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

List of Tables

List of Figures

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

Introduction

Cyberspace is a notional environment that comprises both the virtual, in the form of information, and the physical, in the form of infrastructure, hardware and the components that support it. It is a human-made domain: its existence relies on human-made objects. It also relies on the energies of the electromagnetic spectrum.

Over the past decades, cyberspace's rapid evolution and expansion have rendered it an integral component of modern society. It has facilitated immense increases in the range, reach and volume, and complexity of information available to human actors. Cyberspace enables mass communication, global supply chains, shared intelligence and access to the ideas of a diverse set of cultural norms and customs. Its persistent existence is now integral to everyday life, the functioning of modern states and international order. As a result, cyberspace has grown in strategic significance, with national and international implications that are only now being fully recognised.

The strategic value of cyberspace rests both in the infrastructure itself and in the information that is being globally stored, transmitted and shared. This massive infrastructure moves across state borders – sovereign areas of controlled space. It also traverses expanses that are open to all nations –international waters and orbital pathways and space itself. The data and information flowing through this infrastructure comprises many forms of communication that individuals, nation states, and sub and supra-state organizations rely upon to conduct the transactions underpinning twenty-first-century society. Any deliberate disruption of this infrastructure or the information it contains is likely to be harmful to states, citizens and international stability. Accordingly, governments across the world are expanding their security doctrines to include the defence – and in some cases the exploitation (US Department of Defense, 2015) – of cyberspace.

Traditionally, military doctrine considered land, sea and air as the operational domains of warfare. The advent of orbital and satellite technologies saw the addition of the operational

domain of space. Now, cyber warfare is increasingly being recognized as a new, fifth, domain of warfare. Its rising significance is illustrated by its prominence in national strategy, military doctrine and major investments in relevant capabilities. But what are the implications of this? What does it mean to wage war in cyberspace? How can a military secure cyberspace? What new weapons will need to be developed and deployed to do so?

Finding definitive answers to these questions is difficult, particularly as dominant, consistent definitions of the terms 'cyber war' and 'cyber warfare' have yet to be established. Indeed, since their emergence in academic literature in the 1990s, definitions of 'cyber war' and cyber warfare' have been divergent, inconsistent and sometimes ambiguous. A plethora of definitions exist, both within and across disciplines, yet most have exerted minimal influence. As a result, the academic discourse surrounding definitions of cyber war and cyber warfare could be seen as diffused, opaque and even contradictory.

Definitions do matter. They are a foundation of shared understanding, allowing for consistent articulations of problems and opportunities. Hence, they contribute to the type of concentrated and sustained analysis that enables comprehensive, reconcilable and synergistic research. In a nascent field of study, concerned with the explication and implications of the defence of newly emerged technologies, definitions become crucial. Definitions, however, are not fixed. Change is a constant in any discourse, and definitions should and will change in response to incisive analysis and empirical events. Nonetheless, researchers and practitioners within any domain of knowledge should understand the definitions that underlie their subject of enquiry. If, such as in the domain of cyber war and cyber warfare, definitions are multiple and mutable, then research is needed to identify inconsistent definitions, examine the differences between them, and articulate the implications for theoretical and practical applications. It is the purpose of this thesis to produce such research.

To address this need, this thesis seeks to fulfil as series of research objectives, each of which attempts to uncover or clarify an attribute of the definitions of cyber war and cyber warfare,

or the overall discourse surrounding these definitions. The research objectives of this thesis are to identify:

- The most commonly occurring characteristics of definitions of cyber war and cyber warfare;
- Which academic disciplines have contributed the greatest number of definitions;
- Whether the current body of literature provides the basis for clear distinction and separate definitions of cyber war and cyber warfare;
- Whether there are relevant historical patterns of how definitions have emerged over time;
- Which definitions of cyber war and cyber warfare have been most influential;
- The nature of the relationships between definitions;
- The key points of inconsistency between definitions; and
- Whether the inconsistencies between the definitions can be fully or partially resolved.

The information generated by meeting each research objective will then be used as a basis to construct foundational definitions of cyber war and cyber warfare, which both represent and reconcile the broader discourse. The resultant definition is intended to be unifying, but not absolute. It will have the structural integrity and explanative power to capture the essential characteristics of all the definitions to date, with the potential to provide a basis for future research. It will also have the flexibility to encompass and enfold the evolution of the discourse and the inevitable changes that will occur as our understanding of cyber war is challenged by new research and real world events.

Problem Analysis

This thesis comprises six chapters. The first chapter, 'Problem Analysis', contains the results of the author's initial, exploratory review of academic and military literature relevant to this study. The purpose of the literature review was to confirm the scope of the problem: inconsistencies between a plethora of definitions of cyber war and cyber warfare and an

absence of literature that attempted to articulate or resolve these definitional inconsistencies. Findings from the review included:

- The identification of several inconsistent definitions;
- A lack of delineation between definitions of ‘cyber war’ and ‘cyber warfare’; and
- Instances where researchers identified problematic analysis and discussion within the discourse which they attributed to inconsistencies between definitions of cyber war and cyber warfare

These conclusions provided sufficient evidentiary basis to justify continuance of the research.

Methodological Design

Chapter Two, ‘Methodological Design’, details the methodological design of the thesis: a discourse analysis-driven survey and comparative analysis of definitions of cyber war and cyber warfare encountered in pertinent academic and military articles. Included in the chapter is an articulation of the theory of discourse analysis and how it was applied to create a research framework. Furthermore, consideration is given to how the application of methodology within the research framework meets key criteria of research credibility. Chapter Two also details how this methodology was used to generate the research sample, as well as to structure the analysis performed on the sample. The result is a tailored methodological design, which enables analysis to be performed at three descending levels of abstraction: overall discourse, individual definitions and the structural components of the definitions.

The Discourse of Definitions

The analysis presented in Chapter Three, ‘The Discourse of Definitions, is focused on eliciting the characteristics of the discourse related to definitions of cyber war and cyber warfare. Using the quantitative information generated through the application of the methodological design, a number of discourse characteristics are presented and analysed. These include usage of the terms ‘cyber war’ and ‘cyber warfare’, the distinctions made between these terms, and

statistics on the number of articles that offer a distinct, explicit definition of cyber war or cyber warfare, as opposed to an implicit conception.

Chapter Three also analyses the history of definitions and considers the impact that major relevant cyber events may have had on the expansion of the discourse. Finally, Chapter Three maps the influence and interaction of different academic disciplines within the discourse, identifying those disciplines that contributed the highest number of definitions and those that contributed the most influential definitions, where influence was calculated according to academic citation count.

A Hierarchy of Definitions

Chapter Four, 'A Hierarchy of Definitions', shifts the analysis to the level of individual definitions of cyber war and cyber warfare. It includes further consideration of the academic disciplines that definitions had arisen from and their relative academic influence. Academic influence is also used to identify the individual definitions that have had the greatest influence within the discourse, and analysis is then presented to map the relationships between the individual definitions, with the ultimate goal of constructing a definitional hierarchy. Through this hierarchy, the author seeks to represent all the encountered definitions under a single model, which summarises the influence and interrelationships between definitions of cyber war and cyber warfare. This hierarchal model provides the foundation for the analysis conducted in Chapter Five.

Definitional Components

Taking as its starting point the hierarchal model constructed in Chapter Four, Chapter Five, 'Definitional Components', analyses the underlying structural components of definitions. These structural components then form the basis for the creation of a structural model of definitions of cyber war and cyber warfare. The explanative power of this model is tested by measuring its applicability to each definition encountered in the sample. The structural definition model is then used to conduct comparative analysis of each definitional component.

It is through this analysis that the foundational definition of cyber war and cyber warfare becomes apparent. Concomitantly, analysis of the structural components enables the identification of the key areas of divergence between definitions.

Structural Definitions – Applications and Future Research

Chapter Six, 'Structural Definitions – Applications and Future Research, summarises the results of the analysis that utilised the structural definition model. It presents the context, applications and implications of the foundational definition of cyber war and cyber warfare. This includes further explication of the purpose of the foundational definition and the spirit in which it is offered, in addition to consideration of areas where inconsistencies within the discourse remain unresolved. Immediate applications presented include the construction of a taxonomy of definitions of cyber war and cyber warfare, as well as the consideration of new methods to analyse, construct and reconcile definitions.

The implications of the research findings are then considered, including how they may influence the interpretation of empirical events that could qualify as cyber war or cyber warfare, as well as how research findings may relate to policy, doctrine and strategy. The thesis concludes by identifying future research that may build upon the findings of this thesis, and in turn how the findings of this thesis can contextualise and reconcile future relevant research within the domain.

Chapter One: Problem Analysis

Purpose

The purpose of this chapter is to capture the results of the author's initial engagement with literature relevant to definitions of cyber war and cyber warfare. In contrast to the methodological survey and comparative analysis of literature upon which the majority of this thesis is based, the author's initial review of the literature was exploratory. Its primary objective was to provide evidence to support the author's understanding of the research problem – inconsistency and divergence between a multitude of definitions of cyber war and cyber warfare.

By mapping the problem's parameters, the exploratory literature review also sought to identify the extent and impact of the research problem. Furthermore it sought to construct an empirical foundation on which to base the methodological design. In this sense it can be understood as analogous to the literature review present in many theses.

The Emergence and Growth of Definitions

The review's starting point was the first academic definition of the term cyber war, provided in Arquilla and Ronfeldt's 1993 paper, 'Cyberwar is Coming!'. Arquilla and Ronfeldt define cyber war as 'conducting, and preparing to conduct, military operations according to information-related principles.' This includes disrupting and destroying enemy information and communication systems and 'trying to know everything about an adversary while keeping the adversary from knowing much about oneself' (Arquilla & Ronfeldt, 1993).

Definitions of the term have since proliferated in response to technological advancements, and as the term propagated into academic and military literature. As of 2016, the terms cyber war and cyber warfare are used across academic disciplines and sub-disciplines including strategic studies (Arquilla & Ronfeldt, 1993; Farwell & Rohozinski, 2011; Rid, 2012), defence and security studies (Gartzke, 2013; Rid & McBurney, 2012), computer science (Bendrath, 2001;

Eom, Kim, Kim, & Chung, 2012), cultural and political studies (Fritz, 2008), military studies (Fink, Jordan, & Wells, 2014; Bonner, 2014), and international law (Schapp, 2009; O'Connell, 2012; Schmitt, 2013). Influential works were also produced by private organisations (Libicki, 2009; Lewis, 2002) as political briefings (Wilson, 2007) and as statements of strategic intent (US Department of Defense, 2011; 2015).

Despite their prevalence across disciplines, precise definitions of cyber war and cyber warfare remain elusive (Shakarian, Shakarian, & Reuf 2013; Theohary & Rollins, 2013). The term 'cyber war' is often used interchangeably with 'cyber warfare', yet if one allows for the traditional military distinction between war and warfare, the two are distinct. Under this distinction, 'war' is held to be the *act* of war while 'warfare' is the *means*; accordingly, cyber warfare can be understood as the *means* of cyber war, and cyber war the *act*. It is accepted, however, that this distinction may not be evidenced in the relevant body of literature. Indeed, consideration of what constitutes an act of cyber war, a means of cyber warfare, or whether the terms are indeed distinct, may be contested both within and across disciplines.

Clausewitz and Cyber War

Clausewitz conceptualises war as inherently violent, instrumental and political (Clausewitz, 1873). The idea that cyber war, by definition, should adhere to Clausewitz's principles of war is presented by Rid (2012) in his provocatively titled article 'Cyber War Will Not Take Place'. Applying Clausewitz's definitions to the cyber context, he argues that the world 'has never experienced an act of cyber war, which would have to be violent, instrumental, and – most importantly – politically attributed' (Rid, 2012). He further argues that all recorded acts of cyber-aggression labelled as cyber war (and likely future acts) are instead better understood as modern manifestations of the well-established categories of sabotage, espionage and subversion.

When explaining how his interpretation of Clausewitz pertains to cyber war, Rid states that violence must involve the potential for lethality, a threshold which few, if any, actual and

potential acts of cyber-aggression have met. He also emphasises that an act of war is always subservient to political purpose, and that such purpose 'has to be transmitted to the adversary at some point during the confrontation' (Rid, 2012). Such transmission is an admission of responsibility, thus an attribution of a cyber-attack to a particular party. Therefore, according to Rid, any anonymous attack cannot by definition, be an act of cyber war. As anonymity of attack has been a defining feature of recorded acts of cyber-aggression, this threshold significantly limits what can be considered an act of cyber war.

Rid's claims have implications for both the definition of cyber war and its utility as a concept. If one accepts his definitional thresholds of potential lethality and political attribution one can state that there has never been an act of cyber war. If one accepts his arguments regarding how military cyber-attacks are more appropriately understood as acts of sabotage, espionage or subversion, then one is also likely to agree with his assertion that cyber war is unlikely to occur. The study of a phenomenon that has never happened nor is likely to happen in the future is of dubious value; concomitantly, Rid's conception of cyber war belittles it as a concept of ongoing relevance.

Rid's work suggests that the application of Clausewitz's definition of war to cyber war demonstrates that, as a term, cyber war is highly problematic and of dubious analytical value. Useful counter-analysis is, however, provided in the work of Stone (2013). While not denying the value of Rid's analysis in demonstrating the instability of the term, he challenges Rid's deployment of Clausewitz, specifically with regard to the relation between force, violence and lethality, arguing that Rid conflates these terms. Specifically, Stone argues that while in warfare the application of force is linked to violence, there is no inexorable link between violence and lethality – an act of violence that achieves its military objectives does not fail to become an act of war due to the absence of lethality (Stone, 2013).

This argument is strengthened by Stone's reference to Western military strikes that focus on maximum degradation of military capability with minimum casualties. Stone expands on this to challenge Rid's assertion regarding the necessity of attribution for acts of war, pointing to

political goals that can be achieved 'via covert acts of force' (Stone, 2013), and suggests that an act can be both one of sabotage and of war – the categories are not mutually exclusive. Accepting Stone's objections to Rid, the definitional thresholds of cyber war are lowered and an understanding of the term that aligns with Clausewitz's theory of war regains its utility as an explanatory concept.

An alternative definition, but one still influenced by Clausewitz, is offered by Shakarian et al. (2013). They define cyber war as 'an extension of policy by actions taken in cyber space by state or non-state actors that either constitute a threat to a nation's security or are conducted in response to a perceived threat against a nation's security'. While retaining a focus on political instrumentality, this definition does not place the same emphasis on the use of violence and force to achieve political ends. This gives it additional flexibility to potentially encompass cyber activities undertaken for political ends that do not in themselves reach a threshold of violence, as the term is commonly understood. An example of this type of political, but non-violent attack is provided by the sustained and coordinated campaign of hacking, Distributed Denial of Service (DDoS), and Botnet attacks directed against Estonian telecommunication infrastructure in 2007, attacks generally thought, but not definitively proved, to be of Russian origin (Blank, 2008). A similar campaign of cyber attacks was launched at Georgia in 2008, both before and during a traditional, if limited, military conflict with the Russian Federation (Hollis, 2009; Korns & Kastenburg, 2009).

International Law, Cyber War and Cyber Warfare

Another emergent definition pertains to international law and how it may act to shape a conceptual definition of cyber war and cyber warfare. Arguably the most influential text in this area is The Tallinn Manual on The International Law Applicable to Cyber Warfare[1] (Schmitt, 2013). This was collaboratively authored by a group of international experts, at the invitation of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence. At

[1] An update to the Tallinn Manual was published in February 2017. Due to its recent publication, it has not been included in the sample of this thesis.

its core, the Tallinn Manual is an examination of the international law governing cyber warfare. 'It encompasses both the *jus ad bellum*[2], the international law governing the resort to force by States as an instrument of their national policy, and the *jus in bello*[3], the international law regulating the conduct of armed conflict' (Schmitt, 2013). It does not offer an explicit definition of cyber war or warfare, but instead uses the term cyber warfare in a 'purely descriptive, non-normative sense' recognising the 'normative ambiguity' (Schmitt, 2013) that surrounds the idea. By labelling cyber warfare as normatively ambiguous, the Tallinn Manual suggests that current definitions of cyber war and cyber warfare lack precision and it would be difficult for these terms to be used as a basis for legal regulation.

However, the analysis in the Tallinn Manual explicitly excludes some activities from the scope of cyber warfare. Specifically, the Tallinn Manual's analysis of cyber warfare does not include cyber activities that occur below the level of a 'use of force' (as understood in the *jus ad bellu*[4]) such as cyber criminality and cyber espionage. It does, however, include any cyber activities 'undertaken in the context of an armed conflict', in so far as it states that 'in a situation of on-going kinetic hostilities amounting to an armed conflict, the applicable law of international or non-international armed conflict will govern cyber operations taken in regard to that conflict' (Schmitt, 2013).

Accordingly, the Tallinn Manual establishes an implied definition, where cyber warfare is understood to be the activities within cyberspace that either cross the threshold of the 'use of force' (according to international law) or are taken in furtherance of an armed conflict. Such a definition may have normative insufficiencies, in so far as it may lack sufficient detail to account for the full spectrum of cyber activities to which norms could be applied to. However, it still has normative elements, involving a deliberate delimitation of the activities to which any emergent norms pertaining to cyber warfare may be applied to.

[2] Right to war.
[3] The law in waging war.

Further analysis of the application of international law to cyber war was carried out by Schaap (2009). His recognition of the multitude of definitions of the terms cyber war and cyber warfare led him to propose the use of an alternative term, 'cyber warfare operations', defined as 'the use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, of another state' (Schaap, 2009). While he states that cyber attacks are 'indisputably, a method of warfare', Schaap does not believe that all cyber warfare operations rise above the level of 'use of force'.

Instead, drawing upon analysis of the U.N. Charter, Schaap examines the implications and measures the actual or potential impact of different types of cyber warfare operations to judge on a case by case basis whether the threshold of 'use of force' has been reached. For example, he notes the consensus in the international community that DDoS attacks are unlikely to rise to the level of the 'use of force', while cyber attacks against civilian infrastructure with the potential for significant death and destruction will likely be considered to have reached this threshold, and may constitute an armed attack under Article 51 of the U.N. Charter.

He makes these observations noting that a binding definition of what constitutes 'use of force' has never been reached, lending the concept a substantive interpretive element. While this ambiguity does create a potential lack of consistency, as well as difficulties in enforcement, it does encompass an element of flexibility beneficial to interpreting new methods of force, such as military operations in cyberspace. An implication of Schaap's analysis is that cyber war or cyber warfare may be considered as a class of warfare for which violence is not a necessary attribute, a position in direct conflict with those offered by Clausewitz and Rid. Schaap's position suggests that one must either accept that violence is not a necessary component of warfare, or that, despite labels, cyber war or cyber warfare are not a class of warfare as traditionally understood.

Military Operations in the Cyber Domain

Schaap's use of the term 'cyber warfare operations' is indicative of another use of the terms cyber war and cyber warfare, where they are used to refer to a class of military operations within the operational or 'warfighting' domain of cyberspace. An operational domain is a location in which military operations occur, and the United States Department of Defense (DoD) identified cyberspace as the fifth military domain (the other domains are land, sea, air and space). Cyberspace has been accorded this status as it 'presents security challenges that are too novel and too serious for it to be treated as an add-on to […] traditional operations on land, at sea, or in the air' (USCYBERCOM, 2011). The notion of cyber war as military operations in the domain of cyberspace was advanced in the work of Libicki (2009), though he later challenged the utility of the concept (Libicki, 2012).

The status of cyberspace as an operational domain was formalised in 2011 by proclamation of the Secretary of Defense and in the DoD Strategy for Operating in Cyberspace (DoD, 2011). This classification remained consistent in the 2015 DoD Cyber Strategy; notably, neither the 2011 nor the 2015 version of the strategy make reference to the terms cyber war or cyber warfare. In the most recent iteration of the strategy, focus was instead placed on 'three primary missions in cyberspace'. These missions were (a) defence of the DoD's own 'networks, systems, and information' and a readiness 'to operate in an environment where access to cyberspace is contested'; (b) defence of 'the United States and its interests against cyberattacks of significant consequence'; and (c) the ability 'to provide integrated cyber capabilities to support military operations and contingency plans' (DoD, 2015).

While the DoD Cyber Strategy avoids specific use of the terms cyber war and cyber warfare, the actions it acknowledges as lying in its scope of interest are likely to be considered by many as exemplary acts of cyber warfare. For example, the strategy notes how 'the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military related networks or infrastructure' or to 'use cyber operations to terminate an ongoing conflict on U.S. terms'. Furthermore, the

strategy notes how U.S. Cyber Command (USCYBERCOM) may be used 'to deter or defeat strategic threats in other domains', and sets a specific strategic goal that focuses on the creation and maintenance of cyber options to 'control conflict escalation and to shape the conflict environment at all stages' (DoD, 2015).

Arguably the focus on operational and strategic outcomes and the absence of contested terms like 'cyber war' and 'cyber warfare' allows for greater specificity on how cyber military capabilities may be used to advance U.S. interests. Considering the degree of force required to achieve many of the outcomes discussed, however, the author considers it uncontroversial to accord the status of cyber war and cyber warfare to the more aggressive actions outlined in the DoD strategy.

Violence and Kinetic Effect as Thresholds of Cyber War and Cyber Warfare

Several divergent definitions of cyber war and cyber warfare have now been identified. These include Arquilla and Ronfeldt's historic definition, various definitions derived from or influenced by the views of Clausewitz, definitions arising from international law, and a definition representative of military operations in the cyber-domain. The existence of multiple divergent definitions and the inconsistencies between them, provide a foundation of evidence for consideration of the research problem.

Across and within these definitions, however, lies another complicating thread. This is an insistence by some researchers that cyber events must surpass a certain threshold of violence or kinetic effect to qualify as cyber war or cyber warfare. Whether a cyber event must be violent, or even potentially lethal, to qualify as cyber war or cyber warfare has already been explored in the discussion of the work of Rid (2012), Stone (2013) and Schaap (2009).

Further insight can be found in the work of Lewis (2013) who offers a Clausewitz-influenced definition, where cyber war is 'the use of cyber techniques to cause damage, destruction, or casualties for political effect by states or political groups' and a cyber attack 'is an individual act intended to cause damage, destruction, or casualties' (Lewis, 2013). Importantly, Lewis

maintains that attacks require violence and violence requires the use of force, but accepts that within cyberspace there are a number of ‘grey areas’ where it may be unclear if a particular event has risen to the level of use of force, and thus violence (Lewis, 2013).

An example is disruption of cyber services; minor hacktivism would not reach the threshold of use of force; however, disruption on a massive enough scale to approximate an economic blockade most likely would. Further examples are cyber manifestations of the accepted international practices of espionage and reconnaissance. These activities would not usually meet the threshold of use of force, but in the cyber domain these activities can be used to plant weapons and vulnerabilities, actions more likely to reach the threshold of use of force when considered from the perspective of more traditional domains. Lewis further observes that decisions on whether these types of grey activities cross the threshold of use of force will be political and made on a case by case basis. From a definitional perspective, this creates a situation where the threshold of cyber war is determined through the interpretation of an initiating or effected political actor.

Of similar relevance to definitions of cyber war and cyber warfare is the threshold of kinetic, or physical effect. This concerns whether a cyber activity must have an effect in the physical world to be considered as an act cyber war or means of cyber warfare. The works of Park and Duggan (2011) and McGraw (2013) both present the position that cyber war must have a kinetic effect – ‘a consequential impact in the real world’ (McGraw, 2013).

Determining exactly what constitutes a kinetic effect, however, falls subject to the same ambiguities that inflict the determination of whether a cyber act meets a certain threshold of violence. For example, Parks and Duggan argue that effects that influence ‘the minds of decision-makers in the physical world’ should be considered kinetic. This approach is problematic in that it leaves very little that cannot be considered kinetic. Other examples, such as Park and Duggan’s description of physically destructive attacks on infrastructure, or McGraw’s description of using a cyber attack to control an adversary’s drones and

commanding them to attack the wrong targets, provide less ambiguous examples of what could be considered a kinetic effect.

An example that further demonstrates the ambiguity of kinetic thresholds is Operation Orchard, the successful Israeli bombing of a suspected Syrian nuclear facility in 2007. During this airborne attack 'Syria's formidable air-defense system could not track inbound Israeli aircraft because it was taken over by Israeli cyber warriors who incapacitated or otherwise blinded it before the raid' (McGraw, 2013). Unlike an attack on infrastructure, the relevant cyber activities had no direct effect on the mission's target. Rather, it is an example where a cyber attack (that could be considered as non-kinetic) acted as a force multiplier for traditional military capabilities, with successful kinetic results.

