarchy of Cyber War Definitions. *In Proceedings of Pacific-Asia Workshop on Intelligence and Security Informatics*. May 24, South Korea.

Acknowledgements

The author wishes to acknowledge:

His parents, Peter and Bridget, for their unconditional enthusiasm and support;

His supervisor and mentor, Dr Andrew Colarik, for his knowledge, guidance and encouragement;

And most importantly Emma, for her patience, grace and affection.

Contents

Abstract II
Acknowledgements IV
Contents V
List of Tables VII
List of Figures VIII
List of Acronyms IX
Introduction 1
Problem Analysis 3
Methodological Design 4
The Discourse of Definitions 4
A Hierarchy of Definitions 5
Definitional Components 5
Structural Definitions – Applications and Future Research 6
Chapter One: Problem Analysis 7
Purpose 7
The Emergence and Growth of Definitions 7
Clausewitz and Cyber War 8
International Law, Cyber War and Cyber Warfare 10
Military Operations in the Cyber Domain 13
Violence and Kinetic Effect as Thresholds of Cyber War and Cyber Warfare 14
The Implications of Definitional Uncertainty 16
Chapter Two: Methodological Design 19
Application of Methodology 21
Auditability and Dependability 24
Validity and Authenticity 25
Applicability 25
Chapter Three: The Discourse of Definitions 30
Usage of Terms: Cyber War and Cyber Warfare 30
Explicit versus Implicit Definitions 31
History of the Discourse 32
Disciplines within the Discourse 34
Influence of Disciplines on the Discourse 36
Chapter Four: A Hierarchy of Definitions 40
Analysis: Explicit Definitions 40

Analysis: Cross-Disciplinary Definitions 42
A Discourse Hierarchy of Definitions of Cyber War and Cyber Warfare 47
Chapter Five: Definitional Components 55
A Structural Definition Model 55
Relevance of the Structural Definition Model to the Sample 58
Definitional Spectrums 61
A Foundational Definition 80
Chapter Six: Structural Definitions – Applications and Future Research 83
Applications 87
A Discourse Taxonomy 87
Constructing Definitions 90
Reconciling the Discourse 93
Future Research and Applications 94
Conclusion 98
Bibliography 102
Appendix A: Source Article Analysis 106

List of Tables

TABLE 1. OCCURRENCE OF TERMS IN THE SAMPLE ARTICLES 30
TABLE 2. DEFINITIONS IN ARTICLES - EXPLICIT VS. IMPLICIT 32
TABLE 3. IMPLICIT/EXPLICIT DEFINITIONS BY DISCIPLINE 34
TABLE 4. AVERAGE IMPACT OF ARTICLES BY DISCIPLINE 36
TABLE 5. EXPLICIT DEFINITIONS (DUPLICATES REMOVED) 41
TABLE 6. TOP DEFINITIONS BY INFLUENCE (CITATION COUNT) 41
TABLE 7. BREAKDOWN OF CROSS DISCIPLINARY DEFINITIONS 42
TABLE 8. MOST INFLUENTIAL DEFINITIONS BY CITATION COUNT 47
TABLE 9. CORE DEFINITIONS OF CYBER WAR AND CYBER WARFARE 56
TABLE 10. STRUCTURAL DEFINITION MODEL – CORE DEFINITIONS 59
TABLE 11. NUMBER OF STRUCTURAL DEFINITION MODEL COMPONENTS IN DEFINITIONS 60
TABLE 12. PREVALENCE OF STRUCTURAL MODEL COMPONENTS IN DEFINITIONS 60
TABLE 13. ACTORS IDENTIFIED IN DEFINITIONS OF CYBER WAR AND CYBER WARFARE 64
TABLE 14. CYBER MEANS IDENTIFIED IN DEFINITIONS OF CYBER WAR AND CYBER WARFARE 66
TABLE 15. INTENT IDENTIFIED IN DEFINITIONS OF CYBER WAR AND CYBER WARFARE 67
TABLE 16. GROUPINGS OF INTENT IDENTIFIED IN DEFINITIONS 68
TABLE 17. EFFECTS IDENTIFIED IN DEFINITIONS OF CYBER WAR AND CYBER WARFARE 70
TABLE 18. TARGETS IDENTIFIED IN DEFINITIONS OF CYBER WAR AND CYBER WARFARE 72
TABLE 19. OBJECTIVES IDENTIFIED IN DEFINITIONS OF CYBER WAR AND CYBER WARFARE 75
TABLE 20. CYBER WAR AND CYBER WARFARE OBJECTIVES RELATED TO LEVELS OF WAR 76
TABLE 21. TARGET ACTORS IDENTIFIED IN DEFINITIONS OF CYBER WAR AND CYBER WARFARE 78
TABLE 22. POLITICAL ENDS IDENTIFIED IN DEFINITIONS OF CYBER WAR AND CYBER WARFARE 79
TABLE 23. SUMMARY OF ANALYSIS – DEFINITIONAL SPECTRUMS 80

List of Figures

FIGURE 1. IMPLICIT/EXPLICIT DEFINITIONS BY YEAR OF PUBLICATION 33
FIGURE 2. DISCOURSE HIERARCHY OF CYBER WAR AND CYBER WARFARE DEFINITIONS 49
FIGURE 3. STRUCTURAL DEFINITION MODEL FOR DEFINITIONS OF CYBER WAR AND CYBER WARFARE.. 57
FIGURE 4. ANALYSIS OF DEFINITIONAL SPECTRUMS 62
FIGURE 5. DEFINITIONAL SPECTRUM – 'ACTOR' 65
FIGURE 6. DEFINITIONAL SPECTRUM – 'INTENT' 69
FIGURE 7. DEFINITIONAL SPECTRUM –'EFFECTS' 70
FIGURE 8. DEFINITIONAL SPECTRUM – 'TARGETS' 73
FIGURE 9: DEFINITIONAL SPECTRUM – 'OBJECTIVE' 77
FIGURE 10. DEFINITIONAL SPECTRUM – 'TARGET ACTOR' 78
FIGURE 11. THE DISCOURSE OF CYBER WAR AND CYBER WARFARE DEFINITIONS 84
FIGURE 12. ILLUSTRATION OF THE FOUNDATIONAL DEFINITION OF CYBER WAR AND CYBER WARFARE 86
FIGURE 13. TAXONOMY OF CYBER WAR AND CYBER WARFARE DEFINITIONS – PART ONE 88
FIGURE 14. TAXONOMY OF CYBER WAR AND CYBER WARFARE DEFINITIONS – PART TWO 89
FIGURE 15. DEFINITION OF CYBER WAR AND CYBER WARFARE – EXCLUSIVE 91

List of Acronyms

CNA: Computer Network Attack

CND: Computer Network Defence

CNE: Computer Network Exploitation

CNO: Computer Network Operations

CO: Cyber Operations

DCO: Defensive Cyber Operations

DoD: (US) Department of Defense

ICT: Information and Communications Technology

OCO: Offensive Cyber Operations

UN: United Nations

USCYBERCOM: United States Cyber Command