The implication of this type of cyber-enabled force amplification is that the threshold of kinetic effect may need to be considered with reference to broader military or political objectives, to which a cyber operation may make a necessary, but not sufficient contribution. Additional questions concerning the necessity of kinetic effect as a necessary component of cyber war and cyber warfare could consider the well-established tactics of espionage, disinformation, diversion, subterfuge and feints in support of military action. Each of these acts may make significant contributions to the achievement of a military objective. However these tactics may produce little to no kinetic effect on the physical world.

The Implications of Definitional Uncertainty

Interpretive complications surrounding thresholds of violence and kinetic effect in cyber war and cyber warfare further contribute to the research problem – inconsistency and divergence between a multitude of definitions of cyber war and cyber warfare. This issue is further exacerbated by the inconsistent use and lack of delineation between the terms cyber war and cyber warfare. In the works analysed thus far, some researchers have used the term cyber war, some researchers have used cyber warfare, and one researcher has used the alternative term cyber warfare operations. In the material examined, no researchers offer the means to clearly

distinguish between these terms, or how these terms relate to one another. The distinction between the terms as understood by the author, where cyber war is an act and cyber warfare a means, has not been validated by engagement with the literature.

The exploratory literature survey has now presented an evidential basis for the research problem, having demonstrated:

- The existence of multiple divergent definitions;
- The interpretive difficulty that surrounds the concepts of thresholds of violence and kinetic effect; and
- The lack of clear delineation between the terms cyber war and cyber warfare.

This provides a basis to consider the effects of the research problem, aspects of which have already been contemplated by researchers within the discourse. For example, Raboin (2011) states that 'the lack of workable, universally accepted definitions of cyberspace and cyber warfare only further exacerbates any attempt to analyse international regulation of activities, such as cyber warfare, occurring within the cyberspace domain'. A complementary opinion is presented by Liff (2012), who notes 'writings on cyberwarfare have long been plagued by major definitional problems, one consequence of which has been a lack of analytical coherence'.

The author acknowledges that some degree of divergence between definitions may be understood as a natural result of multiple researchers examining cyber war and cyber warfare in different contexts and for different purposes. However, the opinions offered above by Raboin and Liff broadly reflect the author's own; that a failure to consider the relationships and inconsistencies between divergent definitions are an impediment to the creation of focused, consistent and reconcilable research. As a result, the academic progression of the domain is inhibited, along with the ability to produce effective and explanative theory and to analyse the implications of new empirical cyber events.

Conclusions

Through this exploratory survey of literature, the author has drawn several interim conclusions that will contribute towards the determination of an appropriate approach and methodology. Evidence of the problem includes:

- The existence of a series of divergent, inconsistent definitions;
- A lack of analysis that considers the implications of the relationships and inconsistencies between definitions;
- The degree of interpretive complexity that surrounds the application of thresholds of violence and kinetic effect as a necessary component of definitions; and
- A lack of distinction between the terms cyber war and cyber warfare.

This formulation of the research problem, and its related effects, establishes the basis for the research undertaken in this thesis. An explication of the tools used to ensure that credible research is produced – a research framework and methodological design – is presented in the next chapter.

Chapter Two: Methodological Design

The research surveyed in Chapter One indicated the following:

- The presence, within discourse, of a number of divergent and inconsistent definitions of cyber war and cyber warfare;
- That the relationships between definitions and between the terms ‘cyber war’ and ‘cyber warfare’ are indistinct and under explored;
- That it is not obvious if one definition is, or should be dominant; and
- That the absence of material that considers the relationships and inconsistencies between definitions may impede consistent discussion of the terms cyber war and cyber warfare.

The survey conducted in Chapter One, however, was exploratory. Its purpose was to identify whether there was an issue justifying further research and to draw initial conclusions that would allow for the selection of an appropriate research methodology and approach. To explore and validate the conclusions drawn in Chapter One, a comprehensive survey and comparative analysis of definitions of cyber war and cyber warfare is required.

As the research activity was to be conducted primarily by the engagement of an individual researcher with definitions presented in various texts, an interpretive element to the research findings would be unavoidable. Where appropriate, the measurement and analysis of quantitative information would be used to support conclusions drawn from the interpretation of qualitative definitions; however, the deployment of quantitative analysis would be supplementary, rather than dominant. Accordingly, it was crucial that a research framework was developed that structured the author’s interpretive analysis in a manner that ensured academic credibility. Based on the subject of the study, definitions vying for influence and authority, it was judged that a methodology based on the theory and practice of discourse analysis would be best suited to form the basis of the research framework.

Discourse Analysis as a Methodology

There are substantial variations within the theory and practice of discourse analysis. This is significant in that it provides researchers with the ability to strategically adapt a discourse analysis methodology to meet their specific research objectives. Expanding on arguments put forward by Jorgensen and Phillips (2002), any adaptation should, however:

- Articulate a consistent set of theoretical foundations on which the discourse analysis is built;
- Identify the epistemological nature of the knowledge that the discourse analysis will generate;
- Establish how the concept of 'discourse' will be applied within the parameters of the research; and
- Identify the limits of the discourse to be analysed.

The methodological design of this research project can be considered as an instance of this type of tailored discourse analysis. Thus, each of the aforementioned criteria, as well as the relevance they have to the research subject, are addressed below.

The foundational theory of the discourse analysis methodology used in this thesis is based on social constructivism. Social constructivism is an approach to knowledge emphasising that knowledge can be produced, or constructed, by social actions (Detel, 2015). It aligns with the four premises that appear across all manifestations of social constructivism, as set out by Burr (1995), who in turn built upon the work of Gergen (1985). The author's own representation of the premises is outlined below.

1. Our knowledge is not unfiltered, but rather mediated through discursive practices, for example communicative acts, language use or broader processes of social construction.
2. Our interpretations and representations of events are contingent products of our cultural background and historical location; perspective is malleable and subject to change.

3. Our understanding of events is created through social processes that allow us to construct knowledge and compete for its successful propagation.
4. As knowledge construction solidifies into worldviews, value judgements become inevitable; the construction of knowledge and truth has consequences.

Application of Methodology

In this thesis, each of the four premises of social constructivism set out above are closely linked to the research subject:

1. Our knowledge of cyber war and cyber warfare and hence, how we define them, is mediated through discursive practices. The discursive practices examined in this research are the publication of academic or military documents.
2. Interpretations and representations of cyber war and cyber warfare, thus definitions, are contingent products of perspective. The research in this thesis analyses perspective as it applies to definitions by considering the academic origins and historical authenticity of the definitions.
3. Definitions of cyber war and cyber warfare are, in part, constructed. In this thesis a definition's claim to authority is considered to be made through successful propagation. This was studied by measuring their academic influence.
4. Definitions underlie how the phenomena of cyber war and cyber warfare are understood. This informs value judgements as to whether an empirical event qualifies as cyber war or cyber warfare and even as to whether the phenomenon is strategically significant. The influence of definitions on value judgements thus underscores the need to fully consider the implications the definitions have on the understanding and interpretation of cyber war and cyber warfare. This aspect is addressed in the final chapter of this thesis.

The epistemological nature of the knowledge produced by this thesis is in part driven by these theoretical foundations and their alignment to social constructivist theory. The social constructivist view that all knowledge is contingent is an anti-foundationalist perspective; it

contrasts with the foundationalist perspective that knowledge can be founded on a meta-theoretical foundation beyond human contingency (Jorgensen & Phillips, 2002). The epistemological nature of the knowledge in this thesis, however, sits midway on a continuum between the poles of anti-foundationalism and foundationalism. The knowledge produced herein is anti-foundationalist, in so far as it is based on definitions, which are constituted by contingent human interpretation of a phenomenon – in this case of cyber war and cyber warfare. However, a foundationalist element is also present, in that definitions arise in response to real world events, which can be empirically measured with a degree of objectivity.

This thesis' deployment of discourse is based on a tailored application of the concept of an 'order of discourse' (Fairclough, 1995; Jorgensen & Phillips, 2002). The order of discourse is understood as a terrain upon which competing discourses attempt to disseminate their claims to authoritative knowledge. In this thesis, the competing discourses are individual definitions of cyber war and cyber warfare, which are differentiated through inconsistency. The 'order of discourse' is a sum representation of all the definitions and the contest between them.

Within the order of discourse definitions are represented as competing to gain influence and claim pre-eminence as the authoritative definition. Definitions that fail to gain influence are marginalised and so have a weakened position within the order of discourse. Thus, through the analysis of a representative sample of definitions of cyber war and cyber warfare, this thesis analyses both discourse and order of discourse. In doing so it examines both the characteristics of individual definitions (discourses), and the relationships and conflict between them (the order of discourse).

As a result of ongoing discursive practices, the boundaries of discourse and orders of discourse are not fixed; rather they are subject to constant change and interpretation. The delimitation of a particular discourse thus becomes a choice made by the researcher. This in turn significantly influences the methodological design of the research.

In accordance with this principle, the analysis of the discourses and orders of discourse in this thesis is limited to academic and military discussion of definitions of cyber war and cyber warfare. The objects (texts) which were chosen to represent the discourses, and upon which analysis will be performed, are published articles and papers accessible via an academic search engine. Within each text, the discourse analysis was limited to considerations regarding the text's presentation of the relevant discourses, in this case the text's presentation of definitions of the terms 'cyber war' and 'cyber warfare'. Limits on qualifying literature were placed to generate a body of data for analysis that was representative and authoritative, but would not overwhelm the capabilities of a single researcher to perform the analysis in a timely fashion. Further information on the actions taken to ensure that the sample was representative and authoritative is provided under 'Applicability', on pages 25 and 26.

Academic Validity

This thesis produced empirical data subject to the positivist standards of objectivity, reproducibility and reliability. However, as the research project deploys discourse analysis as its primary methodology, a substantial amount of research output is qualitative. Accordingly, positivist standards of objectivity, reproducibility and reliability partially lose their applicability as standards of credibility. This creates a risk concerning the effect of researcher bias on research validity.

Guided by the work of O'Leary (2002), this research project addressed the underlying concerns regarding subjectivity through use of the post-positivist criteria of transparency, auditability and dependability. As opposed to objectivity, where results are considered to be free from researcher subjectivity, transparency focuses on rendering explicit the effect researcher bias may have on the conclusions drawn. Whereas reproducibility aims for homogenous results when a single methodology is followed by multiple researchers, auditability allows for deviations in results due to variations in researcher perspective, so long as the research methods are explicated to allow readers to trace how the researchers have drawn their conclusions. Finally, the criterion of reliability, which concerns the ability of

research results to be consistently reproduced under multiple trials, is instead met with dependability. By using the concept of dependability, the author accepts that interpretivist research, while having lower empirical reliability, is dependable if it adheres to a meticulous and well-documented research process.

Auditability and Dependability

The criteria of auditability and dependability are met through clear articulation of the process the author has followed to generate and analyse the sample, detailed at the conclusion of this chapter. To meet the required standards of transparency, it is necessary for the author to make clear his own potential bias concerning the subject matter. This potential bias is best represented by the author's own published definitions of cyber warfare, presented below.

> 'Cyber warfare is … an extension of policy via the military exploitation of cyberspace to create kinetic effects that approximate the effects of conventional weaponry. These effects either constitute a serious threat to a nation's security, or are conducted in response to a perceived threat against a nation's security' (Hughes & Colarik, 2016); and
>
> 'The critical features of cyber warfare can be summarised in three points. First, cyber warfare involves actions that achieve political or military effect. Second, it involves the use of cyberspace to deliver direct or cascading kinetic effects that have comparable results to traditional military capabilities. Third, it creates results that either cause, or are a crucial component of a serious threat to a nation's security, or that are conducted in response to such a threat' (Hughes & Colarik, 2016).

A failure of the author to manage the subjectivity represented by these definitions would likely manifest as an unwarranted privileging of definitions that most closely matched his own. To avoid undue impact on the research results, the author has managed this subjectivity by, where applicable, basing his analysis on verbatim text, rather than on interpreted text. Awareness of

the potential impact of this subjectivity has also been maintained throughout the production of this thesis.

Validity and Authenticity

The research presented in this thesis further addresses standards of academic integrity through negotiation between the positivist benchmark of validity and the post-positivist benchmark of authenticity. Validity is concerned with obtaining a single 'correct' truth value using a methodological design that establishes a 'clear relationship between the reality that is being studied and the reality that is being reported' (O'Leary, 2002). A limited consideration of validity is integral to methodological design; in this thesis, it is demonstrated by the cohesion between the methodology and the explored topic. However, in consideration of the theoretical assumptions of this thesis' application of discourse analysis, no one definition can be ascribed the status of a single 'correct' truth. Accordingly, the methodological deign of the thesis also relies on the concept of authenticity. While authenticity is also concerned with truth values, it allows for an expansion beyond conventional conceptions of a singular truth, recognising that multiple truths may exist. In the context of this thesis, this is recognised by acknowledging that multiple definitions each lay claim to a truth. The research presented in this thesis is therefore considered authentic in so far as it acknowledges the possibility of multiple-truth values amongst the definitions, as well as by its success in portraying each definition's claim to truth, without bias.

Applicability

The final criterion of research credibility addressed is applicability – whether the results of the research are applicable beyond the framework through which they have been generated. In this thesis applicability has been met through the generation of a broad sample that can be considered representative of the discourse being examined. The sample was generated by searching the academic search engine 'Google Scholar' for published documents that include the terms 'cyber war' or 'cyber warfare' in their title, as key words, in an abstract or at least

five times in the main document body. To qualify for inclusion in the sample, a document must also have been published on or before 31 July, 2016 meet the following criteria and be either

- A peer-reviewed article from an academic journal; or
- A peer-reviewed paper from a published conference proceeding; or
- A publicly available military document that was published for internal or external use; and
- Be included in the first 20 pages of results returned by the search engine.

As the focus of the research was on academic and military texts, non-military policy documents were excluded form search results.

The search methodology was repeated for slight lexical variations of terms, such as 'cyberwar', or 'cyber-war'; these were considered as synonymous with cyber war and cyber warfare for the purposes of determining qualifying literature. The application of the methodological design of the thesis generated 159 qualifying articles to create the sample for the thesis. A complete table of results can be found at Appendix A.

Research Questions and Analytical Approach

Having determined the boundaries of the sample, a series of layered research questions were developed. These questions align with the research objectives set out in the Introduction and each question was designed to uncover or clarify an attribute of definitions of cyber war or cyber warfare, or the related discourse. The research questions are as follows.

1. What are the most commonly occurring characteristics of the definitions of the terms 'cyber war' and 'cyber warfare' within the current body of publicly available academic and military literature?
2. Which academic disciplines contribute the greatest number of definitions of 'cyber war' and 'cyber warfare' within the current body of publicly available academic and military literature?

3. Does the current body of publicly available academic and military literature provide the basis for clear distinction and separate definitions of the terms ‘cyber war’ and ‘cyber warfare’?
4. What is the history of the definitions of the terms ‘cyber war’ and ‘cyber warfare’ and how have they emerged over time?
5. What are the most influential definitions of the terms ‘cyber war’ and ‘cyber warfare’, evidenced by academic citation count?
6. What are the relationships between divergent definitions of the terms ‘cyber war’ and ‘cyber warfare’?
7. What are the inconsistencies between definitions of the terms ‘cyber war’ and ‘cyber warfare’?
8. How can the inconsistencies between definitions of the terms ‘cyber war’ and ‘cyber warfare’ be fully or partially resolved?

To address these questions, each qualifying document was analysed according to an analytical model based on six interrogative categories.

- The first category determined whether the text offered either an explicit or implicit definition of cyber war or cyber warfare. A definition was considered explicit when it presented a conception of cyber war or cyber warfare that was distinct, clearly stated, and unambiguous. A definition was considered implicit when it did not meet the aforementioned criteria for explicit definitions.
- The second category of analysis considered the terminology used in the text; whether it used the term ‘cyber war’, ‘cyber warfare’, or used both terms.
- The third category concerned academic discipline; it sought to identify the academic discipline which the text that contained the definition was most closely aligned with. Academic discipline was determined by the publishing venue of the text – for example, academic journal or conference proceedings. Texts published through military organisations were categorised as belonging to the military discipline.

- The fourth category of analysis concerned the historical context of the definition offered in the text. This was determined by recording the year in which the text was first published.
- The fifth category concerned the influence of the text and the definition therein. This was determined by recording the academic citation count of each text, extracted from Google Scholar when the article was accessed.
- The final category concerned the attributes and characteristics of the definition offered in the text. Where possible, definitions were recorded through a verbatim extraction from the document. When this was not possible – as for example, for some implicit definitions – the author supplemented the extraction of the definition through contextualised analysis and interpretation of the surrounding text.

Conclusions

This chapter describes the methodological design of this thesis: a discourse analysis-driven survey and comparative analysis of definitions of cyber war and cyber warfare. The scope of the discourse analysis has been set; analysis will consider definitions present in academic articles in peer reviewed journals and conference proceedings, as well as military publications. The theory of discourse analysis and its application to the methodological design has been presented, as has consideration to how the application of methodology within the research framework meets key criteria of research validity. The chapter has detailed how methodology was used to generate a representative research sample and to structure the analysis performed on the sample.

The result is a tailored methodological design, enabling analysis to be performed at three descending levels of abstraction:

- The level of discourse;
- The level of individual definitions; and
- The level of structural components of definitions.

Chapters are presented according to these levels of abstraction:

- Chapter Three focuses on the level of discourse;
- Chapter Four focuses on individual definitions;
- Chapter Five focuses on the structural components of the definitions; and
- Chapter Six considers the collective applications from research findings, as well as opportunities for further research.

Chapter Three: The Discourse of Definitions

As set out in Chapter Two, the first level of analysis performed on the sample was carried out at the level of discourse. This included analysis of any consistent delineation of meaning between cyber war and cyber warfare and the prevalence of distinct, inconsistent definitions in the literature. Discourse-level analysis also allowed for examination of the emergence and evolution of the discourse over time and consideration of the different academic disciplines of which the discourse has been comprised.

Usage of Terms: Cyber War and Cyber Warfare

The first act of analysis performed on the sample was to map the frequency with which the terms cyber war and cyber warfare were used in the discourse. Table 1 demonstrates the prevalence of each of the terms in the sample of 159 articles.

Table 1. Occurrence of Terms in the Sample Articles

Use of Terms in Articles	Quantity
Cyber War Only	39
Cyber Warfare Only	43
Both Terms, No Distinction	75
Both Terms, Different Definition	2
Total	159

Tellingly, over half of the articles only used a single term in their analysis; 39 articles exclusively used ‘cyber war’ and 43 articles exclusively used ‘cyber warfare’. 75 articles used both terms, but did not offer a means to formally distinguish between the terms. Only two articles offered distinct definitions of each term. Out of the 75 articles that made use of both terms, 35 used cyber warfare as the dominant term, 20 used cyber war as the dominant term, while 20 articles used both terms with comparable frequency. A term was considered to be dominant if it was used at least twice as often as the alternative term.

It was noted that in 12 out of the 35 articles that included both terms, with cyber warfare as the dominant term, cyber war was used to denote a particular act or event, which aligns with the author's original premise regarding the distinction between 'war' and 'warfare'. A similar pattern appeared in articles that used both terms with comparable frequency; five out of 20 articles used cyber war to indicate an act or event.

While these trends are notable, the author did not feel that they were of sufficient weight to alter the key conclusion drawn from this information – that within the examined discourse, the clarity of distinction between the terms cyber war and cyber warfare is insufficient. Indeed this analysis suggests that many authors use these terms interchangeably. In some articles the degree to which the terms are interchanged without apparent consideration suggests that some authors use the terms synonymously. This is not to say that the lack of distinction between the terms is desirable; indeed, the state of ambiguous equivalence between the terms can be considered as an impediment to the clarity of the discourse.

Explicit versus Implicit Definitions

The next task focused on analysis of the proportion of articles that offered a clearly stated explicit definition of cyber war or cyber warfare, versus articles that offered an implicit definition of cyber war or warfare. As per the methodological design of the research project, the definitions were categorised as explicit or implicit. Definitions were considered explicit when an article presented a conception of cyber war or cyber warfare that was distinct, clearly stated and unambiguous. The implicit definition category was used to group conceptions of cyber war and cyber warfare presented in the articles where an explicit definition of cyber war or cyber warfare was not present. Implicit definitions encompassed a wide spectrum of lingual specificity. This includes uses of the terms where reasonably precise definitions could be inferred from the text, through to uses of the terms in a 'purely descriptive, non-normative sense' (Schmitt, 2013) such as in The Tallinn Manual on the International Law Applicable to Cyber Warfare, to uses of the terms that were regarded as largely superficial.

As illustrated in Table 2, out of the 159 articles examined, only 56 offered explicit definitions, versus 103 articles that based their analysis on generally weaker, implicit definitions of cyber war or warfare.

Table 2. Definitions in Articles - Explicit vs. Implicit

Definition Category	Quantity
Explicit Definitions	56
Implicit Definitions	103
Total	**159**

The finding that the majority of articles that base their analysis on implicit rather than explicit definitions provides an evidentiary basis for the author's agreement with the conclusions of Raboin (2011) and Liff (2012), presented in Chapter Two, which state that the analytical utility of the cyber war and warfare discourse has been weakened by ambiguous terminology and major definitional problems. As a result, the meaning of cyber war and cyber warfare has become extremely convoluted. It is acknowledged that some articles offer instead an explicit definition of related terms such as 'cyber-attack' (Schmitt, 2013, Nguyen, 2013) or 'cyber conflict' (Otis & Lorents, 2010). However, unless the relationship of such ancillary terms to cyber war and cyber warfare is clearly articulated, the definition of further related terms does little to clarify the discourse.

History of the Discourse

As set out in methodological design in Chapter Two, the history of the definitions of cyber war and cyberwarfare, as well as the nature of the emergence of the definitions over time, is a key area of enquiry. The oldest article in the sample is Arquilla and Ronfeldt's 1993 article 'Cyberwar is Coming!' (Arquilla & Ronfeldt, 1993). The data, shown in Figure 1, illustrates that from the publication of Arquilla and Ronfeldt's article to the turn of the century, cyber war and cyber warfare discourse remained on the margins of academic debate. From 2000 until 2008 there was a gradual increase in the number of articles published. It was not, however,

until 2009 that rapid growth in the discourse became evident. The number of articles published in the domain peaked in 2011, then remained strong through to 2013. From 2014 onwards there was a notable drop in the number of articles published.

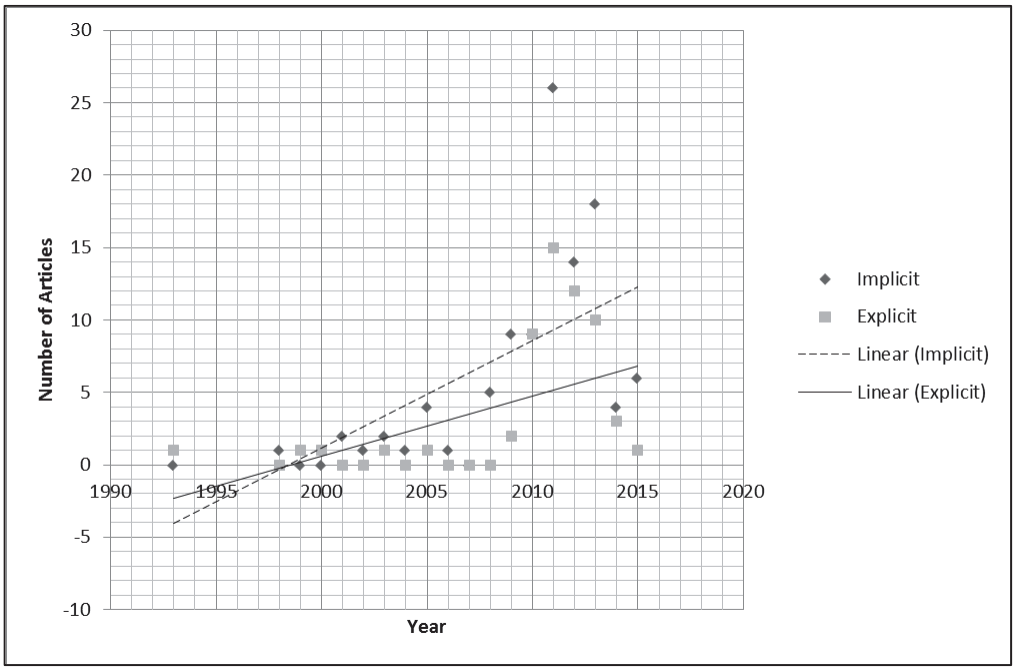

Figure 1. Implicit/explicit definitions of cyber war and cyberwarfare in the sample articles by year of publication

It is proposed that the number of articles published in the discourse peaked in response to what could be considered the three most notable cyber incidents in the international domain; the cyber conflicts between Russia and Estonia in 2007, between Russia and Georgia in 2008 and the Stuxnet attack in 2011. The 'lag' between the incidents of 2007 and 2008 and the marked increase in publications within the discourse is likely attributable to the time taken for reliable information to emerge, in addition to the time required to take an article from conception through to publication in a peer-reviewed conference or journal.

Based on these observations of the waxing and waning of the discourse over time, it is possible that the discourse will once again expand in response to future empirical incidents of cyber conflict. For example, while the majority of the researchers whose work has been analysed

would be unlikely to consider the recent Russian cyber-attacks against the US Democratic Party and alleged interference in the 2016 U.S. election as cyber war or cyber warfare, this event may still generate a considerable body of academic work of relevance to the discourse of cyber war and warfare definitions.

Disciplines within the Discourse

As analysis of the results of the project's methodological enquiry progressed, the inter-disciplinary nature of the discourse soon became apparent. As per the methodological design, articles were categorised into different academic disciplines, based on the discipline that the publication the article appeared in was most closely associated with (Table 3).

Table 3. Implicit/Explicit Definitions by Discipline

Implicit and Explicit Definitions by Discipline				
Discipline	**Implicit**	**Implicit %**	**Explicit**	**Explicit %**
Law	27	16.88%	14	8.75%
Military	22	13.75%	15	9.38%
Information and Communications Technology	22	13.75%	10	6.25%
Strategic Studies & Security Studies	15	9.38%	8	5.00%
Other	8	5.00%	3	1.88%
International Conference on Cyber Conflict	4	2.50%	4	2.50%
International Relations	5	3.13%	3	1.88%
Total	**103**	**64.38**	**57**[5]	**35.62%**

The discourse is dominated by four disciplines; Information and Communication Technology (ICT), Law, Military Studies, and Strategic and Security Studies. These four disciplines account for 133 out of the total 160 definitions encountered, and 47 out of the 57 explicit definitions. The remaining articles were grouped into the categories of International Relations, the International Conference on Cyber Conflict and 'Other'. The International Conference on Cyber Conflict is hosted by the NATO Cooperative Cyber Defence Centre of Excellence

[5] One article offered two explicit definitions, hence the number of definitions (160) is different from the number of articles (159)

(CCDCOE) and includes submissions relevant to cyber security from a wide range of academic disciplines. Accordingly, the author believed that articles published from conference proceedings could not accurately be categorised under a single academic discipline; indeed, the diverse backgrounds of researchers participating in this conference is representative of the multi-disciplinary nature of the discourse. A similar conclusion can be drawn from the composition of the 'other' category, which includes articles from publications associated with International Management, Political Geography, and Philosophy.

Out of the four dominant disciplines within the discourse, the largest body of work was associated with Law, with the majority of articles concerned with the implications that the emergence of cyber war and warfare will have on the existing Law of Armed Conflict, particularly the conditions under whether cyber war or warfare can be considered as a 'use of force', or 'armed attack'. The second largest body of work encountered in the sample was associated with ICT. This was considered the most fragmented discipline, both in the divergence of definitions presented and the ambiguity with which the terms cyber war and warfare were used. While it included articles that made valuable contributions to the discourse (Lewis, 2011; Parks & Duggan, 2011), articles were also encountered where the terms cyber war or cyber warfare were used with a significant degree of ambiguity and superficiality (Wang & Wang, 2004; Catuogno & De Santis, 2008).

The discipline of Military Studies made the third largest contribution of articles to the discourse. Unsurprisingly, articles associated with the military discipline focused predominantly on the means by which cyber war and warfare capabilities could be used to achieve military advantage. In addition, the articles discus the ramifications of cyber war and warfare in regard to military ethics, ethos and force development. Readers should note that this category includes publications from Military Law journals, which were included in the category because of the belief that their primary focus was on military, rather than on purely legal matters.

The final dominant discipline identified in the discourse relates to the fields of Strategic Studies and Security Studies. While these are usually thought of as distinct disciplines, they have similar fields of enquiry and are often published in venues that encompass both fields. For these reasons it was decided to represent them as a single discipline for the purpose of this thesis. As could be expected, articles associated with this discipline placed much greater emphasis on the political, international and strategic aspects of cyber war and cyber warfare.

Influence of Disciplines on the Discourse

The next area of enquiry was the influence of the articles associated with each discipline. As set out in the methodological design, the measure of influence was the number of times an article had been cited. Average citations per article in each discipline were calculated by adding the total citations of each article, then dividing by the total number of articles in that discipline. This information was further broken down into average citations for both implicit and explicit definitions in each discipline.

Table 4. Average Impact of Articles by Discipline

Average Impact by Article			
Discipline	**Implicit**	**Explicit**	**Total**
Strategic Studies & Security Studies	39.70	128.00	84.00
Information and Communications Technology	48.18	26.90	37.54
Law	39.74	21.08	30.41
International Relations	16.60	27.67	26.30
Other	37.13	3.25	20.70
International Conference on Cyber Conflict	22.50	15.00	18.80
Military	16.73	18.27	17.70
Total	31.51	34.31	33.64

The most influential disciplines in the discourse by citation count are as follows:

1. Strategic and Security Studies;
2. ICT;

3. Law;
4. International Relations;
5. Other;
6. Cyber Conflict Conference;
7. Military.

However, if citations from articles with implicit definitions are discounted, the rankings change to:

1. Strategic and Security Studies;
2. International Relations;
3. ICT;
4. Law;
5. Military;
6. Cyber Conflict Conference;
7. Other.

This indicates that despite having the lowest number of articles of the major disciplines active in the discourse, the fields of Strategic and Security Studies had the greatest impact on the discourse. Conversely, Military Studies, which has the second highest number of articles in our sample, had a low degree of influence.

While the average citation count for articles featuring explicit definitions was slightly greater than that for articles featuring implicit definitions (34.31 to 31.51), the author was surprised that this was not higher – it had been assumed that articles with explicit definitions would be more influential in the discourse. In accordance with this observation it is noted that articles in the Law, ICT and Other categories with implicit definitions were more influential than articles with explicit definitions. In the ICT category, some of this phenomenon can be ascribed to an outlying article – Wang and Wang's 'Cyber Warfare: Steganography vs. Steganalysis' (2004). The large number of citations it has accrued (428) does not align with

its limited relevance to the domain (cyber warfare is only mentioned once in the document), granting it a disproportionate weight in the calculations. If this outlier is removed the average citations for ICT articles with implicit definitions is reduced from 48.18 to 30.01, and the total average citations for all articles with implicit definitions in our sample is reduced from 34.31 to 28.91. A similar pattern was observed in the Other category, where two heavily cited articles with only ancillary discussion of cyber war and cyber warfare acted to inflate the average citation count for articles with implicit definitions.

The extent to which articles in the Law discipline with implicit definitions exerted considerably greater influence than those with explicit definitions, is worthy of further consideration. The author contends this is due to a focus of the discipline, namely how cyber incidents should be conceived of with regard to The Law of Armed Conflict and International Humanitarian Law. More specifically, a substantial number of documents from the legal discipline consider the circumstances under which acts of cyber aggression should be considered as either a 'use of force', or an 'armed attack', as those terms are defined within Article 51 of the U.N. Charter. The majority of this analysis does not require a perennial definition of cyber war or warfare, as it is focused on whether individual acts would cross thresholds established in international law.

Conclusions

The initial results of the application of the research methodology set out in Chapter Two has allowed the presentation of the following conclusions. First, when considered form the perspective of how the terms are used in texts, the discourse shows a lack of clear distinction between the terms 'cyber war' and cyber warfare'. It has been demonstrated that authors have a tendency to use the terms interchangeably, arguably synonymously. Second, despite being located in a domain ostensibly concerned with the explication and implications of newly emerged technologies and modalities, the majority of articles do not offer explicit definitions of either cyber war or cyber warfare on which to base their analysis. Third, an analysis of the emergence of the discourse over time suggests that there is a correlation between major

international cyber incidents and the expansion (and decline) of the discourse. Fourth, the discourse is inherently inter-disciplinary. This is demonstrated by the considerable bodies of research arising from publications associated with the disciplines of Information Communication Technology, Military Studies, Law, and Strategic and Security Studies. Having examined the general characteristics of the discourse, as represented by the entirety of the sample, analysis will now turn to a focused subset of the discourse – explicit definitions of cyber war and cyber warfare.

Chapter Four: A Hierarchy of Definitions

The previous chapter focused on the entirety of definitions encountered in the sample – both implicit and explicit. Consideration of implicit definitions has provided valuable information as to the shape of the discourse. It was the author's considered view, however, that further insight would be achieved through a more comprehensive analysis of the explicit definitions encountered in the sample. By focusing close analysis on explicit definitions, the author sought to reduce the effect of his subjectivity. This was achieved by only conducting close analysis on explicit definitions where the author of the source text's intention was rendered overt via a clear, unambiguous definition that attributed distinct properties to cyber war or cyber warfare. This approach would limit interpretive ambiguities that may arise from examining implicit definitions, where the intent of the author as represented by the text was often ambiguous.

Analysis: Explicit Definitions

Out of the 159 articles examined, 56 offered explicit definitions of cyber war or cyber warfare. One article offered two definitions, for a total of 57 explicit definitions. The first action was to order the explicit definitions more effectively by consolidating duplicated definitions – definitions that appeared verbatim in more than one text. This was achieved by counting each duplicate definition once, then associating it with the discipline of the article using that definition that had the highest citation count. This resulted in the total number of explicit definitions being reduced from 57 to 44, as well as minor adjustments to the number of definitions associated with each discipline. The results of this process are illustrated in Table 5.

Table 5. Explicit Definitions (Duplicates Removed)

Explicit Definitions (Duplicates Removed)		
Discipline	**Explicit**	**Percentage**
Military	13	29.55%
Law	10	22.73%
Strategic Studies & Security Studies	7	15.91%
Information and Communications Technology	6	13.64%
International Conference on Cyber Conflict	3	6.82%
Other	3	6.82%
International Relations	2	4.55%
Total	44	100%

The next action was to shift the analysis down to the level of individual explicit definitions, then to rank these according to influence. As per the methodological design this was determined by citation count. The top five definitions by citation count are captured in Table 6.

Table 6. Top Definitions by Influence (Citation Count)

Reference	Definition	Citations	Discipline
Arquilla, J., & Ronfeldt, D. (1993)	Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting, if not destroying, information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to know itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, and so forth. It means trying to know everything about an adversary while keeping the adversary from knowing much about oneself.	655	Strategic & Security Studies
Rid, T. (2012)	(Cyber) War has to have the potential to be lethal; it has to be instrumental; and it has to be political.	225	Strategic & Security Studies
Nicholson et al. (2012)	Attacks and defence issued by nation states take place over networks rather than by physical means.	117	ICT
Schaap, A. J. (2009)	The use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, of another state.	95	Law
Nye Jr, J. S. (2011)	Hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence.	65	Military

Analysis: Cross-Disciplinary Definitions

The five definitions listed in Table 6 had the greatest influence by citation count out of the individual articles encountered in the sample. As noted, however, several definitions were encountered that were repeated in several articles across several disciplines. While this can be regarded as further evidence of the cross-disciplinary nature of the cyber war and warfare discourse, the author also considered that a more in-depth examination of these 'cross-disciplinary definitions' could provide another viable method to explore the influence of the definitions. This led to the construction of Table 7, which identifies:

- Each cross-disciplinary definition;
- The references for the articles in which the definition appeared;
- The discipline of each article in which the definition appeared;
- The number of times each article had been cited;
- The original source of the definition;
- The number of citations arising from the source article; and
- The total number of citations associated with the cross-disciplinary definition.

Table 7. Breakdown of Cross Disciplinary Definitions

Definition	Reference	Discipline	Citations	Original Source	Citations from Source	Total Citations
Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles.	Cimbala, S. J. (2011).	Military	7	Arquilla, J., & Ronfeldt, D. (1993)	655	712
	Arquilla, J., & Ronfeldt, D. (1993).	Strategic & Security Studies	655			
	Liles et al. (2012)	Conference on Cyber Conflict	11			
	Reich et al.(2010)	Law	14			
	Arquilla, J. (2011).	IR	5			
Any act intended to compel an opponent to fulfil our national will, executed against the software	Alford, L. D. (2000).	Military	9	Alford, L. D. (2000)	9	20
	Cahill, et al. (2003)	ICT	11			

Definition	Reference	Discipline	Citations	Original Source	Citations from Source	Total Citations
controlling processes within an opponent's system.						
Cyber war is the uses of ICTs within an offensive or defensive military strategy endorsed by a state and aiming the immediate disruption or control of the enemy's resources.	Taddeo, M. (2012)	Conference on Cyber Conflict	9	Taddeo, M. (2012)	9	13
	Ganji et al. (2013)	ICT	4			
The US Department of Defense defines a combined concept of computer network operations (CNO) as including CNA, computer network defence (CND) and computer network exploitation (CNE).	Leblanc et al. M. (2011)	ICT	12	US Department of Defence/ Joint Chiefs of Staff	130	173
	Chappelle et al. (2013).	Military	8			
	Kirsch, C. M. (2011).	Law	10			
	Turns, D. (2012).	Law	13			
Cyber war is the act of nation state to penetrate another nation's computer or network in order to cause damage or disruption.	Uma, M., & Padmavathi, G. (2013).	ICT	20	Clarke, R. A., & Knake, R. K. (2011)	792	830
	Saad et al. (2011).	ICT	5			
	Caplan, N. (2013).	Strategy & Security	4			
	Feil, J. A. (2012).	Law	5			
	Jolley, J. D. (2012).	Law	4			

Out of the five cross-disciplinary definitions captured in Table 7, only the Arquilla and Ronfeldt definition is present in Table 6 – the initial table constructed to demonstrate definitional influence. The author notes that in 2011 Arquilla modified his and Ronfeldt's original 1993 definition of cyber war (conducting military operations according to information related principles) to what may be considered a more modern formulation – 'An emergent

mode of conflict enabled by and primarily waged with advanced information systems, which are in themselves both tools and targets' (Arquilla, 2011).

Out of the four remaining cross-disciplinary definitions, neither Alford's nor Taddeo's definitions were considered to be sufficiently influential to warrant further analysis. Both definitions were encountered in only one other article and generated substantially fewer citations than the other cross disciplinary definitions. Clarke and Knake's definition – 'Cyber war is the act of nation state to penetrate another nation's computer or network in order to cause damage or disruption' (Clarke & Knake, 2011) – is succinct enough to require little explanation. Aside from its state-centric focus, its most noteworthy point is the volume of citations it has generated – nearly 800. The background and context of the remaining cross-disciplinary definition – the concept of Computer Network Operations, promulgated by the U.S. DoD – is more complex and worthy of further explication.

As defined by the U.S. DoD, Computer Network Operations (CNO) is a combined concept defined as consisting of Computer Network Attack (CNA), Computer Network Defence (CND) and Computer Network Exploitation (CNE). CNA is defined as '[a]ctions taken through the use of computer networks to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves' (DoD, 2010). CND is defined as '[a]ctions taken to protect, monitor, analyse, detect, and respond to unauthorised activity within the Department of Defense information systems and computer networks' (DoD, 2010). CNE is defined as '[e]nabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks' (DoD, 2010).

Two caveats must accompany the author's presentation of CNO as a definition of cyber war or cyber warfare. First, the concept of CNO as it appears in the academic discourse originates in a superseded version of Joint Publication 1-02 – the DoD Dictionary of Military and Associated Terms. Cyber Operations (CO) is no longer considered by the DoD to be a subset of Information Operations (IO); it has evolved 'from its computer network operations roots

into a way to operationally integrate CO with joint operations.' (DoD, 2013). This evolution has seen the US DoD retire the terms CNO, CNA, CND and CNE retired in favour of newly defined terms: Cyber Operations, 'the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace'; Offensive Cyber Operations (OCO), CO intended to project power by applying force in and through cyberspace; and Defensive Cyber Operations, 'CO intended to defend DOD or other friendly cyberspace' (DoD, 2013).

While the distinction between CO and CNO is important, there is substantial consistency between the terms. Such consistency is evident within Joint Publication 3-12(R), and demonstrated by the close correlation of the term 'Cyberspace Attack' – '[c]yberspace actions that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction)' (DoD, 2013) – with CNA. Similar consistency is also evident between the term 'Cyberspace Defense' – [a]ctions normally created within DOD cyberspace for securing, operating, and defending the DODIN (DOD Information Network),' (DoD, 2013) – and CND. Thus, the author considers it unnecessary to replace the concept of CNO with that of CO. Indeed, doing so would misrepresent the considerable influence of the concept of CNO within the discourse. Furthermore, such a replacement is not consistent with the discourse analysis driven methodological design of the thesis.

The second caveat, alluded to in Chapter One, is that the DoD does not equate either the concept of CNO, or that of CO, to cyber war or cyber warfare. However, this equivalence is made in the works of Turns (2012), Kirsch (2011), Leblanc, Partington, Chapman, & Bernier (2011), and Chappelle, McDonald, Christensen, Prince, Goodman, Thompson, & Hayes (2013). The equivalence these authors assert between the terms CNO and cyber war or cyber warfare is valid, particularly when the concept of CNO is considered in light of the DoD's Strategy for Operating in Cyberspace (DoD, 2015). As noted in Chapter Two, despite not making explicit use of the terms cyber war or cyber warfare, the strategy outlined in this document includes actions likely to be considered by many researchers in the discourse as

exemplary acts of cyber war or cyber warfare. For example, the strategy notes how 'the President or the Secretary of Defense may determine that it would be appropriate for the U.S. military to conduct cyber operations to disrupt an adversary's military related networks or infrastructure', or to 'use cyber operations to terminate an ongoing conflict on U.S. terms' (DoD, 2015). Furthermore, the strategy notes how USCYBERCOM may be used 'to deter or defeat strategic threats in other domains', and sets a specific strategic goal that focuses on the creation and maintenance of cyber options to 'control conflict escalation and to shape the conflict environment at all stages' (DoD, 2015).

Notably, neither of the source documents from which the Clarke and Knake or U.S. DoD definitions arose were included in the sample. Clarke and Knake's definition was not originally published through an academic venue, while the source document for the U.S. DoD's concept of CNO was not returned in search results – presumably because it does not include the terms cyber war or cyber warfare. The analysis presented, however, shows that both these works have had considerable influence on the discourse. Indeed, as noted, Clarke and Knake's work generated more citations than any other work.

Based on the above analysis of the cross-disciplinary definitions, Table 6 – the most influential definitions by citation count from a single article, was combined with Table 7 – the breakdown of cross-disciplinary definitions. The results are captured in Table 8. For reasons previously stated concerning low citations, Alford's 2010 definition and Taddeo's 2012 definition were omitted.

Table 8. Most Influential Definitions by Citation Count

Reference	Definition	Citations	Discipline
Clarke, R. A., & Knake, R. K. (2011)	Cyber war is the act of nation state to penetrate another nation's computer or network in order to cause damage or disruption.	830	N/A
Arquilla, J., & Ronfeldt, D. (1993)	Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles.	655	Strategic & Security Studies
Rid, Thomas. (2012)	A potentially lethal, instrumental, and political act of force conducted through malicious code.	225	Strategic & Security Studies
US Department of Defence (2010-2012)	Computer Network Operations (CNO) as including computer Network Attack (CNA), computer network defence (CND) and computer network exploitation (CNE).	173	Military Studies
Nicholson et al. (2012)	Attacks and defence issued by nation states take place over networks rather than by physical means.	117	ICT
Schaap, A. J. (2009)	The use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, of another state.	95	Law
Nye Jr, J. S. (2011)	Hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence.	65	Military

A Discourse Hierarchy of Definitions of Cyber War and Cyber Warfare

Table 8 contains the seven most influential definitions that appeared in the sample. However, under further analysis only five of these are characterised as 'essential' or 'core' definitions, in that they ascribe cyber war or warfare certain characteristics or thresholds that cannot be deduced from other definitions. The five core definitions identified are:

- Clarke & Knake (2011);

- Arquilla and Ronfeldt (1993),;
- Rid (2012);
- U.S. DoD (2010); and
- Nye (2011).

The author contends that the definitions offered by Nicholson, Webber, Dyer, Patel, & Janicke (2012) and Schaap (2009) are more correctly viewed as being derived from the definitions offered by Clarke and Knake and the U.S. DoD. Both definitions utilise the state-centric concept of cyber war and cyber warfare found in Clarke and Knake in addition to the emphasis on CNO that is the focus of the DoD's definition. This omission is further justified by the observation that Schaap's definition uses the language from the DoD definition – 'the use of computer networks to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves' (DoD, 2010) – verbatim.

This analysis leads the author to contend that the five core definitions identified form the foundation for a 'discourse hierarchy' of cyber war and cyber warfare definitions. Out of the 44 explicit definitions encountered in the sample, 43 can be logically placed in the hierarchy structure[6]. Most definitions in the hierarchy have a one-to-one relationship with a core definition. Alternatively, in cases where the definition in question is perceived to include components from two distinct core definitions, a definition may have one to two relationships with two core definitions. The discourse hierarchy is presented overleaf in Figure 2. To clarify the underlying logic of the relationships within it, it is necessary to expand upon each of the five core definitions that form its basis.

[6] One outlying definition, (Brown et al., 2012), could not logically be placed in the model. The definition offered described cyber warfare as 'a technical academic core of tightly interrelated subject matter, as well as a wide range of important topics that, while dependent on the technical core for fullest appreciation, are not dependent on each other. Stated another way, cyber warfare is comprised of, first, a foundational component, dealing with a set of interconnected fundamental technical concepts, and second, a wide range of interdisciplinary topics, touching upon the areas of law, political science, strategy and tactics, policy, ethics, and the study of foreign languages and culture' (Brown et al., 2010)

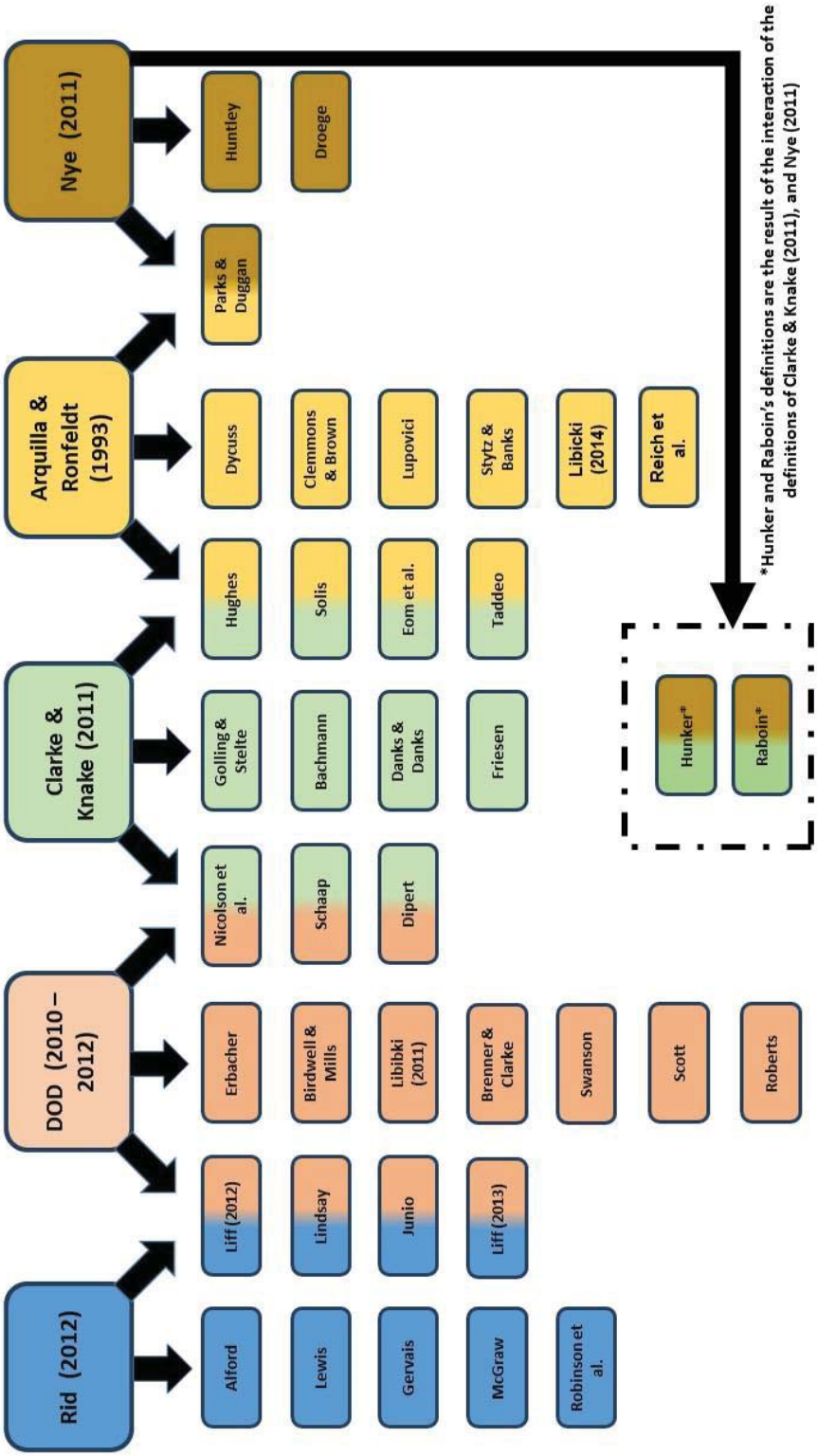

Figure 2. Discourse hierarchy of cyber war and cyber warfare definitions

Rid's definition was discussed in Chapter Two. Taking as his starting point the conception of war presented by Clausewitz (1873), Rid states that cyber war is 'a potentially lethal, instrumental, and political act of force conducted through malicious code' (Rid, 2012). This places an extremely high threshold on what would constitute cyber war or cyber warfare; indeed, Rid argues 'that cyber war has never happened in the past, that cyber war does not take place in the present, and that it is unlikely that cyber war will occur in the future' (Rid, 2012). No other authors encountered placed such demanding thresholds within their definition of cyber war or cyber warfare. However, a considerable number of definitions include sufficient components of Rid's definition to enable them to be grouped under his definition in the discourse hierarchy. Alford's 2000 definition, previously encountered in the analysis of cross-disciplinary definitions, is a useful example. Alford defines cyber warfare as 'any act intended to compel an opponent to fulfil our national will, executed against the software controlling processes within an opponent's system' (Alford, 2000). While it omits Rid's criterion of potentially lethal violence, Alford's definition shares Rid's conception that cyber war and cyber warfare must involve an instrumental and political act of force.

Lewis's 2011 definition – 'the use of cybertechniques to cause damage, destruction, or casualties for political effect by States or political groups' (Lewis, 2011) is in even closer alignment with Rid, although, in a similar manner to Alford, he stops short of saying that cyber war or cyber warfare must be potentially lethal. Moreover, while one could argue that the concept of instrumentality is implicit in his definition, it is not an explicit threshold, as is the case with Rid. A final example is the definition offered by McGraw, who defines cyber war as the application of violent, physical force via virtual means by groups for 'political, economic, or ideological reasons' (McGraw, 2013).

The definitions above have a one-to-one relationship with Rid's definition in the discourse hierarchy. There are other definitions, however, that utilise components of both Rid's definition and the DoD's conception of CNO. An example is the definition offered by Junio

(2013), where cyber war is defined as a coercive act (using force to change or preserve a political status quo) involving CNA (where information is disrupted, degraded, or destroyed). The emphasis on cyber war as a coercive act ties back to Rid, while the reference to CNA and the disruption, degradation or destruction of information is sourced from the DoD's concept of CNO. A similar combination of definition components is evident in Liff's 2012 definition where 'cyberwarfare is conceptualised as including only computer network attacks (CNA) with direct political and/or military objectives – namely, attacks with coercive intent and/or as a means to some strategic and/or brute force end – and computer network defence (CND)' (Liff, 2012).

While Junio's and Liff's definitions are the result of the combination of the definitions offered by Rid and the DoD, numerous other definitions can be traced solely to the DoD. Birdwell and Mills define 'cyber war-fighting actions as CNA plus a subset of CND called CND-response actions (CND-RA)' (Birdwell & Mills, 2011), notably omitting Computer Network Exploitation (CNE) from their definition. A similar definition is offered by Scott, Hardy, Martin, and Thomas (2011): 'Cyber warfare is typically associated with the fields of Computer Network Attack (CNA) and Computer Network Defence (CND)… CNA attempts to create tactical and strategic effects through the control and exploitation of network resources, whereas CND defends against these same objectives'. Related definitions are observed through the combination of the DoD definition and the Clarke and Knake definition. The definitions by Schaap (2009) and Nicholson et al. (2012) are useful examples. In addition, the definition offered by Dipert (2013) is similarly comprised.

One of the key characteristics of Clarke and Knake's definition is that it stipulates cyber war and cyber warfare as something that occurs between nation states. The definitions located under Clarke and Knake within the hierarchy share this state-centric focus, albeit with slight variations. The definition offered by Golling and Stelte (2011) expands the scope of actors involved in cyber war and cyber warfare to include groups operating 'on behalf of, or in support of, a government'. However, the definition of Danks and Danks (2013) does not have

a strict criterion that cyber war or warfare either originates from or is targeted at a state. Rather, they state that 'Cyberwarfare involves groups with the expertise and resources to mount a significant attack, including the accompanying research and development costs, and so arguably includes only those with the backing of a nation-state, whether the group is officially part of the state (e.g. military), or only sponsored (e.g., contractors), encouraged (e.g., patriotic hackers), or tolerated (e.g., international crime) by the state'. They further note that state-backed groups 'typically have a goal that serves the interest of a particular state or state-like group' (Danks & Danks, 2013). Conversely, Bachmann's definition does not require that a specific category of actor initiates cyber war or cyber warfare, so long as the actor in question targets a state and has the means to launch 'a sustained campaign of concerted cyber operations' (Bachmann, 2012).

In a pattern similar to that observed elsewhere in the hierarchy, a number of definitions reflect a dual relationship with both Clarke and Knake's and Arquilla and Ronfeldt's definitions. Definitions such as those offered by Hughes (2010), and Taddeo (2012) utilise Arquilla and Ronfeldt's conception of cyber war and warfare – conducting military operations according to information-related principles – but add the criterion that cyber war and cyber warfare is used 'within an offensive or defensive military strategy endorsed by a state' (Taddeo, 2012), or is 'waged by states and significant non-state actors' (Hughes, 2010). Other definitions grouped solely under Arquilla and Ronfeldt focus more exclusively on operational warfare and the furtherance of traditional, kinetic combat (see Libicki (2014), Clemmons and Brown (1999), and Lupovici (2011)).

The final core definition within the hierarchy is that advanced by Nye – 'hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence' (Nye, 2011). Nye's definition is useful as a means of categorising those definitions that refer to the concepts of 'use of force' and 'armed attack', as they appear in international law. A considerable part of the legal discourse pertaining to cyber war and cyber warfare discusses how these concepts, enshrined in the U.N. Charter, apply to cyber conflict. While there is

considerable disagreement as to whether acts of cyber disruption can ever reach the threshold of the use of force, or even armed attack, there is near universal agreement that cyber war or warfare that causes physical destruction to a level equivalent to traditional kinetic weapons would cross these thresholds. Thus, within the hierarchy, definitions that make reference to 'use of force', or 'armed attack', such as those offered by Huntley (2010) and Droege (2012), were aligned with Nye's definition.

The definition offered by Hunker (2012) was categorised as derived from a combination of Nye's definition with that of Clarke and Knake, as he draws upon the latter's conception of cyber war as something that occurs between nation states. Raboin's definition was similarly categorised, as he states that 'cyber warfare … has come to symbolise a state-sponsored use of weapons functioning within the cyberspace domain to create problematic and destructive real world effects' (Raboin, 2011). The final definition associated with Nye, that proposed by Parks and Duggan, is related to Arquilla and Ronfeldt's definition. They state that 'cyber-warfare, is a combination of computer network attack and computer network defence' and that 'cyber warfare must have kinetic world effects' (Parks & Duggan, 2011). From the context of their paper 'The Principles of Cyber-warfare', this is interpreted to primarily mean kinetic military effects.

Conclusions

The analysis performed in this chapter on explicit definitions of cyber war and cyber warfare encountered in the sample has allowed the presentation of the following conclusion. The discourse is characterised by the existence of a multitude of inconsistent definitions both within and between disciplines. Most of these definitions have exerted minimal academic influence. While there are definitions that have been comparatively influential, there is no dominant functional definition of significance to the discourse. It is proposed that this is indicative of a discourse contested by a multitude of stakeholders with differing agendas. Furthermore, this may be a factor in the discourse of the domain to produce a dominant functional definition. An examination of the effect of pertinent interests of competing

stakeholders in the discourse – for example those working within distinct academic disciplines – as it relates to the failure of the discourse to produce a dominant definition, may be a promising area for future discourse-focused research.

While some element of fragmentation within the discourse may be inevitable, it has nonetheless been shown that almost all of the definitions encountered can be deduced from five core definitions – those identified through sustained analysis of the results produced by the application of discourse analysis on the sample. The identification of these core definitions has, in turn, allowed the author to construct a discourse hierarchy of cyber war and warfare definitions. In itself, the hierarchy has value in its ability to represent a plethora of disparate definitions under a single model and demonstrating the relationships between them. However, it is proposed that the greater value of the hierarchy is its ability to identify points of consistency, rather than inconsistency, between definitions. The author contends that it is the identification of these points of consistency which paves the way for an analytic model which can be used to uncover the structural components of the definitions of cyber war and cyber warfare. The application and construction of this model is presented in the next chapter.

Chapter Five: Definitional Components

The analysis conducted in the previous chapter allowed the construction of a discourse hierarchy of cyber war and cyber warfare definitions. This demonstrated the primacy of five core definitions of cyber war and cyber warfare, both in explanative power and their ability to represent the discourse. Using these five definitions as a starting point, the analysis in this chapter will consider the structural components of the definitions of cyber war and cyber warfare. This will be achieved through the creation of a *structural definition model*, which will be used to analyse the structural components of each definition of cyber war or cyber warfare encountered in the sample.

The structural definition model provides for a rigorous, component-by-component comparative analysis of divergent definitions of cyber war and cyber warfare. While time-consuming, this analysis is crucial in that it provides for the establishment of a foundational definition of cyber war and cyber warfare. Concomitantly, this analysis identifies key points of inter-definitional inconsistency. Collectively, these are essential analytic outputs. They allow for partial reconciliation of the discrepancies between definitions, as well as for future consideration of the doctrinal, strategic and political implications that definitional permutations may have.

A Structural Definition Model

The creation of the structural definition model begins with consideration of the five core definitions of cyber war and cyber warfare, listed in Table 9.

Table 9. Core Definitions of Cyber War and Cyber Warfare

Author	Definition
Arquilla and Ronfeldt (1993)	Cyberwar refers to conducting […] military operations according to information-related principles. It means disrupting, if not destroying, information and communications systems […] It means trying to know everything about an adversary while keeping the adversary from knowing much about oneself.
US Department of Defense (2010)[7]	Computer Network Operations (CNO) as including computer Network Attack (CNA), computer network defence (CND) and computer network exploitation (CNE).
Nye (2011)	Hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence.
Rid (2012)	A potentially lethal, instrumental, and political act of force conducted through malicious code.
Clarke and Knake (2012)	Cyber war is the act of a nation state to penetrate another nation's computer or network in order to cause damage or disruption.

At first observation, it is the dissimilarity between the five core definitions of cyber war and cyber warfare that is most apparent. Arquilla and Ronfeldt's definition can be characterised by its military focus; it principal concern is on the operational or tactical application of cyber techniques to further combat performance. The DoD definition is more expansive, but ultimately shares Arquilla and Ronfeldt's focus on the operational and tactical application of cyber force. Conversely, Rid's definition is the result of the application of Clausewitz's conception of war into the cyber domain; it represents cyber war as an activity where violence is necessary, but is subordinate to strategic and political calculations. Clarke and Knake's definition casts cyber war as solely the province of nation states, while Nye's definition focuses on the effects of cyber war, without consideration to actors, political intent, or military application.

While the differences between these definitions is evident, through a collective application of the key components of each definition, an element of consistency is also apparent. This is

[7] As noted in Chapter Four, the concept of CNO has been retired by the DoD. However it continues to exert considerable influence on the discourse, hence remains as an object of analysis.

demonstrated by how each definition is consistent with the other definitions in that it would accord the following theoretical cyber event the status of cyber war or cyber warfare:

> *A nation state launches a computer network attack with potentially lethal effects against the computer networks and military information and communication systems of another nation state, in order to achieve an objective that is instrumental to a political end.*

Such an event meets the thresholds established in the definitions offered by Rid (the act is potentially lethal, instrumental and political), Clarke (the actors are nation states), and Nye (the act is hostile and will cause effects equivalent to major kinetic violence). Furthermore, the event aligns with the DoD concept of CNA and Arquilla and Ronfeldt's emphasis on the use of military force against adversary information and communication systems.

The consistency of the explanative power of the five definitions to the same cyber event allows the construction of a structural definition model, which seeks to identify structural components that are common to all existing definitions of cyber war and cyber warfare. Through the construction of this model it is proposed that the consistencies, discrepancies and relationships between the different definitions will become more apparent. The structural definition model is presented in Figure 3.

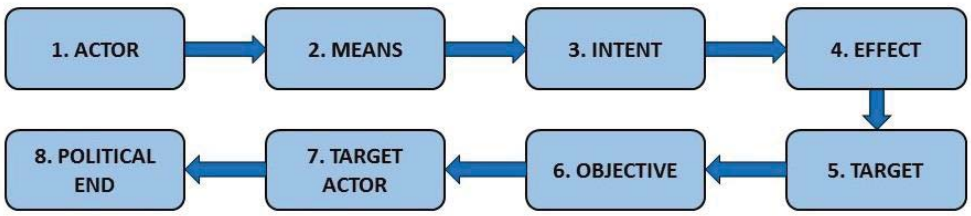

Figure 3. Structural definition model for definitions of cyber war and cyber warfare

Based on analysis of the five core definitions of cyber war and cyber warfare, the structural definition model identifies eight components of which a definition of cyber war or cyber

warfare may be comprised. ‘Actor’ refers to the agent initiating the cyber action. In Clarke and Knake’s definition the actor is a nation state, while Rid’s definition requires the presence of a political actor. ‘Means’ refers to the cyber techniques used in the cyber action. In the DoD definition, the means are computer networks. In Rid’s definition the means is malicious code or malware, spread either through networks or by direct insertion into the target. ‘Intent’ is an aspect of the purpose of the action; the intent present in most of the five definitions is coercive or offensive. CNO, however, also allows for defensive and exploitive intent. ‘Effect’ is a result of the interaction of the means and the intent. Rid’s and Nye’s definitions require the presence of kinetically violent, potentially lethal effects. The other definitions, however, allow for a lower threshold of effect – for example disruption, manipulation or degradation. ‘Target’ concerns the object(s) that the cyber effects will be directed against. ‘Objective’ is the immediate goal to be achieved through cyber war or cyber warfare. The ‘Target Actor’ is the agent that controls the target through or against which an objective is to be achieved. Finally, ‘Political End’ concerns the political outcome that the cyber action seeks to realise.

Relevance of the Structural Definition Model to the Sample

The relevance and explanative power of the structural definition model was tested by examining its correlation with the five core definitions of cyber war and cyber warfare and with the broader sample. Table 10 shows the results of the population of the model with the five core definitions of cyber war and cyber warfare.

Table 10. Structural Definition Model – Core Definitions

Definition	Actor	Means	Intent	Effects	Target	Objective	Target Actor	Political End
Rid (2012)	Political Actor	Malicious Code	Coercive/ Offensive	Potentially lethal	*Unspecified*	Instrumental Objective	*Unspecified*	Unspecified Political End
Nye (2011)	*Unspecified*	*Unspecified*	Coercive/ Offensive	Amplification or equivalence to major kinetic violence	*Unspecified*	*Unspecified*	*Unspecified*	*Unspecified*
Clarke & Knake (2011)	Nation State	*Unspecified*	Coercive/ Offensive	Damage and disruption	Computer or network	*Unspecified*	Nation State	*Unspecified*
DoD (2010):	*Unspecified*	Computer networks	Coercive/ Offensive, Defensive, Exploitive	Disruption, Degradation, Manipulation, Destruction Defend Exploit	Information, Computers, Computer Networks	*Unspecified*	*Unspecified*	*Unspecified*
Arquilla & Ronfeldt (1993):	*Unspecified*	*Unspecified*	Coercive/ Offensive	Disruption, Destruction	Information Communication Systems	Information Superiority	Unspecified Adversary	*Unspecified*

Through population of the model, the underlying structure of each definition becomes apparent. No one definition contains entries in every category; however, the collective application of the definitions results in each category being populated with at least one value. Notably, each definition specifies intent and effects. Crucially, the absence of a structural component within a definition does not lessen the model's explanative power regarding the structural components that are present within a definition.

Such a structural view of definitions provides another means to consider the relationships between the definitions. Definitions that specify the same number of structural components as one another can be understood to have a relationship characterised by a high degree of structural consistency. Conversely, definitions that have considerable divergence in definitional components have a relationship characterised by structural inconsistency.

To further explore the model's explanative utility, the model was next populated with all the explicit definitions of cyber war and cyber warfare that were analysed under the discourse hierarchy of definitions presented in Chapter Four – a total of 43 definitions.

Table 11. Number of Structural Definition Model Components in Definitions of Cyber War and Cyber Warfare

Number of Structural Model Definition Components Present	Number of Definitions (out of 43)	Percentage of Total Definitions
8	2	4.65%
7	0	0.00%
6	10	23.26%
5	12	27.91%
4	9	20.93%
3	8	18.60%
2	2	4.65%
1	0	0.00%

Table 11 shows the number of components of the structural definition model that are present in individual definitions. The data shows that most definitions include between four and six components of the structural definition model. The median number of components in a definition was five, and the average was 5.375. This demonstrates that (a) the model has explanative power regarding the structure of the majority of definitions; and (b) the encountered definitions have a considerable degree of variance in their complexity and comprehensiveness.

Table 12. Prevalence of Structural Model Components in Definitions of Cyber War and Cyber Warfare

Model Definition Component	Number of Definitions Including Component	Percentage of Definitions Including Component
Actor	18	41.86%
Means	36	83.72%
Intent	43	100.00%
Effect	29	67.44%
Target	29	67.44%
Objective	19	44.49%
Target Actor	11	25.58%
Political End	13	30.23%

Table 12 captures the prevalence of the specific components of the model in each of the definitions analysed. It demonstrates that Means, Intent, Effect and Target are the most common components found in the definitions of cyber war and cyber warfare, while Target Actor and Political End were the least common.

Definitional Spectrums

The population of the structural definition model with each explicit definition encountered in the sample allows the construction of what the author has labelled 'definitional spectrums' – one for each of the eight components of the model. The analysis of each definitional spectrum allows for two crucial outputs to be identified; a *foundational definitional component* of cyber war and cyber warfare, and key areas of *inter-definitional conflict*. A schematic representation of the definitional spectrums and their relationship to the structural definition model, foundational definitional components and inter-definitional conflict, is provided in Figure 4, overleaf.

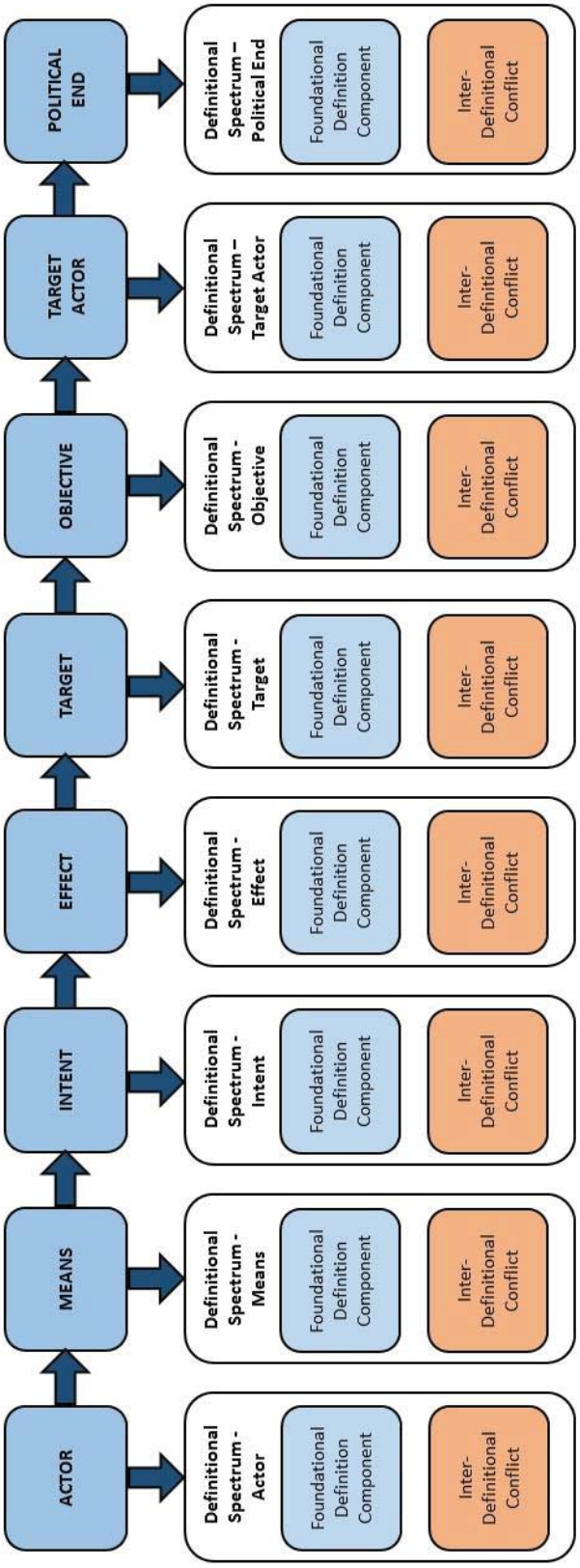

Figure 4. Analysis of definitional spectrums

A foundational definitional component is the attribute or value that has the greatest power to contextualise and explain the complete spectrum of responses encountered under each component of the model. Foundational definitional components should be understood as unifying. They are an attempt to represent the *majority* opinion of the discourse as it relates to a particular definitional component.

Foundational definitional components, however, should not be understood as final, or absolute. Previous chapters have shown the degree to which definitions are inconsistent on the attributes that should be attributed to cyber war or cyber warfare. Accordingly, in many definitional spectrums there is what, for the purposes of this analysis, has been labelled as inter-definitional conflict. Inter-definitional conflict occurs when there is divergence between a foundational definitional component, representing the majority opinion of the discourse, and a minority within the discourse that have dissenting views on how a definitional component should be represented. This is not to say that it was the intent of those who authored definitions for their definitions to be in competition in conflict with other definitions. Rather the inter-definitional conflict referred to is a representation by the author of the inconsistencies between definitions within the discourse.

Inter-definitional conflict is recorded and analysed when one of three conditions are met:

1. When there is irreconcilable disagreement between definitions concerning a property of cyber war or cyber warfare;
2. Where a majority of definitions attribute a specific property to cyber war or cyber warfare that is different to, but can be subsumed under the property identified as the foundational definitional component; and
3. Where less than one third of the encountered definitions specify a particular component of the structural definition model, thus challenging the applicability and relevance of that component.

Definitional Spectrum: 'Actor'

There were 18 definitions that specified Actor as a definitional component. A consolidated list of the actors that were specified in explicit definitions encountered in the sample is shown in Table 13.

Table 13. Actors Identified in Definitions of Cyber War and Cyber Warfare

Actor	Number of Definitions
Actor with a command structure and political or military goals	1
Groups with the expertise and resources to mount a significant attack	1
Nation states	7
Nation state & non-state actors	3
Nation state endorsed actor	2
Nation states, agents of states, non-state actors and groups	2
Political actors	2
Total	**18**

The majority of actors identified are either nation states, or are primarily constituted by their relationship to a nation state. Accordingly, it is proposed that the Actor definitional spectrum is organised according to the cohesiveness and power of a political actor. At the lower end of the spectrum, actors identified in the definitions include non-state actors (Solis, 2014; Hughes, 2010), actors with a command structure and political or military goals (Dipert, 2013), and actors with the expertise and resources to mount a significant attack (Danks & Danks, 2013). The mid-point of the spectrum is represented by definitions that identified state-sponsored organisations (Raboin, 2011; Solis, 2013), while the high end of the spectrum is represented by definitions that identified nation-states as the primary initiating actor in cyber war or cyber warfare (Clarke & Knake, 2011; Nicholson et al., 2012; Schapp, 2009; Droege, 2012; Hunker, 2010). A visual representation of the Actor spectrum is shown in Figure 5.

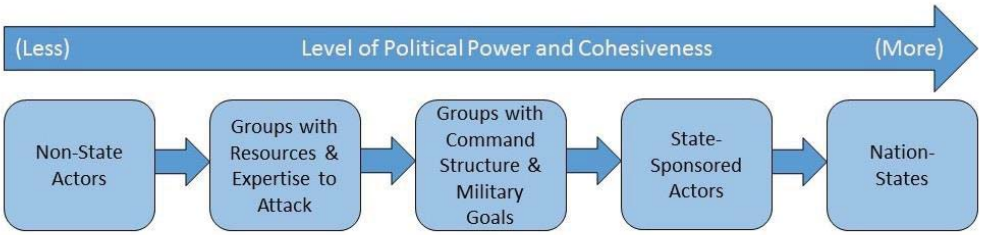

Figure 5. Definitional spectrum – 'Actor'

Based on this analysis, the foundational definitional component of the Actor spectrum is *political actor*. This is justified by the observation that all of these definitions that specified the Actor component were consistent in that they identified cyber war or cyber warfare as something that is initiated by some form of political actor. Furthermore, there is inter-definitional conflict within the Actor spectrum on whether Actor is required to be a nation state. While the concept of nation state can be subsumed under that of political actor, seven definitions specified that Actor must be a nation state. In addition, four definitions specified that Actor should either be a nation state or a group constituted by its relationship to a nation state – for example a state-sponsored group or a state agent.

Definitional Spectrum: 'Means'

Means was the second most common component of the structural definitional model present in the encountered definitions. Over 80% of the definitions specified this component in their conception of cyber war or cyber warfare. A consolidated list of the means specified in explicit definitions encountered in the sample is presented in Table 14.

Table 14. Cyber Means Identified in Definitions of Cyber War and Cyber Warfare

Means	Number of Definitions
Computer networks	14
Cyber actions/operations/techniques/means/capabilities	8
Cyber attack	4
ICTs	2
Cyber and electronic weapons	2
Actions executed against software controlling processes	1
Information operations	1
Malicious code	1
Non-kinetic actions	1
Systematic use of information	1
Virtual application of force	1
Total	36

In the analysed definitions, means are consistently described using expansive terms that encompassed a broad range of activities. Cyber actions, operations, techniques, means and capabilities are broad enough terms that nearly any cyber activity could be categorised under them. Information operations, non-kinetic actions and the systematic use of information share this characteristic. Cyber attack and the virtual application of force are slightly more restrictive, but nonetheless provide for the description of a broad array of cyber activities. The only exception is the means of 'malicious code', which can be subsumed under any of the other means identified.

While 'computer networks' was the most commonly identified Means encountered, it has significant deficiencies in its explanative power. As stated by Dipert (2013), significant cyber effects can be achieved using Other Than Internet (OTI) means, such as the exploitation of portable media or certain uses of electromagnetic radiation (Dipert, 2013). The evolution of the DoD concept of CNO to CO, as discussed in Chapter Four, is considered as further evidence of insufficiencies of using computer networks as a primary explanatory example of cyber means.

In consideration of the above, no organising principle of the Means definitional spectrum is apparent. All the definitions that include this component are similar in that they specify Means as some form of cyber, computer or network based activity. Accordingly, it is proposed that the foundational definitional component of the Means spectrum can be represented by any suitably inclusive term that indicates that the Means in question are cyber-enabled. For simplicity, the term *cyber means* is offered as a suitable term. In accordance with this analysis it is proposed that there is no inter-definitional conflict within the Means definitional spectrum. Instead, the disagreement in the discourse regarding the means of cyber war or cyber warfare appears superficial and largely lexical.

Definitional Spectrum: 'Intent'

The definitional spectrum for Intent was unique in that every explicit definition encountered in the sample ascribed one or more types of intent to cyber war or cyber warfare. As shown in Table 15, three types of intent were identified: coercive, defensive and exploitive.

Table 15. Intent Identified in Definitions of Cyber War and Cyber Warfare

Intent	Number of Definitions	Percentage of Definitions
Coercive	43	100.00%
Defensive	16	37.21%
Exploitive	4	9.30%

Based on the material examined, offensive intent was regarded as equivalent to coercive intent; every offensive action, whether conducted at a tactical, operational or strategic level, seeks to coerce an adversary. All the definitions encountered associated a coercive intent to cyber war or cyber warfare. Sixteen definitions also identified a defensive intent, while four definitions also identified an exploitive intent.

To complement Table 15, Table 16 illustrates the number of definitions that identified multiple intents. It demonstrates that definitions with multiple intents always include coercive and

defensive as the primary intents associated with cyber war and cyber warfare. In addition, four definitions also associated cyber war and cyber warfare with an exploitive intent.

Table 16. Groupings of Intent Identified in Definitions of Cyber War and Cyber Warfare

Intent	Number of Definitions
Coercive	27
Coercive & Defensive	12
Coercive, Defensive, & Exploitive	4
Total	43

Exploitation in the cyber realm is closely linked to espionage, with some authors equating CNE with cyber espionage (Roscini, 2010; Lobel, 2011). An alternative conception of exploitive intent is provided in Applegate's conception of 'exploitive manoeuvre', which he identifies as a basic form of offensive cyber manoeuvre. He defines exploitive manoeuvre as 'the process of capturing information resources in order to gain a strategic, operational or tactical competitive advantage' (Applegate, 2012). Both conceptions of exploitive intent allow it to be considered as a coercive or a defensive activity, depending on the objectives of the exploiting agent.

In consideration of the above, three propositions are offered regarding the Intent definitional spectrum. The first proposition is that the spectrum is organised according to the degree of coercive intent motivating a cyber action. As shown in Figure 5, defensive intent is at the low end of the spectrum. Exploitive intent, which can be either defensive or coercive in nature, depending on the objective of exploitive activities, sits at the midpoint of the spectrum. Coercive intent is established at the high end of the spectrum.

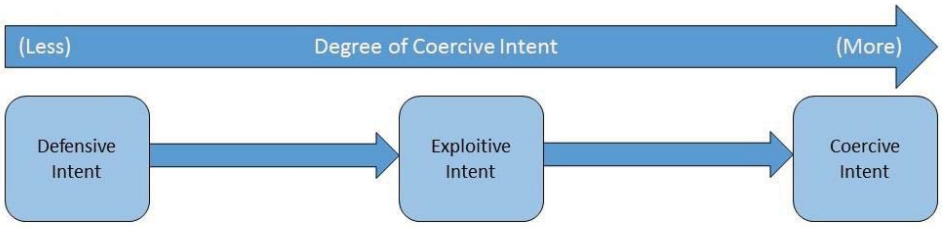

Figure 6. Definitional spectrum – 'Intent'

The second proposition is that the foundational definitional component of the Intent spectrum is *coercive*. This choice was justified due to the presence of coercive or offensive intent in every definition of cyber war and cyber warfare encountered. It was unclear from the discourse whether defensive intent was a necessary component of a definition of cyber war or cyber warfare; less than 40% of the definitions specified defensive intent. It can be argued, however, that defensive intent is a crucial component of a definition of cyber war or cyber warfare. Any action motivated by coercive intent may be met by an action driven by defensive intent, and both actions form part of the same cyber war event. However, there is no necessity that demands that coercive intent must be met with defensive intent; rather, a targeted actor may respond with a coercive action of their own, or not respond at all. The inclusion of exploitive intent can also be contested. While it was present in less than 10% of definitions, the close relationship of exploitive intent to both defensive and coercive intent suggests that further consideration of its relevance to the definitions of cyber war and cyber warfare is warranted. Accordingly, the third proposition arising from analysis of the Intent spectrum is that there is inter-definitional conflict in the Intent definitional spectrum concerning the status of defensive and exploitive intent.

Definitional Spectrum: 'Effect'

Effect(s) was one of the most commonly encountered components of the structural definition model, present in 29 out of 43 definitions. Single definitions identified multiple effects, resulting in a broad array of effects varying in severity from defacement to casualties. A

consolidated list of Effect(s) specified in explicit definitions encountered in the sample is presented in Table 17.

Table 17. Effects Identified in Definitions of Cyber War and Cyber Warfare

Effect	Times Mentioned in Definitions
Defacement	1
Disruption	19
Denial	4
Degradation	11
Manipulation	8
Damage	3
Destruction	15
Amplify kinetic violence	1
Use of force	3
Potentially lethal effects	1
Major kinetic violence	1
Armed attack	2
Casualties	1

This suggests that the Effect(s) spectrum is organised according to the degree of violence inherent in an effect. This is illustrated in Figure 7.

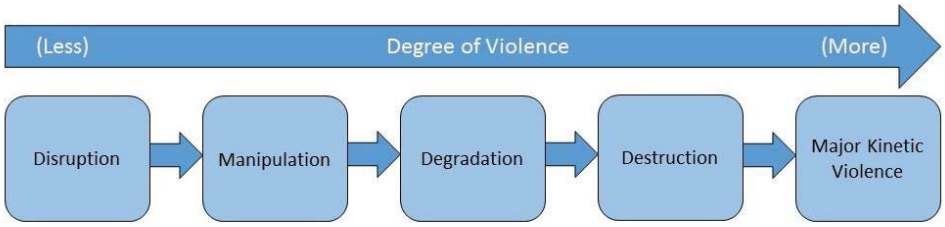

Figure 7. Definitional spectrum –'Effects'

Figure 7 does not, however, capture the full complexity of the Effect(s) encountered in definitions of cyber war and cyber warfare. It is the author's considered view that there are

two categories of effects present in the definitions – primary effects, which have a direct effect on a target, and cascading effects, which are the result of the interaction of a primary effect and a specific target. Out of the effects identified in the definitions, defacement, disruption, denial, degradation, manipulation, damage and destruction are considered as primary effects. The amplification of kinetic violence, use of force, potentially lethal effects, major kinetic violence, armed attack and casualties are considered as cascading effects.

It is important to maintain a distinction between cascading effects and objectives. Cascading effects are rarely objectives in themselves; political actors seldom seek violence as an end in itself. Instead, as articulated in the structural definition model, the application of violence is directed towards an objective, which in turn contributes to or achieves a political end. Nor does the discourse provide sufficient evidence to conclude that a definition of cyber war must include consideration of both primary and cascading effects. Indeed, a considerable majority of the definitions encountered include primary, rather than cascading effects, in their conception of cyber war or cyber warfare.

While numerically small, the number of definitions that focus on cascading effects have had considerable influence within the discourse. For example, two of the five core definitions identified –Rid (2012) and Nye (2011) – emphasise cascading rather than primary effects in their definitions. These definitions insist that the primary effect of kinetic destruction creates a 'threshold of violence' that must be reached before a cyber event can properly be considered as cyber war or cyber warfare. In the case of Rid, his insistence on this threshold can be traced to his utilisation of Clausewitz's conception of war, namely as something that is essentially violent. The mantra that violence is a necessary condition of cyber war and cyber warfare is also found in the works of Dinstein (2013), Stone (2013) and Lewis (2011). When considered against the entirety of the discourse, however, these are minority opinions. Accordingly, it is proposed that primary effects form the basis for the foundational definitional component of the Effect(s) spectrum. Due to the prevalence with which they are encountered in the definitions (as shown in Table 17), it is argued that the most appropriate effects to represent

the foundational definitional component are *disruption, manipulation, degradation and destruction*.

Importantly, definitions that do not directly reference cascading effects do not exclude cascading effects, such as major kinetic violence, from their scope. Disruption, manipulation, degradation and destruction can cause or amplify major kinetic violence when applied to a susceptible target under the right conditions. In consideration, however, of the influence of dissenting opinion, it is recognised that there is inter-definitional conflict within the Effect(s) spectrum regarding whether the effects of cyber war or cyber warfare must be equivalent to major kinetic violence.

Definitional Spectrum: 'Target'

Target was another commonly utilised component of the structural definition model. Like Effect(s), it was encountered in 29 out of 43 definitions. Several definitions identified multiple targets; a consolidated list of the targets specified in the explicit definitions encountered in the sample is shown in Table 18.

Table 18. Targets Identified in Definitions of Cyber War and Cyber Warfare

Target	Number of Times Mentioned in Definitions
Computers & Computer Networks	31
Information	14
Information Based Processes/Systems	6
Military Targets	5
Infrastructure	4
Communication Systems	2
Cyber Controlled Objects	1

The dominant targets identified were:

- Computers and computer networks;
- Information, information based processes and systems;

- Military targets and infrastructure.

These targets can be rationalised into three categories:

- Information;
- Information based systems and processes; and
- Cyber controlled objects.

Information based systems and processes are considered an appropriate parent category for computers, computer networks and computer systems. These objects are all constituted through an interaction of the virtual (information) with the physical (hardware). Considering the potential reach of cyber effects, sole reference to computers and computer networks is regarded as unnecessarily restrictive in the consideration of targets of cyber war and cyber warfare. The category of cyber-controlled objects has similar utility, it is sufficiently expansive to encompass the wide array of potential targets, including but not limited to critical infrastructure and military hardware.

Based on this analysis, the organising principle for the definitional spectrum of Target is the degree of physicality that a target possesses. This is illustrated in Figure 8. On the far end of the spectrum is information, which in the cyber realm is purely virtual. The mid-point of the spectrum is information-based systems and processes, comprising both virtual information and physical hardware. The far end of the spectrum is cyber controlled objects – objects in the kinetic domain controlled by cyber means.

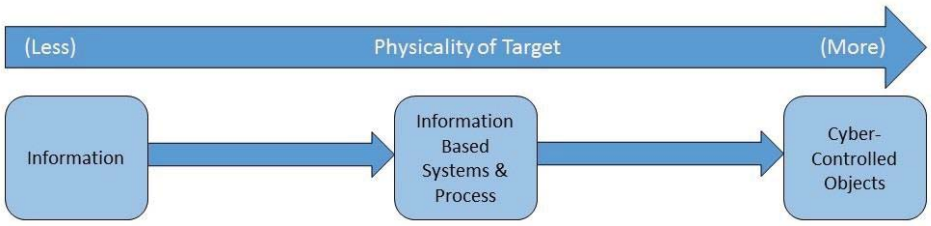

Figure 8. Definitional spectrum – 'Targets'

In alignment with Figure 8, the foundational definitional component for the Target spectrum is *information, information based systems and processes, and cyber-controlled objects*. This judgement is based on the ability of these categories to represent all of the individual targets specified in the encountered definitions. Thus, there is no inter-definitional conflict within the Target definitional spectrum.

Definitional Spectrum: Objective

Less than half of the encountered definitions specified objectives in their articulation of cyber war or cyber warfare. Out of those 21 definitions, however, the majority listed multiple objectives towards which cyber war or cyber warfare activities could be orientated. A consolidated list of the objectives specified in the explicit definitions encountered in the sample is captured in Table 19.

Table 19. Objectives Identified in Definitions of Cyber War and Cyber Warfare

Objective	Number of Times Mentioned in Definitions
Achieve tactical and strategic effect	1
Affect adversary will	1
Defend networks	4
Deny freedom of movement in cyberspace	1
Detect, deny, deter, defeat enemies	1
Deter information attacks	1
Disrupt communications	1
Disrupt infrastructure	1
Disrupt offensive capability	1
Enable operations	1
Frame actor	1
Further combat performance	1
Information superiority	3
Intelligence	2
Instrumental objective	1
Military defence	1
Prevent aggression	1
Reduce enemy defensive capability	2
Support defensive military strategy	1
Support offensive military strategy	2
Take control of enemy resources	1
Unspecified military objectives	1

What is first evident is the number and extent of the identified targets. There are objectives that are limited to a combination of effects and targets – for example disrupt communications or defend networks. More important is the scope of the identified objectives; objectives such as the support of offensive or defensive military strategy, enabling operations or achieving information superiority have the potential to encompass a vast number of interrelated sub-objectives. Moreover, many of the identified objectives, depending on context and application, are understood by the author to operate across the multiple levels of war i.e. strategic, operational and tactical. This phenomenon is represented in Table 20, with a preliminary interpretation of which levels of war the identified objectives are most closely linked with.

Table 20. Cyber War and Cyber Warfare Objectives Related to Levels of War[8]

Objective	Tactical	Operational	Strategic
Achieve tactical and strategic effect	✓	✓	✓
Affect adversary will		✓	✓
Defend networks	✓	✓	
Deny freedom of movement in cyberspace	✓	✓	
Detect, deny, deter, defeat enemies	✓	✓	✓
Deter information attacks		✓	✓
Disrupt communications	✓	✓	
Disrupt infrastructure	✓	✓	
Disrupt offensive capability	✓	✓	
Enable operations	✓	✓	
Frame actor			✓
Further combat performance	✓	✓	
Information superiority		✓	✓
Intelligence	✓	✓	
Instrumental objective			✓
Military defence	✓	✓	
Prevent aggression		✓	✓
Reduce enemy defensive capability	✓	✓	
Support defensive military strategy	✓	✓	
Support offensive military strategy	✓	✓	
Take control of enemy resources	✓	✓	✓

This suggests that the Objective spectrum is organised according to the level of warfare – whether an objective is most appropriately categorised as a tactical, operational or strategic. This is illustrated in Figure 9.

[8] The analysis has been conducted on the basis that, while any tactical or operational action may be linked to strategic intent, many tactical and operational actions are not inherently strategic and should not be identified as such.

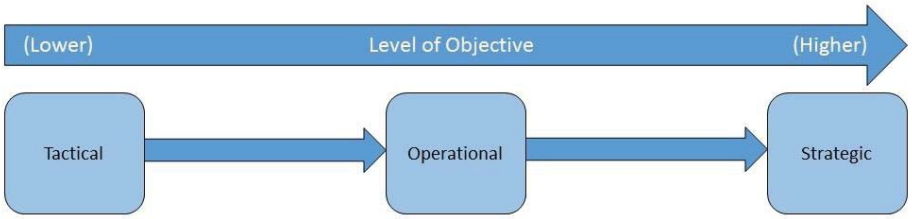

Figure 9: Definitional spectrum – 'Objective'

While objectives can function across multiple levels, empirical examples of the objectives of cyber war or cyber warfare will be subject to an additional level of specificity, allowing better categorisation as a tactical, operational or strategic objective. Thus, categorising objectives according to whether they are tactical, operational or strategic is both representative of the discourse and provides sufficient explanative flexibility to encompass the wide array of objectives sought in cyber war or cyber warfare. Accordingly, the foundational definitional component for the Objective spectrum is *tactical, operational and strategic objectives*. As these concepts are sufficiently broad to encompass all of the objectives encountered in the definitions, there is no inter-definitional conflict within the Objective definitional spectrum.

Definitional Spectrum: Target Actor

Expectedly, the definitional spectrum for Target Actor is similar to that of (initiating) Actor. All the definitions included in this component identified some form of political agent as a target actor, with nation state as the dominant response. A list of the target actors specified in explicit definitions encountered in the sample is presented in Table 21.

Table 21. Target Actors Identified in Definitions of Cyber War and Cyber Warfare

Target Actor	Number of Definitions
Actor with a command structure and political or military goals	1
Nation states	7
Nation state and non-state actors	1
Unspecified adversary	1
Political actors	2
Unspecified	31
Total	**43**

Based on analysis of this information and its correspondence with the (initiating) Actor spectrum, the definitional spectrum for Target Actor is organised according to the power and cohesiveness of the political actor, as shown in Figure 10.

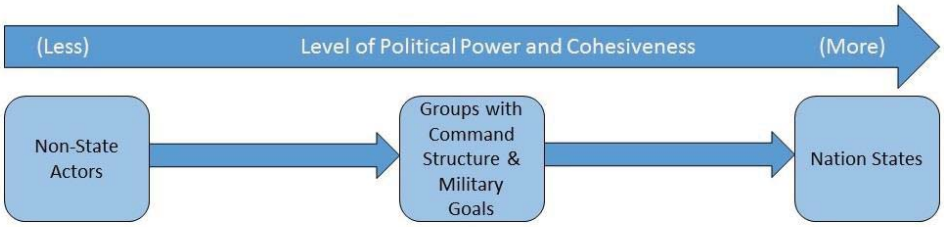

Figure 10. Definitional Spectrum – 'Target Actor'

Furthermore, as per the (initiating) Actor spectrum, the foundational definitional component for the Target Actor spectrum is *political actor*. It is relevant, however, to note that there were noticeably fewer definitions specifying a Target Actor (11/43) than there were definitions specifying an (initiating) Actor (18/43), and less than one third of the definitions specified a Target Actor. In addition, as per the analysis of the (initiating) Actor spectrum, there was a prevalence of definitions that maintained that the Target Actor must be a nation state. Accordingly, there is inter-definitional conflict within the Target Actor definitional spectrum regarding both these points.

Definitional Spectrum: Political End

The final component of the structural definitional model is Political End. This was the second least utilised component, with 13 out of 43 definitions specifying it in their conception of cyber war or cyber warfare. The Political Ends specified in the explicit definitions encountered in the sample are presented in Table 22.

Table 22. Political Ends Identified in Definitions of Cyber War and Cyber Warfare

Political End	Number of Definitions
Achieve desired end	1
Achieve political gain	1
Change or preserve a political status quo	1
Extract political concessions	1
Fulfil national will	1
Further social, ideological, religious, political or similar objectives	1
Unspecified political end	7
No political end specified	30
Total	**43**

All the definitions specifying this component used slight lexical variations of the concept of political end. This leads to the conclusion that the specification of a specific political end is not relevant in a definition of cyber war or cyber warfare. Rather, what is important in the definition is the presence or absence of a non-specific political end towards which the cyber war or cyber warfare is orientated.

Therefore, no organising principle was identified for the definitional spectrum of Political End. All the definitions encountered specified variations, rather than progressions of the concept of political end. Following this observation to its conclusion, the foundational definitional component of the Political End spectrum can be represented by any articulation of the concept of political end. To align with the structural definition model, *political end* is proposed as a suitable term. However, as less than one third of the definitions specified a Political End, there

is inter-definitional conflict within the spectrum as to whether Political End is an essential component of a definition of cyber war or cyber warfare.

A Foundational Definition

The results of the analysis of all the definitional spectrums can now be presented in Table 23.

Table 23. Summary of Analysis – Definitional Spectrums

Structural Model Component	Foundational Definitional Component	Inter-Definitional Conflict
Actor	Political Actor	- Whether Actor must be nation state
Means	Cyber Means	- No significant conflict
Intent	Coercive	- Inclusion of defensive and exploitive intent
Effect	Disrupt, manipulate, degrade, destroy	- Effect must be equivalent to major kinetic violence
Target	Information, information based processes, cyber controlled objects	- No significant conflict
Objective	Tactical, operational, strategic	- No significant conflict
Target Actor	Political Actor	- Target Actor as a necessary component of a definition. - Whether Target Actor must be nation state
Political End	Political End	- Political end as a necessary component of a definition.

The analysis of the definitional spectrums allows the presentation of a foundational definition of cyber war and cyber warfare, comprising the foundational definitional components identified above. This definition is as follows:

Cyber war or cyber warfare is initiated by a political actor using cyber means with a coercive intent through the disruption, manipulation, degradation or destruction of information, information based systems and processes, or cyber controlled objects to achieve tactical, operational or strategic objectives against a political actor in order to achieve a political end.

In part this definition is considered foundational in that it both represents and is consistent with the majority opinion of cyber war and cyber warfare definitions present in the discourse. Equally, its ability to also act as a foundational definition is provided through its adherence to the structural form of Actor, Means, Intent, Effect, Target, Objective, Target Actor, Political End and the componentised comparative analysis this structure allows. It is this component-by-component analysis that allows the points of conflict between the definitions to be articulated. The identification of these points of contention – whether actors must be nation states; whether exploitive and defensive intent fall within the scope of cyber war or cyber warfare; whether effects must have results comparable to major kinetic violence; and whether target actors and political ends are necessary components of definitions – are crucial. It is when both these outputs are considered together that the definition truly becomes foundational, in that the implications for policy, doctrine and strategy arising from both majority and dissenting perspectives can be captured and analysed.

Conclusions

Based on the consistency with which the five core definitions identified in Chapter Four can be applied to a hypothetical cyber event, a structural definition model of definitions of cyber war and cyber warfare was created. The applicability of the model to definitions encountered in the discourse was evidenced by quantitative analysis demonstrating how the components of the model are broadly and consistently used in the explicit definitions of cyber war and cyber warfare identified in the sample. The utility of the model was demonstrated by its ability to allow for the identification and analysis of definitional spectrums for each component of the structural definition model. This enabled comparative analysis between the explicit definitions encountered in the sample at a structural level. This analysis identified a foundational definition of cyber war and cyber warfare, presented as a comprehensive, reconciliatory definition which best represents the discourse. Importantly, it also allowed the author to identify areas where inconsistency between the definitions is most evident. Full

consideration of the implications and applications of the output of the structural definition model are presented in Chapter Six: Structural Definitions – Applications and Future Research.

Chapter Six: Structural Definitions – Applications and Future Research

In Chapter Five, the author constructed a structural definition model and used it as a basis to conduct comparative analysis of the components which comprise definitions of cyber war and cyber warfare. The key outputs from this process were the identification of definitional spectrums for each structural component, the construction of a foundational definition of cyber warfare, along with the identification of those components where there is 'inter-definitional conflict' - significant disagreement between definitions. Together, these outputs are a representation of the discourse of cyber war and cyber warfare. A schematic representation is provided overleaf in Figure 11.

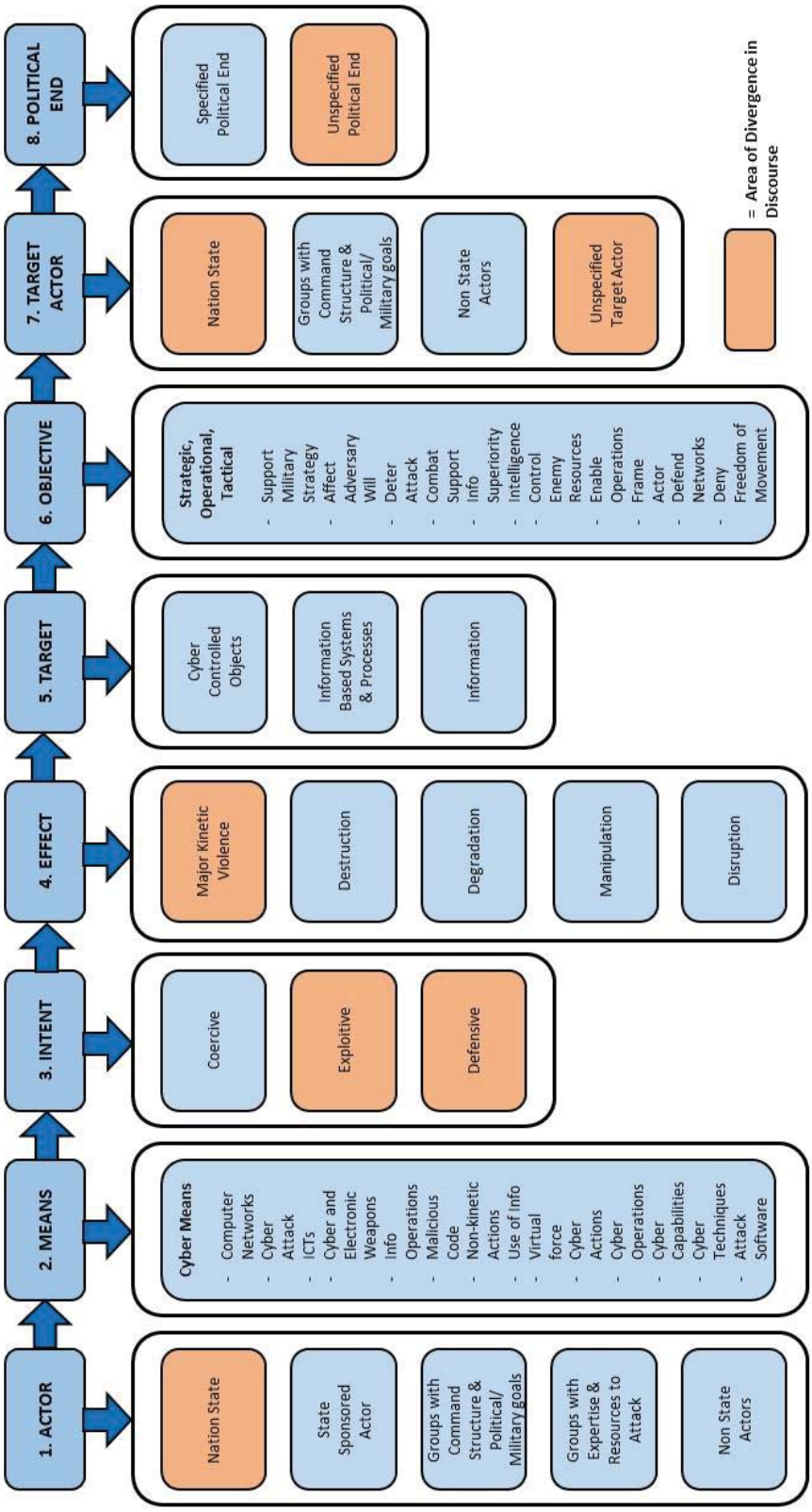

Figure 11. The discourse of cyber war and cyber warfare definitions

In Figure 11 the underlying structure common to the definitions across the discourse is demonstrated by the top row, which sets out each constitutive component of the structural definition model. A summary of each definitional spectrum is also presented, which allows a researcher to better understand the range of responses encountered in the definitions under each component of the structural definition model. A consolidated list of values encountered in the definitions is presented for each spectrum, along with the identification of areas where the inter-definitional disagreement is strongest (dark shaded areas). As detailed in Chapter Five, this information provides the basis for a foundational definition of cyber war and cyber warfare. The foundational definition, along with its relation to the structural definition model, is presented overleaf in Figure 12.

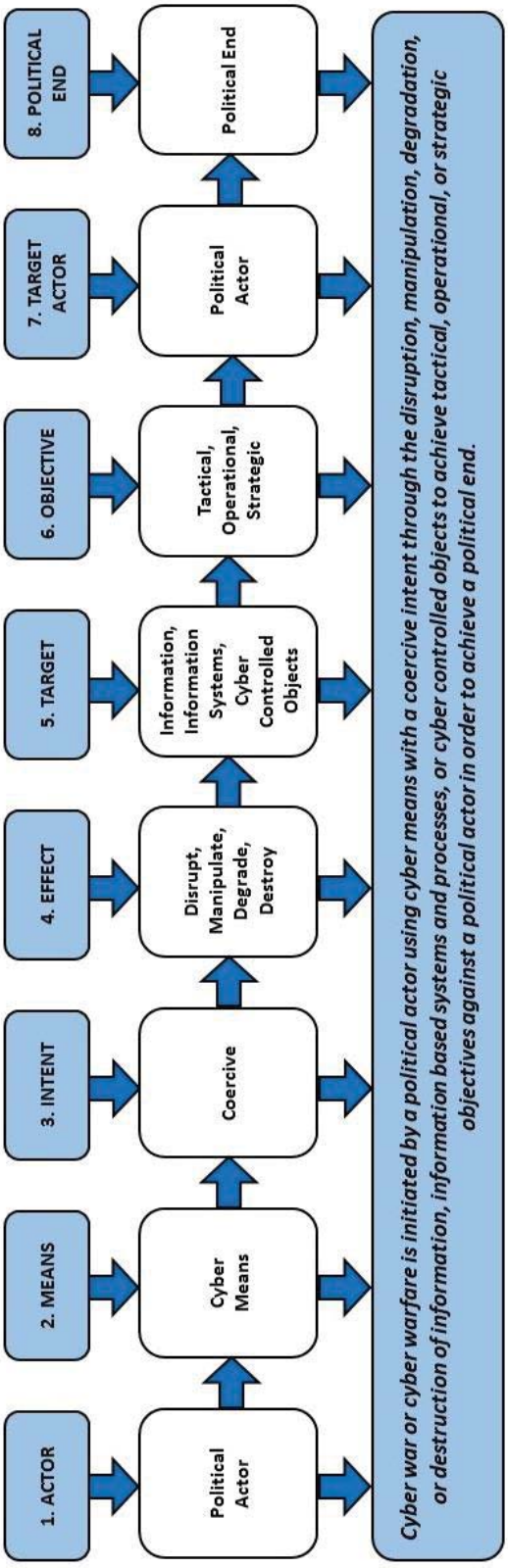

Figure 12. Illustration of the foundational definition of cyber war and cyber warfare

Applications

The output of the analysis conducted in Chapter Five (illustrated in Figures 11 and 12) has several immediate applications. One such application is the construction of a discourse-driven taxonomy of definitions of cyber war and cyber warfare. Another application is to act as a basis for the formulation of alternative definitions, which either emerge in response to new developments, or are tailored to represent the perspective or interests of a particular actor. Alternative definitions constructed in this manner may vary from the foundational definition offered above, but will possess the same underlying structural components. This not only allows for more effective comparative analysis between definitions, but provides the basis for future reconciliation in the discourse. This reconciliation may be provided for by the nature of the structural definition model; its ultimate concern is with the structural components of the definitions; thus, it retains its integrity even if the values that represent each structural component change. This provides the model with the potential to retain its utility even if the discourse of cyber war and cyber warfare definitions changes substantially. A more detailed consideration of each of these applications is presented below.

A Discourse Taxonomy

To the best of the author's knowledge, a taxonomy of definitions of cyber war and cyber warfare has yet to be created. Such a taxonomy can provide a means to conceptualise the characteristics of the definitions of cyber war and cyber warfare, as well as to contextualise individual definitions. By repurposing the results of the analysis supporting the structural definition model, the foundations of such a taxonomy can be created. Like the foundational definition of cyber war and cyber warfare, a discourse-driven taxonomy of cyber war and cyber warfare definitions is constructed through comparative analysis of the explicit definitions encountered in the sample, considered through the lens of the definitional components of the structural definition model. An initial discourse taxonomy of cyber war and cyber warfare definitions is presented overleaf in Figures 13 and 14.

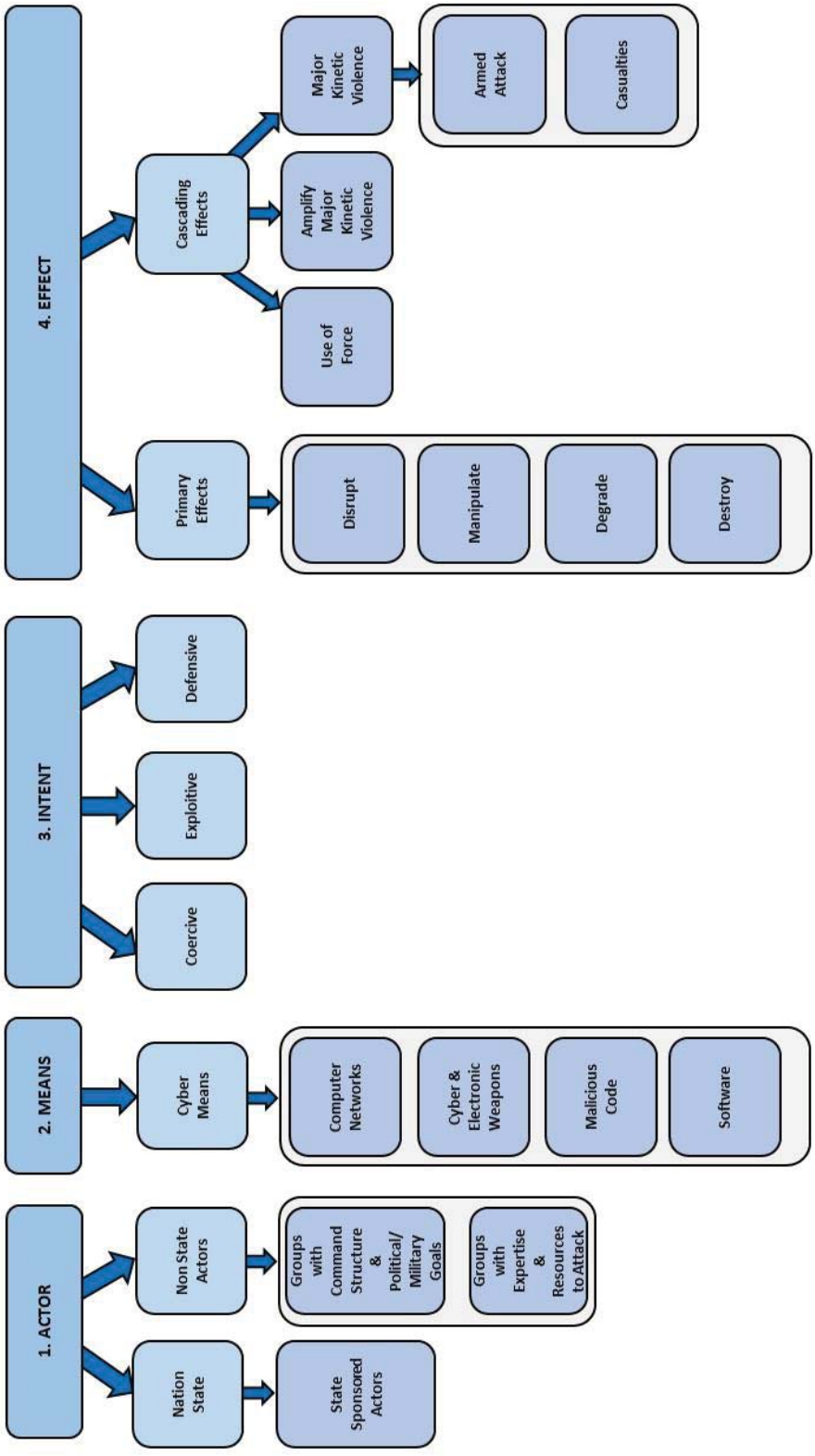

Figure 13. Taxonomy of cyber war and cyber warfare definitions – part one

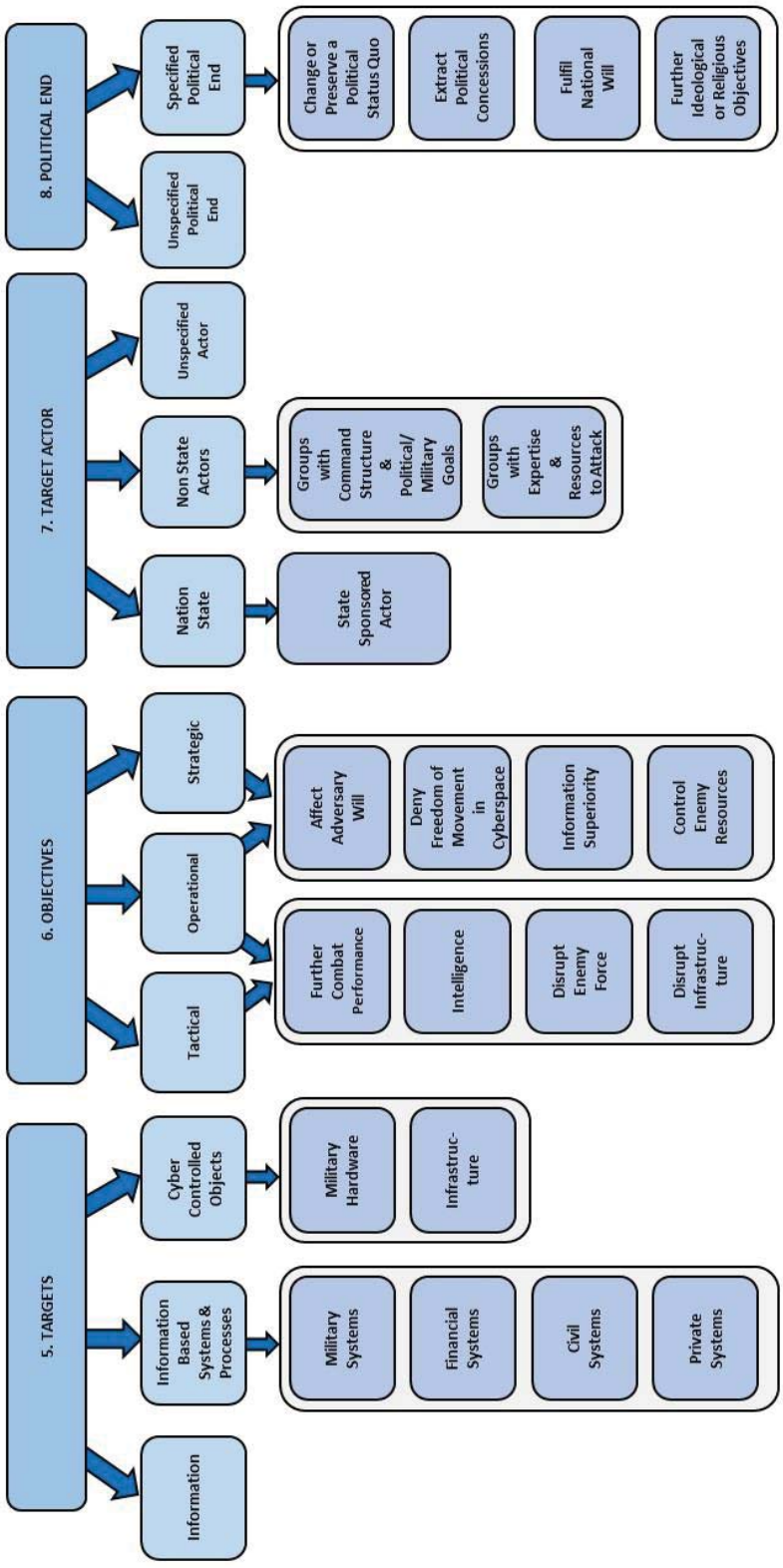

Figure 14. Taxonomy of cyber war and cyber warfare definitions – part two

Working horizontally along the model it is possible to contextualise a particular definition within the discourse by identifying which components of the taxonomy it features. It also provides another means of viewing the definitional spectrums associated with the structural definition model; instead of being represented on a continuum, spectrums are now represented by category. The categories were created based on the collective analysis of the explicit definitions according to the structural definition model, and present information extracted directly from the text of the relevant definitions. The taxonomy is presented as foundational, rather than complete. More nuance and complexity is possible through a more in-depth examination and analysis of the definitions that form its basis, as well as by incorporating any definitions and major developments not captured in the sample. However, even at this initial stage, the taxonomy provides an alternative visual representation of the structure of and relationships between the definitions, as well as how the structural definition model can be further applied to increase definitional clarity.

Constructing Definitions

Based on the analysis conducted in Chapter Five, the author constructed a foundational definition of cyber war and cyber warfare, which was presented alongside the key points of inter-definitional divergence. However, using the form provided by the structural definition model, alternative but structurally consistent definitions can easily be composed. If the foundational definition can be considered an *inclusive* definition, in that it is representative of the majority of the discourse, it is possible to form an alternative *exclusive* definition, which captures the highest thresholds that different researchers have assigned to each definitional component. Based on the definitions encountered in the sample, an exclusive definition of cyber war and cyber warfare is presented in Figure 15.

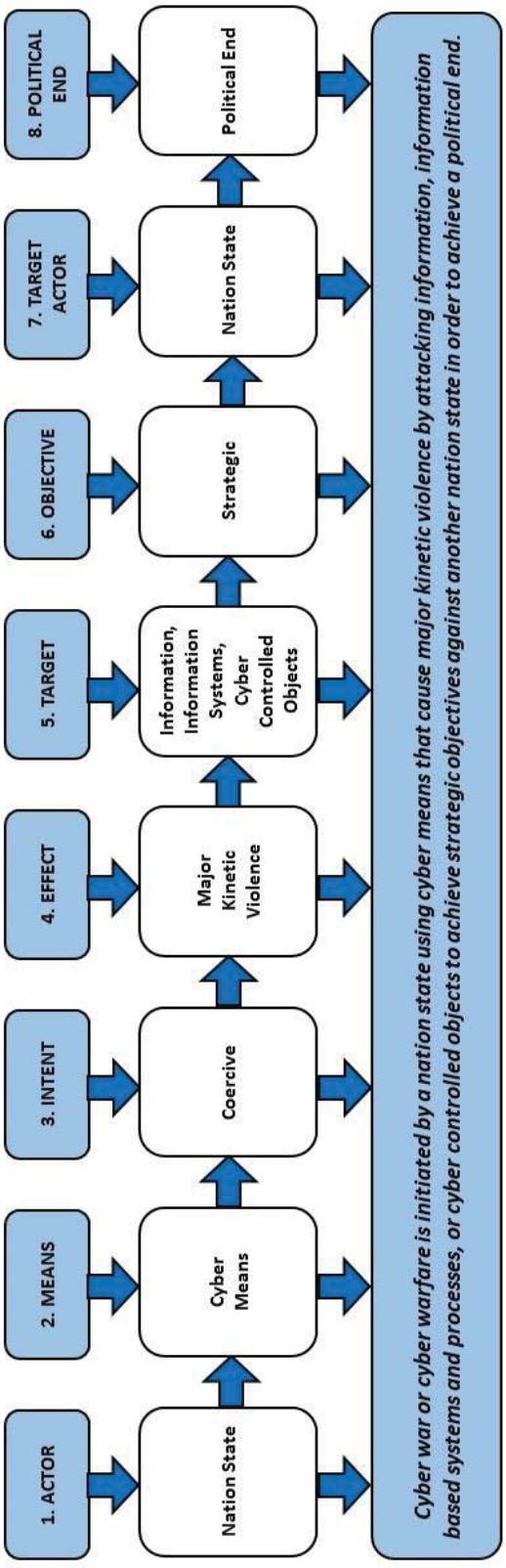

Figure 15. Definition of cyber war and cyber warfare – exclusive

The exclusive definition presented above differs from the foundational definition in its presentation of Actor, Effect, Objective and Target Actor. In the exclusive definition, each of these components is represented by the most exclusive value encountered in the explicit definitions. For example, by specifying that Actor and Target Actor must be nation states, the definition excludes any cyber aggression perpetrated by or against sub-state groups. Similarly, by specifying that Effect must be of a major kinetic violent nature, the definition excludes any cyber aggression that does not reach this threshold from the scope of cyber war or cyber warfare.

The exclusive definition presented above demonstrates the ease with which the values that represent each structural component can be altered without changing a definition's underlying structure. Indeed, while the current discourse of the definitions of cyber war and cyber warfare inspired the model's construction, it can be utilised without reference to the discourse at all. A researcher or practitioner may use the model to create structural components of a definition of cyber war or cyber warfare that are a result of their own independent thought, or that are representative of the expertise, interests and strategy of a particular actor, political or otherwise.

This suggests another application of the structural definition model – it can be used by a political actor, such as a nation state, to clarify or construct a formal definition which more accurately reflects their own doctrine pertaining to cyber war or cyber warfare. For example, a state's cyber doctrine may have a strong focus on military applications of cyber power that cause or amplify major kinetic violence against other states. In this situation the Actor and Target Actor of that state's definition of cyber war or cyber warfare would be nation states, and the Effect must cause or amplify major kinetic violence. Alternatively, a nation states cyber doctrine may have a strong focus on sub state actors and a broader conception of the effects that qualify as cyber war. In this case the Actor and Target Actor can include sub-state groups, and Effects may encompass disruption, manipulation, and degradation.

A related application of the model is a structural comparative analysis of any existing definitions of cyber war or cyber warfare represented in the policies of different states. Similar to the example above, if the policy of a particular state is to define Actor as a nation state, then the scope of their response to cyber war and cyber warfare is likely to differ considerably from a state whose specification of Actor includes sub-state groups. Furthermore, if a state does not have a formal definition of cyber war or warfare, then it is possible for an outside party to use the structural definition model to retroactively construct a definition that represents the relevant actions and policy of that state. This would be achieved through analysis of the actions taken by a state, a published policy, relevant investments, and consideration of the organisation and structure of relevant state agencies.

The United States provides a useful example. The Actor is a nation state – in this case the United States via the DoD. From analysis of relevant material, such as the DoD Cyber Strategy, and Joint Publication 12-R, Cyber Operations, we can deduce that a Target Actor may be a sub-state actor as well as a nation state. We can also determine that Intent can be coercive, defensive or exploitive (DoD, 2013). This is a limited analysis conducted to demonstrate a potential application of the structural definition model; however, it is proposed that a more in-depth application of this analytical method may generate information that will make a valuable contribution to the discourse.

Reconciling the Discourse

The section above explored ways in which the structural definition model can be used to construct new definitions. Reflecting on the research presented in this thesis regarding the analytical confusion caused by a multitude of inconsistent definitions, one may question whether new definitions are necessary or beneficial. It must be recognised, however, that like the discourse, definitions are not immutable. In coming years, the discourse of the definitions of cyber war and cyber warfare is likely to expand rather than contract, particularly as new cyber events occur that challenge our understanding of what cyber war or cyber warfare should signify. It is proposed, however, that the structural definition model will retain its utility with

the emergence of new definitions. Due to the ease with which the components of the model can be adjusted to represent new values, the structural definition model can be used to interrogate new definitions and link them back to the original discourse. This provides a means to quickly determine whether a recently coined definition is novel, or whether it is simply a reformulation of existing definitions. When new definitions of value do emerge, the model can be used to identify precisely how new thought challenges or refines the established definitional components of Actor, Means, Intent, Effect, Target, Objective, Target Actor and Political End. In some cases this could result in an alteration of the foundational definition of cyber war and cyber warfare presented in this thesis. For example, if a sufficiently large weight of new definitions emerges – perhaps in response to a major cyber event – that specify that Effect must cause major kinetic violence, then it would be appropriate to update the foundational definition to reflect this evolution of thought.

These potential applications underscore the value of the structural definition model as a reconciliatory tool. By providing a structural basis for new research to be reconciled with the existing discourse, the model indicates that, despite the conflict between them, current and future definitions can share a common foundation. If the commonality between the definitions can be emphasised, then points of conflict and the implications associated with them can be better understood. Having a consistent way to both represent and analyse these points of commonality and conflict can do much to aid the clarity with which the terms cyber war and cyber warfare are understood and used. By providing a consistent, structural basis for this presentation and analysis, the structural definition model provides a means to substantially increase the analytical specificity with which the terms cyber war and cyber warfare are used.

Future Research and Applications

The findings presented in this thesis suggest that the pursuit of several adjacent threads of research may yield beneficial outcomes. One approach would be to repeat the research process six months to one year after the occurrence of a major cyber event and to simultaneously increase the size of the sample. The sample could be broadened in its entirety by adding

sources such as published texts and relevant theses and dissertations. Alternatively, the sample could be broadened by using more expansive search terms such as ‘cyber weapons’, ‘cyber attack’ and ‘cyber military’, as well as searching on alternative academic search engines.

Using the results of this study as a starting point, such research could identify any shifts in the discourse that occurred since the publication of this thesis. Such shifts could be evidenced by the emergence of new influential definitions, a decline or increase in the relevance of a particular discipline, or in changes to the foundational definitional of cyber war and cyber warfare. It would also allow one of the findings of this study to be tested – that the volume of relevant publications will increase in response to a major cyber event. This approach would be strengthened by establishing a benchmark, or series of benchmarks over time. This would provide a baseline that will assist in clearly demonstrating the degree of change in the discourse.

An alternative approach may be to conduct targeted research that seeks to identify more definitions of cyber war and cyber warfare for analysis via the structural definition model. If enough new definitions can be identified then the key outputs of the model – the foundational definition and the key areas of inter-definitional conflict – may shift. Alternatively, the structural definition model may be used as a basis to consider how related terms such as ‘cyber attack’ and ‘cyber aggression’ are parsed by the model, identifying commonality and divergence in an effort to map the relationship of these terms, as they are used in the discourse, to cyber war and cyber warfare.

It may also be of benefit to analyse the context in which different definitions are offered. An examination of context as a variable may offer insight into both the purpose of definitions and the intent that led to a definition’s construction. Consideration of context, intent and purpose may be especially valuable to attempts to resolve the major inconsistencies between definitions. For example, it may be the case that major instances of divergences between definitions can be partially explained by the purpose of the organisation or individual proposing a particular definition.

As alluded to in the discussion on applications, the structural definition model can also be used to construct definitions based on the actions and policy of states and political actors, rather than on the discourse. In-depth analysis of relevant policy, action, investment and organisational responsibility across a number of different political actors may allow alternative definitions to be created that are based on the political and military strategy of major political actors, rather than on academic publications.

Of particular interest to the author is research that provides a basis for a formal delineation of meaning between cyber war and cyber warfare. The application of discourse analysis in this thesis has proven insufficient to do so, but it may be the case that analysis over a broader sample may provide more promising results. A second area that the author believes would be particularly relevant would be focused analysis on the areas where inter-definitional divergence is greatest, such as is the case of the definitional components of Actor, Target Actor and Effect. This would involve focused analysis on the implications of each representation of these components on the theory, policy and the scope of the cyber war and cyber warfare enquiry. Findings from such analysis may present valuable opportunities for these inconsistencies to be resolved, or reduced. At the very least, understanding the theoretical and practical implications of these definitional inconsistencies would be valuable in itself.

Conclusions

This chapter considered several potential applications of the structural definition model and its key outputs – the foundational definition of cyber war and cyber warfare and the areas of greatest inter-definitional divergence. One such application was the construction of a discourse-driven taxonomy of cyber war and cyber warfare definitions. While the taxonomy is nascent, it allows researchers to grasp all of the permutations of definitions present in the current discourse in a single visual presentation. Further applications have been demonstrated through the ability of the structural definition model to be used as a basis to construct new definitions that are representative of the interests and actions of a political actor.

While these definitions may vary in their representation of the definitional components, they will retain structural consistency with any other definition that was analysed according to the parameters of the structural definition model. In addition, through comparative structural analysis, the model provides the means for new definitions to be measured against the existing discourse, and their points of commonality and conflict to be clearly articulated. This highlights the reconciliatory nature of the model; it provides a structure for a unified understanding of current definitions, while simultaneously providing the means for new definitions to be enfolded into the current discourse. Importantly, in doing so it provides a structured process by which definitions, and the surrounding discourse, can evolve in response to insightful research or new developments.

Based on the findings of this thesis, this chapter also identified opportunities for future research. These include repeating this research after a major international cyber event, in an attempt to see how the discourse has shifted. Alternative research proposals could focus on further application of the structural definition model; either through analysis of more relevant definitions, consideration of ancillary terms, or construction of definitions based on the policy and actions of political actors rather than on the discourse. Additional opportunities for research also include efforts to definitively clarify the distinction between cyber war and cyber warfare, and focused analysis of the implications and possibilities for reconciliation arising from the areas of greatest inter-definitional conflict.

Conclusion

Definitions do matter. In emergent fields of study, such as that arising from the application of military power to the cyber realm, they become vital. Definitions form a foundation for consistent understanding and interpretation of events. They allow for consistency in the articulation of research, policy and objectives. As political actors shape doctrine and policy in response to the evolving geopolitical implications of cyber conflict, definitions become crucial. Currently, however, a multitude of inconsistent definitions of cyber war and cyber warfare exist, most of which have exerted limited influence. The differences between these definitions are considerable, and the relationships between them have been poorly explored. The result is a discourse in conflict, built upon definitions that have reduced analytical utility due to the inconsistencies created by definitional proliferation.

The research in this thesis sought to bring a measure of clarity to the discourse of cyber war and cyber warfare definitions. It established that the most commonly occurring characteristics of definitions of cyber war and cyber warfare are that they specify a means through which cyber war or cyber warfare is conducted, an intent with which an action in cyber war or cyber warfare is conducted, an effect that is caused against a target, and the identification of a target against which the effects are sought. It has further established that the academic disciplines that have contributed the greatest number of definitions of cyber war and cyber warfare are law, ICT, military studies, strategic studies and security studies. This, in turn, has underscored the inter-disciplinary nature of the discourse.

Despite the intent of the author, the discourse, as evidenced in the sample, did not provide an evidentiary basis to distinguish between definitions of cyber war and cyber warfare. However, historical patterns of how definitions have emerged over time have become apparent. Analysis of the sample selected for this study showed a discourse that emerged in 1993, yet remained on the margins of academic debate for nearly 15 years. The discourse then rapidly grew in a manner that correlates with the occurrence of major international cyber conflict events, but

has since waned. Over this period, comparatively influential definitions of cyber war and cyber warfare have emerged. When academic citation count and originality of content are considered, these definitions are those presented by Clarke and Knake (2011), Arquilla and Ronfeldt (1993), Rid (2012), the U.S. DoD (2010), Schaap (2009) and Nye (2011).

The nature of the relationships between divergent definitions was demonstrated through a hierarchy of the definitions. This hierarchy is based on the five influential definitions set out above, each of which articulate components of a cyber war or cyber warfare definition that forms the basis for the majority of the definitions in the discourse. The definitions can therefore be interpreted as representative of a definitional category, with each category constituted from a core definition. However, the definitions may also be the result of interaction between two core definitions, thus being derived from a relationship between certain core definitions.

Alternatively, the relationships between definitions can be understood through comparative analysis of their structural components. This is achieved by analysing the definitions according to the structural definition model. By identifying which definitional components a definition specifies, it is possible to determine its structural relationship to other definitions. Definitions that specify an equal number of definitional components can be understood to have a relationship characterised by a high degree of structural consistency, while definitions that have considerable divergence in definitional components have a relationship characterised by structural inconsistency.

The structural definition model also provides the means to identify the key points of inconsistency between definitions. These points of inter-definitional inconsistency are:

- Whether an actor initiating cyber war or cyber warfare has to be a nation state;
- Whether the intent of cyber war or cyber warfare needs to be coercive, or whether it can be defensive or exploitive;
- Whether cyber war or cyber warfare must cause major kinetic violence;

- Whether the target actor against whom cyber war is conducted must be a nation state;
- Whether a target actor is a necessary component of the definition of cyber war or cyber warfare; and
- Whether the identification of a political end is a necessary component of a definition of cyber war or cyber warfare.

The number and extent of the inconsistencies between definitions precludes an immediate and complete reconciliation between the definitions presented in this thesis. However, partial reconciliation is possible when the disagreements set out above are considered in conjunction with the structural definition model and the foundational definition of cyber war and cyber warfare. The foundational definition is envisaged as a comprehensive and reconciliatory definition, which best represents the discourse at the time of research. It is unifying, but not fixed. Due to the flexibility of the structural definition model, the foundational definition has the ability to encompass and enfold the evolution of the discourse and the inevitable changes that will occur as understandings of cyber war are challenged by new perspectives introduced by future research and events.

The particular flexibility and utility of the structural definition model was further evidenced by its immediate applications. Examples include the foundation of a discourse-driven taxonomy of definitions of cyber war and cyber warfare and the adaption of the model to construct alternative definitions. These alternative definitions can represent the interests of a particular actor, or the perspective of new research, but are nonetheless structurally consistent with the existing definitions.

This is indicative of the power of the structural definition model as a tool of discourse reconciliation. It provides a structural basis for new research to be reconciled with the existing discourse, suggesting that despite the inconsistency between them, divergent definitions can share a common foundation. If the commonality between definitions can be accentuated, then the inconsistencies between them – and the implications of these inconsistencies – can be addressed. Consistent representations and analysis of these points of commonality and

disagreement can do much to aid the analytic clarity with which the terms cyber war and cyber warfare are used.

As a result of this thesis, several promising avenues for future research have been identified. Similar research could be repeated with an expanded sample size after a major international cyber event, to evaluate any shifts in the discourse. Alternative research proposals could focus on further application of the structural definition model; either through analysis of further definitions, consideration of related terms, or construction of definitions based on the policy and actions of political actors rather than on the discourse. Further opportunities for research include efforts to definitively clarify the distinction between cyber war and cyber warfare, as well as focused analysis of the implications and possibilities for reconciliation arising from the areas of greatest inter-definitional disagreement.

This thesis began with a consideration of the fragmented nature of the discourse surrounding definitions of cyber war and cyber warfare. While this is a characteristic of the current state of the discourse, this thesis has shown that through the application of the correct analytical tools, an underlying consistency between the structure of definitions can be identified. This common structure indicates that, in many cases, the divergence between the definitions is not as great as may be evidenced by surface-level analysis. Rather, through deeper analysis of the structural components of the definitions, opportunities to clarify and partially resolve inter-definitional inconsistency can be made apparent. This thesis thus concludes on an optimistic note; by first emphasising the consistency between the definitions, then focusing the analysis on reconciling the areas of disagreement that remain, dominant, functional definitions of cyber war and cyber warfare may soon become apparent.

Bibliography

Alford, L. D. (2000). *Cyber warfare: Protecting military systems*. DTIC Document.

Applegate, S. D. (2012). *The principle of maneuver in cyber operations.* Paper presented at the Cyber Conflict (CYCON), 2012 4th International Conference on.

Arquilla, J. (2011). The Computer Mouse that Roared: Cyberwar in the Twenty-First Century. *Brown J. World Aff., 18*, 39.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy, 12*(2), 141-165.

Bachmann, S. D. (2012). Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats–mapping the new frontier of global risk and security management.

Bendrath, R. (2001). The cyberwar debate: Perception and politics in US critical infrastructure protection. *Information & Security: An International Journal, 7*(1), 80-103.

Birdwell, M. B., & Mills, R. (2011). *War fighting in cyberspace: evolving force presentation and command and control*. DTIC Document.

Blank, S. (2008). Web war i: Is Europe's first information war a new kind of war? *Comparative Strategy, 27*(3), 227-247.

Bonner III, E. L. (2014). Cyber power in 21st-century joint warfare. *Joint Force Quarterly, 74*, 102.

Brenner, S. W., & Clarke, L. L. (2010). Civilians in Cyberwarfare: Conscripts. *Vand. J. Transnat'l L., 43*, 1011.

Brown, C., Crabbe, F., Doerr, R., Greenlaw, R., Hoffmeister, C., Monroe, J., ... & Schultz, J. (2012, July). Anatomy, dissection, and mechanics of an introductory cyber-security course's curriculum at the United States naval academy. In *Proceedings of the 17th ACM annual conference on Innovation and technology in computer science education* (pp. 303-308). ACM.

Cahill, T. P., Rozinov, K., & Mule, C. (2003). *Cyber warfare peacekeeping.* Paper presented at the Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society.

Caplan, N. (2013). Cyber War: the Challenge to National Security. *Global Security Studies, 4*(1), 93-115.

Carter, A. (2015). The DOD cyber strategy. *Department of Defense: Washington, DC*.

Cartwright, J., & James, W. (2010). Joint terminology for cyberspace operations. *Joint Chiefs of Staff (JCS) Memorandum, Nov*.

Chappelle, W., McDonald, K., Christensen, J., Prince, L., Goodman, T., Thompson, W., & Hayes, W. (2013). *Sources of occupational stress and prevalence of burnout and clinical distress among US Air Force Cyber Warfare Operators*. DTIC Document.

Cimbala, S. J. (2011). Nuclear Crisis Management and "Cyberwar" Phishing for Trouble. *Strategic studies quarterly, 5*(1), 117-131.

Clarke, R. A., & Knake, R. K. (2011). *Cyber war*: HarperCollins.

Clemmons, B. Q., & Brown, G. D. (1999). Cyberwarfare: Ways, Warriors and Weapons of Mass Destruction. *Military Review, 79*(5), 35.

Danks, D., & Danks, J. H. (2013). The Moral Permissibility of Automated Responses during Cyberwarfare. *Journal of Military Ethics, 12*(1), 18-33.

Department of Defense. (2010). JP1-02: Department of Defense Dictionary of Military and Associated Terms 8 November 2010 (as Amended Through 15 November 2012). Retrieved from http://www.docucu-archive.com/view/38403902d2f837c1f5650f4f70bb308f/Joint-Pub-1-02-Defense-Technical-Information.pdf website:

Department of Defense. (2011). Department of Defense Strategy for Operating in Cyberspace. Retrieved from

http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf website:
Department of Defense. (2013). Joint Publication 3-12 (R) Cyberspace Operations. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf website:
Detel, W. (2015). Social Constructivism. 228-234.
Dipert, R. R. (2013). Other-than-Internet (OTI) cyberwarfare: challenges for ethics, law, and policy. *Journal of Military Ethics, 12*(1), 34-53.
Droege, C. (2012). Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross, 94*(886), 533-578.
Dycus, S. (2009). Congress's Role in Cyber Warfare.
Eom, J.-H., Kim, N.-U., Kim, S.-H., & Chung, T.-M. (2012). *Cyber military strategy for cyberspace superiority in cyber warfare.* Paper presented at the Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on.
Erbacher, R. F. (2005). *Extending command and control infrastructures to cyber warfare assets.* Paper presented at the Systems, Man and Cybernetics, 2005 IEEE International Conference on.
Fairclough, N. (1995). Critical discourse analysis. The critical study of language. Language in social life series: London: Longman.
Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival, 53*(1), 23-40.
Feil, J. A. (2012). Cyberwar and unmanned aerial vehicles: using new technologies, from espionage to action. *Case W. Res. J. Int'l L., 45*, 513.
Fink, L. C. K. D., Navy, U., Jordan, M. J. D., Corps, U. M., Wells, M. J. E., & Force, U. A. (2014). Considerations for Offensive Cyberspace Operations. *Military Review*.
Friesen, T. L. (2009). Resolving tomorrow's conflicts today: how new developments within the UN security council can be used to combat cyberwarfare. *Naval L. Rev., 58*, 89.
Fritz, J. (2008). How China will use cyber warfare to leapfrog in military competitiveness.
Ganji, M., Dehghantanha, A., IzuraUdzir, N., & Damshenas, M. (2013). Cyber warfare trends and future. *Advances in Information Sciences and Service Sciences, 5*(13), 1.
Golling, M., & Stelte, B. (2011). *Requirements for a future EWS-Cyber Defence in the internet of the future.* Paper presented at the Cyber conflict (ICCC), 2011 3rd international conference on.
Hollis, D. (2011). Cyberwar case study: Georgia 2008. *Small Wars Journal.* Retrieved from: http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008
Hughes, D., & Colarik, A. (2016). Predicting the Proliferation of Cyber-Weapons into Small States. *Joint Force Quarterly* (83), 19-25.
Hughes, D., & Colarik, A. (2016). *Small State Acquisition of Offensive Cyberwarfare Capabilities: Towards Building an Analytical Framework.* Paper presented at the Pacific-Asia Workshop on Intelligence and Security Informatics.
Hughes, R. (2010). A treaty for cyberspace. *International Affairs, 86*(2), 523-541.
Hunker, J. (2010). Cyber war and cyber power. *Issues for NATO doctrine. Research Paper*
Huntley, T. C. (2010). Controlling the use of force in cyber space: The application of the law of armed conflict during a time of fundamental change in the nature of warfare. *Naval L. Rev., 60*, 1.
Jolley, J. D. (2012). Article 2 (4) and Cyber Warfare: How do Old Rules Control the Brave New World?
Jørgensen, M. W., & Phillips, L. J. (2002). *Discourse analysis as theory and method*: Sage.
Junio, T. J. (2013). How probable is cyber war? Bringing IR theory back in to the cyber conflict debate. *Journal of Strategic Studies, 36*(1), 125-133.
Kirsch, C. M. (2011). Science Fiction No More: Cyber Warfare and the United States. *Denv. J. Int'l L. & Pol'y, 40*, 620.
Korns, S. W., & Kastenberg, J. E. (2008). Georgia's cyber left hook. *Parameters, 38*(4), 60.
Leblanc, S. P., Partington, A., Chapman, I., & Bernier, M. (2011). *An overview of cyber attack and computer network operations simulation.* Paper presented at the Proceedings of the 2011 Military Modeling & Simulation Symposium.

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*: Center for Strategic & International Studies Washington, DC.
Lewis, J. A. (2011). Cyberwar thresholds and effects. *IEEE Security & Privacy, 9*(5), 23-29.
Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*: Rand Corporation.
Libicki, M. C. (2011). Cyberwar as a confidence game. *Strategic studies quarterly, 5*.
Libicki, M. C. (2012). Cyberspace is not a warfighting domain. *ISJLP, 8*, 321.
Libicki, M. C. (2014). *Why cyber war will not and should not have its grand strategist*. DTIC Document.
Liff, A. P. (2012). Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies, 35*(3), 401-428.
Liff, A. P. (2013). The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio. *Journal of Strategic Studies, 36*(1), 134-138.
Liles, S., Dietz, J. E., Rogers, M., & Larson, D. (2012). *Applying traditional military principles to cyber warfare.* Paper presented at the Cyber conflict (CYCON), 2012 4th international conference on.
Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies, 22*(3), 365-404.
Lobel, H. (2011). Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict. *Tex. Int'l LJ, 47*, 617.
Lupovici, A. (2011). Cyber warfare and deterrence: trends and challenges in research. *Military and Strategic Affairs, 3*(3), 49-62.
McGraw, G. (2013). Cyber war is inevitable (unless we build security in). *Journal of Strategic Studies, 36*(1), 109-119.
Nguyen, R. (2013). Navigating jus ad bellum in the age of cyber warfare. *Cal. L. Rev., 101*, 1079.
Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. *Computers & Security, 31*(4), 418-436.
Nye Jr, J. S. (2011). *Nuclear lessons for cyber security*. DTIC Document.
O'Connell, M. E. (2012). Cyber security without cyber war. *Journal of conflict and security law, 17*(2), 187-209.
O'Leary, Z. (2004). *The essential guide to doing research*: Sage.
Ottis, R., & Lorents, P. (2010). *Cyberspace: Definition and implications.* Paper presented at the International Conference on Information Warfare and Security.
Parks, R. C., & Duggan, D. P. (2011). Principles of cyberwarfare. *IEEE Security & Privacy, 9*(5), 30-35.
Raboin, B. (2011). Corresponding Evolution: International Law and the Emergence of Cyber Warfare. *J. Nat'l Ass'n Admin. L. Judiciary, 31*, 602.
Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies, 35*(1), 5-32.
Rid, T., & McBurney, P. (2012). Cyber-weapons. *the RUSI Journal, 157*(1), 6-13.
Roberts, S. (2014). Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors. *N. Ky. L. Rev., 41*, 535.
Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security, 49*, 70-94.
Roscini, M. (2010). World Wide Warfare-'Jus Ad Bellum' and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law*, Vol. 14, pp. 85-130, 2010. Available at SSRN: https://ssrn.com/abstract=1683370
Saad, S., Bazan, S., & Varin, C. (2011). Asymmetric Cyber-warfare between Israel and Hezbollah: the Web as a new strategic battlefield. Retrieved from: http://journal.webscience.org/526/1/96_paper.pdf
Schaap, A. J. (2009). Cyber warfare operations: Development and use under international law. *AFL Rev., 64*, 121.
Schmitt, Michael N., ed. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, 2013.
Scott, A., Hardy, T., Martin, R. K., & Thomas, R. W. (2011). *What are the roles of electronic and cyber warfare in cognitive radio security?* Paper presented at the

Circuits and Systems (MWSCAS), 2011 IEEE 54th International Midwest Symposium on.
Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to cyber-warfare: A multidisciplinary approach*: Newnes.
Solis, G. D. (2014). Cyber warfare. *Mil. L. Rev., 219*, 1.
Stytz, M. R., & Banks, S. B. (2010). Addressing simulation issues posed by cyber warfare technologies. *SCS M&S Magazine. n (3)*.
Swanson, L. (2010). The era of cyber warfare: Applying international humanitarian law to the 2008 Russian-Georgian cyber conflict. *Loy. LA Int'l & Comp. L. Rev., 32*, 303.
Taddeo, M. (2012). *An Analysis for a Just Cyber Warfare.* Paper presented at the 4th International Conference on Cyber Conflict, Tallinn.
Tikk, E., Kaska, K., Rünnimeri, K., Kert, M., Talihärm, A.-M., & Vihul, L. (2008). Cyber attacks against Georgia: Legal lessons identified. *Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, at http://www. carlisle. army. mil/DIME/documents/Georgia, 201*, 200.
Turns, D. (2012). Cyber warfare and the notion of direct participation in hostilities. *Journal of conflict and security law, 17*(2), 279-297.
Uma, M., & Padmavathi, G. (2013). A Survey on Various Cyber Attacks and their Classification. *IJ Network Security, 15*(5), 390-396.
Von Clausewitz, C., & Graham, J. J. (1873). *On war* (Vol. 1): London, N. Trübner & Company.
Wang, H., & Wang, S. (2004). Cyber warfare: steganography vs. steganalysis. *Communications of the ACM, 47*(10), 76-82.
Wilson, C. (2007). *Information operations, electronic warfare, and cyberwar: Capabilities and related policy issues*.

Appendix A: Source Article Analysis

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Golling, M., & Stelte, B. (2011, June). Requirements for a future EWS-Cyber Defence in the internet of the future. In 2011 3rd International Conference on Cyber Conflict (pp. 1-16). IEEE.	Explicit	2011	26	Cyber War and Cyber Warfare	Conference on Cyber Conflict
Eom, J. H., Kim, N. U., Kim, S. H., & Chung, T. M. (2012, June). Cyber military strategy for cyberspace superiority in cyber warfare. In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on (pp. 295-299). IEEE. DOI:10.1109/CyberSec.2012.6246114	Explicit	2012	14	Cyber Warfare	Conference on Cyber Conflict
Liles, S., Dietz, J. E., Rogers, M., & Larson, D. (2012, June). Applying traditional military principles to cyber warfare. In 2012 4th International Conference on Cyber Conflict (CYCON 2012).	Explicit	2012	11	Cyber War and Cyber Warfare	Conference on Cyber Conflict
Taddeo, M. (2012, June). An analysis for a just cyber warfare. In 2012 4th International Conference on Cyber Conflict (CYCON 2012) (pp. 1-10). IEEE.	Explicit	2012	9	Cyber Warfare	Conference on Cyber Conflict
Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. Computers & Security, 31(4), 418-436. DOI: 10.1016/j.cose.2012.02.009	Explicit	2012	117	Cyber War and Cyber Warfare	ICT
Parks, R. C., & Duggan, D. P. (2011). Principles of cyberwarfare. IEEE Security & Privacy Magazine, 9(5), 30-35. DOI: 10.1109/MSP.2011.138	Explicit	2011	61	Cyber Warfare	ICT

[9] Citation counts were extracted from Google Scholar in July and August 2016. Citation counts may differ between sources.

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Uma, M., & Padmavathi, G. (2013). A Survey on Various Cyber Attacks and their Classification. IJ Network Security, 15(5), 390-396.	Explicit	2013	20	Cyber War	ICT
Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. Computers & security, 49, 70-94. DOI:10.1016/j.cose.2014.11.007	Explicit	2015	15	Cyber Warfare	ICT
Leblanc, S. P., Partington, A., Chapman, I., & Bernier, M. (2011, April). An overview of cyber attack and computer network operations simulation. In Proceedings of the 2011 Military Modeling & Simulation Symposium (pp. 92-100). Society for Computer Simulation International.	Explicit	2011	12	Cyber Warfare	ICT
Cahill, T. P., Rozinov, K., & Mule, C. (2003, June). Cyber warfare peacekeeping. In Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society (pp. 100-106). IEEE. DOI:10.1109/SMCSIA.2003.1232407	Explicit	2003	11	Cyber War and Cyber Warfare	ICT
Lewis, J. (2011). Cyberwar thresholds and effects. IEEE Security & Privacy, 9(5), 23-29. DOI:10.1109/MSP.2011.25	Explicit	2011	10	Cyber War and Cyber Warfare	ICT

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Brown, C., Crabbe, F., Doerr, R., Greenlaw, R., Hoffmeister, C., Monroe, J., ... & Schultz, J. (2012, July). Anatomy, dissection, and mechanics of an introductory cyber-security course's curriculum at the United States naval academy. In Proceedings of the 17th ACM annual conference on Innovation and technology in computer science education (pp. 303-308). ACM. DOI:10.1145/2325296.2325367	Explicit	2012	8	Cyber Warfare	ICT
Saad, S., Bazan, S., & Varin, C. (2011). Asymmetric Cyber-warfare between Israel and Hezbollah: the Web as a new strategic battlefield. In: Proceedings of the ACM WebSci'11, June 14-17 2011, Koblenz, Germany	Explicit	2011	5	Cyber War and Cyber Warfare	ICT
Ganji, M., Dehghantanha, A., IzuraUdzir, N., & Damshenas, M. (2013). Cyber warfare trends and future. Advances in Information Sciences and Service Sciences, 5(13), 1.	Explicit	2013	4	Cyber War and Cyber Warfare	ICT
Hughes, R. (2010). A treaty for cyberspace. International Affairs, 86(2), 523-541. DOI: 10.1111/j.1468-2346.2010.00894.x	Explicit	2010	57	Cyber Warfare	International Relations
Droege, C. (2012). Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. International Review of the Red Cross, 94(886), 533-578. DOI:10.1017/S181638311300246	Explicit	2012	21	Cyber War and Cyber Warfare	International Relations
Arquilla, J. (2011). Computer Mouse That Roared: Cyberwar in the Twenty-First Century, The. Brown J. World Aff., 18, 39.	Explicit	2011	5	Cyber War and Cyber Warfare	International Relations

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Schaap, A. J. (2009). Cyber warfare operations: Development and use under international law. AFL Rev., 64, 121.	Explicit	2009	95	Cyber Warfare	Law
Gervais, M. (2011). Cyber Attacks and the Laws of War. Berkeley Journal of International Law. Volume 30 Issue 2	Explicit	2011	39	Cyber War and Cyber Warfare	Law
Brenner, S. W., & Clarke, L. L. (2010). Civilians in Cyberwarfare: Conscripts. Vand. J. Transnat'l L., 43, 1011.	Explicit	2010	25	Cyber Warfare	Law
Dycus, S. (2010). Congress's Role in Cyber Warfare. Journal of National Security Law & Policy, 4, 153.	Explicit	2010	23	Cyber War and Cyber Warfare	Law
Swanson, L. (2010). Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict, The. Loy. LA Int'l & Comp. L. Rev., 32, 303.	Explicit	2010	21	Cyber War and Cyber Warfare	Law
Reich, P. C., Weinstein, S., Wild, C., & Cabanlong, A. S. (2010). Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents–and the Dilemma of Anonymity. European Journal of Law and Technology, 1(2).	Explicit	2010	14	Cyber War and Cyber Warfare	Law
Raboin, B. (2011). Corresponding Evolution: International Law and the Emergence of Cyber Warfare. J. Nat'l Ass'n Admin. L. Judiciary, 31, 602.	Explicit	2011	13	Cyber Warfare	Law
Turns, D. (2012). Cyber warfare and the notion of direct participation in hostilities. Journal of conflict and security law, 17(2), 279-297. DOI: 10.1093/jcsl/krs021	Explicit	2012	13	Cyber War and Cyber Warfare	Law
Kirsch, C. M. (2011). Science Fiction No More: Cyber Warfare and the United States. Denv. J. Int'l L. & Pol'y, 40, 620.	Explicit	2011	10	Cyber War and Cyber Warfare	Law

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Bachmann, S. D. O. V. (2012). Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats–mapping the new frontier of global risk and security management. Amicus Curiae, 88.	Explicit	2012	9	Cyber War and Cyber Warfare	Law
Jolley, J. D. (2012). Article 2 (4) and Cyber Warfare: How do Old Rules Control the Brave New World?. DOI: http://dx.doi.org/10.5539/ilr.v2n1p1	Explicit	2012	4	Cyber War and Cyber Warfare	Law
Roberts, S. (2014). Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors. N. Ky. L. Rev., 41, 535.	Explicit	2014	3	Cyber War and Cyber Warfare	Law
Feil, J. A. (2012). Cyberwar and unmanned aerial vehicles: using new technologies, from espionage to action. Case W. Res. J. Int'l L., 45, 513.	Explicit	2012		Cyber War	Law
Nye Jr, J. S. (2011). Nuclear lessons for cyber security. Air Univ Press Maxwell AFB AL.	Explicit	2011	65	Cyber War	Military Studies
Birdwell, M. B., & Mills, R. (2011). War fighting in cyberspace: evolving force presentation and command and control. Air Univ Maxwell Air Force Research Inst.	Explicit	2011	50	Cyber War	Military Studies
Huntley, T. C. (2010). Controlling the use of force in cyber space: the application of the law of armed conflict during a time of fundamental change in the nature of warfare. Naval L. Rev., 60, 1.	Explicit	2010	30	Cyber War and Cyber Warfare	Military Studies
Libicki, M. C. (2011). Cyberwar as a confidence game. Strategic Studies Quarterly, 5.	Explicit	2011	26	Cyber War and Cyber Warfare	Military Studies
Hunker, J. (2010). Cyber war and cyber power. Issues for NATO doctrine. Research Paper No.	Explicit	2010	16	Cyber War and Cyber Warfare	Military Studies

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Clemmons, B. Q., & Brown, G. D. (1999). Cyberwarfare: Ways, Warriors and Weapons of Mass Destruction. Military Review, 79(5), 35.	Explicit	1999	14	Cyber War and Cyber Warfare	Military Studies
Lupovici, A. (2011). Cyber Warfare and Deterrence: Trends and Challenges in Research. Military and Strategic Affairs, 3(3), 49-62.	Explicit	2011	11	Cyber Warfare	Military Studies
Friesen, T. L. (2009). Resolving tomorrow's conflicts today: how new developments within the UN security council can be used to combat cyberwarfare. Naval L. Rev., 58, 89.	Explicit	2009	10	Cyber War and Cyber Warfare	Military Studies
Dipert, R. R. (2013). Other-than-Internet (OTI) cyberwarfare: challenges for ethics, law, and policy. Journal of Military Ethics, 12(1), 34-53. DOI: 10.1080/15027570.2013.785126	Explicit	2013	10	Cyber War and Cyber Warfare	Military Studies
Alford, L. D. (2000). Cyber warfare: Protecting military systems. Air Force Materiel Command Wright-Patterson AFB OH	Explicit	2000	9	Cyber Warfare	Military Studies
Chappelle, W., McDonald, K., Christensen, J., Prince, L., Goodman, T., Thompson, W., & Hayes, W. (2013). Sources of Occupational Stress and Prevalence of Burnout and Clinical Distress Among US Air Force Cyber Warfare Operators (No. AFRL-SA-WP-TR-2013-0006). School of Aerospace Medicine Wright Patterson AFB OH.	Explicit	2013	8	Cyber Warfare	Military Studies
Libicki, M. C. (2014). Why cyber war will not and should not have its grand strategist. Air Univ Maxwell AFB AL Air Force Research Inst.	Explicit	2014	8	4	Military Studies

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Cimbala, S. J. (2011). Nuclear Crisis Management and "Cyberwar" Phishing for Trouble. Strategic studies quarterly, 5(1), 117-131.	Explicit	2011	7	Cyber War	Military Studies
Danks, D., & Danks, J. H. (2013). The Moral Permissibility of Automated Responses during Cyberwarfare. Journal of Military Ethics, 12(1), 18-33. DOI: 10.1080/15027570.2013.782637	Explicit	2013	6	Cyber War and Cyber Warfare	Military Studies
Solis, G. D. (2014). Cyber warfare. Mil. L. Rev., 219, 1.	Explicit	2014	4	Cyber War and Cyber Warfare	Military Studies
Stytz, M. R., & Banks, S. B. (2010). Addressing Simulation Issues Posed by Cyber Warfare Technologies. SCS M&S Magazine. n (3).	Explicit	2010	5	Cyber Warfare	Other
Erbacher, R. F. (2005, October). Extending command and control infrastructures to cyber warfare assets. In 2005 IEEE International Conference on Systems, Man and Cybernetics (Vol. 4, pp. 3331-3337). IEEE. DOI:10.1109/IAW.2005.1495994	Explicit	2005	4	Cyber War and Cyber Warfare	Other
Scott, A., Hardy, T. J., Martin, R. K., & Thomas, R. W. (2011, August). What are the roles of electronic and cyber warfare in cognitive radio security?. In 2011 IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS) (pp. 1-4). IEEE. DOI: 10.1109/MWSCAS.2011.6026501	Explicit	2011	4	Cyber Warfare	Other
Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming!. Comparative Strategy, 12(2), 141-165. http://dx.doi.org/10.1080/01495939308402915	Explicit	1993	655	Cyber War	Strategic & Security Studies

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Rid, Thomas. "Cyber war will not take place." Journal of strategic studies 35, no. 1 (2012): 5-32. DOI: 10.1080/01402390.2011.608939	Explicit	2012	225	Cyber War	Strategic & Security Studies
Liff, A. P. (2012). Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war. Journal of Strategic Studies, 35(3), 401-428. DOI: 10.1080/01402390.2012.663252	Explicit	2012	54	Cyber War and Cyber Warfare	Strategic & Security Studies
Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365-404. DOI: 10.1080/09636412.2013.816122	Explicit	2013	47	Cyber War and Cyber Warfare	Strategic & Security Studies
McGraw, G. (2013). Cyber war is inevitable (unless we build security in). Journal of Strategic Studies, 36(1), 109-119. DOI: 10.1080/01402390.2012.742013	Explicit	2013	22	Cyber War	Strategic & Security Studies
Junio, T. J. (2013). How probable is cyber war? Bringing IR theory back in to the cyber conflict debate. Journal of Strategic Studies, 36(1), 125-133. DOI: 10.1080/01402390.2012.739561	Explicit	2013	16	Cyber War and Cyber Warfare	Strategic & Security Studies
Caplan, N. (2013). Cyber War: the Challenge to National Security. Global Security Studies, 4(1), 93-115. DOI: 10.1080/09700161.2015.1047221	Explicit	2013	4	Cyber War and Cyber Warfare	Strategic & Security Studies
Liff, A. P. (2013). The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio. Journal of Strategic Studies, 36(1), 134-138. DOI: 10.1080/01402390.2012.733312	Explicit	2013	3	Cyber War and Cyber Warfare	Strategic & Security Studies

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Giles, K. (2011, June). "Information Troops"-A Russian Cyber Command?. In 2011 3rd International Conference on Cyber Conflict (pp. 1-16). IEEE.	Implicit	2011	29	Cyber War and Cyber Warfare	Conference on Cyber Conflict
Cavelty, M. D. (2012, June). The militarisation of cyberspace: Why less may be better. In 2012 4th International Conference on Cyber Conflict (CYCON 2012) (pp. 1-13). IEEE.	Implicit	2012	27	Cyber War	Conference on Cyber Conflict
Ottis, R., & Lorents, P. (2010, April). Cyberspace: Definition and implications. In International Conference on Information Warfare and Security (p. 267). Academic Conferences International Limited.	Implicit	2010	24	Cyber Warfare	Conference on Cyber Conflict
Applegate, S. D. (2012, June). The principle of maneuver in cyber operations. In 2012 4th International Conference on Cyber Conflict (CYCON 2012) (pp. 1-13). IEEE.	Implicit	2012	10	Cyber Warfare	Conference on Cyber Conflict
Wang, H., & Wang, S. (2004). Cyber warfare: steganography vs. steganalysis. Communications of the ACM, 47(10), 76-82. DOI: 10.1145/1022594.1022597	Implicit	2004	428	Cyber Warfare	ICT
Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, 9(3), 49-51. DOI:10.1109/MSP.2011.67	Implicit	2011	312	Cyber Warfare	ICT
Bendrath, R. (2001). The cyberwar debate: Perception and politics in US critical infrastructure protection. Information & Security: An International Journal, 7, 80-103. http://dx.doi.org/10.11610/isij.0705	Implicit	2001	46	Cyber War	ICT

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Knapp, K. J., & Boulton, W. R. (2006). Cyber-warfare threatens corporations: Expansion into commercial environments. Information Systems Management, 23(2), 76. DOI:10.1201/1078.10580530/45925.23.2.20060301/92675.8	Implicit	2006	39	Cyber War and Cyber Warfare	ICT
Kotenko, I. (2005, June). Agent-based modeling and simulation of cyber-warfare between malefactors and security agents in Internet. In 19th European Simulation Multiconference "Simulation in wider Europe."	Implicit	2005	37	Cyber War and Cyber Warfare	ICT
Goel, S. (2011). Cyberwarfare: connecting the dots in cyber intelligence. Communications of the ACM, 54(8), 132-140. DOI: 10.1145/1978542.1978569	Implicit	2011	34	Cyber Warfare	ICT
Denning, D. E. (2012). Stuxnet: what has changed?. Future Internet, 4(3), 672-687. DOI: 10.3390/fi4030672	Implicit	2012	26	Cyber War and Cyber Warfare	ICT
Geers, K. (2009). The cyber threat to national critical infrastructures: Beyond theory. Information Security Journal: A Global Perspective, 18(1), 1-7. DOI: 10.1080/19393550802676097	Implicit	2009	22	Cyber War and Cyber Warfare	ICT
Applegate, S. (2011). Cybermilitias and political hackers: Use of irregular forces in cyberwarfare. IEEE Security and Privacy, 9(5), 16-22. DOI:10.1109/MSP.2011.46	Implicit	2011	18	Cyber Warfare	ICT

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Cohen, F., Phillips, C., Swiler, L. P., Gaylor, T., Leary, P., Rupley, F., & Isler, R. (1998). A cause and effect model of attacks on information systems: Some Analysis Based on That Model, and The Application of that Model for CyberWarfare in CID. Computers & Security, 17(3), 211-221. DOI:10.1016/S0167-4048(98)80312-X	Implicit	1998	15	Cyber Warfare	ICT
Catuogno, L., & De Santis, A. (2008, June). An internet role-game for the laboratory of network security course. In ACM SIGCSE Bulletin (Vol. 40, No. 3, pp. 240-244). ACM. DOI: http://dx.doi.org/10.1145/1597849.1384336	Implicit	2008	14	Cyber War	ICT
Shouman, M., Salah, A., & Faheem, H. M. (2010). Surviving cyber warfare with a hybrid multiagent-based intrusion prevention system. IEEE Potentials, 29(1), 32. DOI:10.1109/MPOT.2009.935611	Implicit	2010	14	Cyber Warfare	ICT
Hunt, E. (2012). US Government Computer Penetration Programs and the Implications for Cyberwar. IEEE Annals of the History of Computing, 34(3), 4-21. DOI:10.1109/MAHC.2011.82	Implicit	2012	8	Cyber War and Cyber Warfare	ICT
Jordan, T. (2001). Mapping hacktivism: Mass virtual direct action (MVDA), individual virtual direct action (IVDA) and cyber-wars. Computer fraud & security, 2001(4), 8-11. DOI:10.1016/S1361-3723(01)00416-X	Implicit	2001	7	Cyber War	ICT
Blunden, B. (2010). Manufactured Consent and Cyberwar. In LockDown Conference proceedings.	Implicit	2010	7	Cyber War	ICT

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Laprise, J. (2005, June). Cyberwarfare seen through a mariner's spyglass. In Proceedings. 2005 International Symposium on Technology and Society, 2005. Weapons and Wires: Prevention and Safety in a Time of Fear. ISTAS 2005. (pp. 52-61). IEEE. DOI:10.1109/ISTAS.2005.1452713	Implicit	2005	6	Cyber War and Cyber Warfare	ICT
Hamilton, S. N., & Hamilton, W. L. (2008, September). Adversary modeling and simulation in cyber warfare. In IFIP International Information Security Conference (pp. 461-475). Springer US. DOI: 10.1007/978-0-387-09699-5_30	Implicit	2008	5	Cyber Warfare	ICT
Colarik, A. M., & Janczewski, L. J. (2011, December). Developing a grand strategy for Cyber War. In IAS (pp. 52-57). DOI: 10.1109/ISIAS.2011.6122794	Implicit	2011	5	Cyber War and Cyber Warfare	ICT
Mina, M., Abdul Azim, A. G., & Shamala, S. (2011). Design of cyberwar laboratory exercises to implement common security attacks against wireless networks. Journal of Computer Systems, Networks, and Communications, 2010.	Implicit	2011	5	Cyber War	ICT
Tinnel, L. S., Saydjari, O. S., & Farrell, D. (2002, June). Cyberwar Strategy and Tactics. An Analysis of Cyber Goals, Strategies, Tactics, and Techniques. In Proceedings of the 2002 IEEE Workshop on Information Assurance. United States Military Academy, West Point, NY (pp. 228-233).	Implicit	2002	4	Cyber War and Cyber Warfare	ICT

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Kallberg, J., Thuraisingham, B., & Lakomaa, E. (2013, August). Societal cyberwar theory applied: the disruptive power of state actor aggression for public sector information security. In Intelligence and Security Informatics Conference (EISIC), 2013 European (pp. 212-215). IEEE. DOI:10.1109/EISIC.2013.47	Implicit	2013	4	Cyber War and Cyber Warfare	ICT
Zeadally, S., & Flowers, A. (2014). Cyberwar: The what, when, why, and how [commentary]. IEEE Technology and Society Magazine, 33(3), 14-21. DOI:10.1109/MTS.2014.2345196	Implicit	2014	4	Cyber War	ICT
Dunn Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. International Studies Review, 15(1), 105-122. DOI: 10.1111/misr.12023	Implicit	2013	43	Cyber War	International Relations
Richards, J. (2009). Denial-of-service: The Estonian cyberwar and its implications for US national security. International Affairs Review, 18(2).	Implicit	2009	19	Cyber War and Cyber Warfare	International Relations
Zhang, L. (2012). A Chinese perspective on cyber war. International Review of the Red Cross, 94(886), 801-807. DOI: 10.1017/S1816383112000823	Implicit	2012	8	Cyber War and Cyber Warfare	International Relations
Glenny, M., & Kavanagh, C. (2012). 800 titles but no policy—Thoughts on cyber warfare. American foreign policy interests, 34(6), 287-294. DOI: 10.1080/10803920.2012.742410	Implicit	2012	7	Cyber War and Cyber Warfare	International Relations
Hughes, R. (2009). Towards a global regime for cyber warfare. Cyber Security Project, Chatham House, London. DOI: 10.3233/978-I-60750-060-5-106	Implicit	2009	6	Cyber War and Cyber Warfare	International Relations

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Schmitt, M. N. (Ed.). (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press.	Implicit	2013	210	Cyber War and Cyber Warfare	Law
Shackelford, S. (2009). From nuclear war to net war: analogizing cyber attacks in international law. Berkley Journal of International Law (BJIL), 25(3).	Implicit	2009	153	Cyber War and Cyber Warfare	Law
Waxman, M. C. (2011). Cyber-attacks and the use of force: Back to the future of article 2 (4). Yale Journal of International Law, 36.	Implicit	2011	144	Cyber War and Cyber Warfare	Law
Kelsey, J. T. (2008). Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare. Michigan Law Review, 1427-1451.	Implicit	2008	85	Cyber Warfare	Law
O'Connell, M. E. (2012). Cyber security without cyber war. Journal of Conflict and Security Law, 17(2), 187-209. DOI: 10.1093/jcsl/krs017	Implicit	2012	54	Cyber War and Cyber Warfare	Law
Jensen, E. T. (2009). Cyber warfare and precautions against the effects of attacks. Tex. L. Rev., 88, 1533.	Implicit	2009	51	Cyber War	Law
Ophardt, J. A. (2010). Cyber warfare and the crime of aggression: The need for individual accountability on tomorrow's battlefield. Duke L. & Tech. Rev., i.	Implicit	2010	44	Cyber War and Cyber Warfare	Law
Hoisington, M. (2009). Cyberwarfare and the use of force giving rise to the right of self-defense. Boston College International and Comparative Law Review, 32, 439.	Implicit	2009	42	Cyber War and Cyber Warfare	Law
Geers, K. (2010). The challenge of cyber attack deterrence. Computer Law & Security Review, 26(3), 298-303. DOI:10.1016/j.clsr.2010.03.00	Implicit	2010	36	Cyber War and Cyber Warfare	Law

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Roscini, M. (2010). World Wide Warfare-'Jus Ad Bellum'and the Use of Cyber Force. Max Planck Yearbook of United Nations Law, 14, 85-130. DOI: 10.1163/18757413-90000050	Implicit	2010	34	Cyber Warfare	Law
Nguyen, R. (2013). Navigating jus ad bellum in the age of cyber warfare. Cal. L. Rev., 101, 1079.	Implicit	2013	27	Cyber War and Cyber Warfare	Law
Jurich, J. P. (2008). Cyberwar and customary international law: The potential of a bottom-up approach to an international law of information operations. Chi. J. Int'l L., 9, 275.	Implicit	2008	26	Cyber War and Cyber Warfare	Law
Buchan, R. (2012). Cyber attacks: unlawful uses of force or prohibited interventions?. Journal of Conflict and Security Law, 17(2), 212-227. DOI: 10.1093/jcsl/krs014	Implicit	2012	26	Cyber War	Law
Schmitt, M. N. (2014). Law of Cyber Warfare: Quo Vadis, The. Stan. L. & Pol'y Rev., 25, 269.	Implicit	2014	20	Cyber Warfare	Law
Richardson, J. (2011). Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield. J. Marshall J. Computer & Info. L., 29, 1.	Implicit	2011	16	Cyber War and Cyber Warfare	Law
Dinstein, Y. (2012). The principle of distinction and cyber war in International Armed Conflicts. Journal of Conflict and Security Law, 17(2), 261-277. DOI: 10.1093/jcsl/krs015	Implicit	2012	14	Cyber War	Law
Brenner, S. W., & Clarke, L. L. (2010). Civilians in cyberwarfare: casualties. SMU science & technology law review, 13.	Implicit	2010	13	Cyber War and Cyber Warfare	Law
Lobel, H. (2011). Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict. Tex. Int'l LJ, 47, 617.	Implicit	2011	13	Cyber War	Law

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Goldsmith, J. (2013). How cyber changes the laws of war. European Journal of International Law, 24(1), 129-138.	Implicit	2013	13	Cyber War	Law
Fleck, D. (2013). Searching for international rules applicable to cyber warfare—A critical first assessment of the new Tallinn manual. Journal of Conflict and Security Law, 18(2), 331-351. DOI: 10.1093/jcsl/krt011	Implicit	2013	12	Cyber War and Cyber Warfare	Law
Geiß, R., & Lahmann, H. (2012). Cyber warfare: Applying the principle of distinction in an interconnected space. Israel Law Review, 45(03), 381-399. DOI: 10.1017/S0021223712000179	Implicit	2012	8	Cyber Warfare	Law
Malawer, S. (2010). Cyberwarfare: Law & Policy Proposals for US & Global Governance. Virginia Lawyer, 58, 28.	Implicit	2010	7	Cyber War and Cyber Warfare	Law
Kessler, O., & Werner, W. (2013). Expertise, uncertainty, and international law: a study of the Tallinn Manual on cyberwarfare. Leiden Journal of International Law, 26(04), 793-810. DOI:10.1017/S0922156513000411	Implicit	2013	7	Cyber War and Cyber Warfare	Law
Muir, L. (2011). The Case Against an International Cyber Warfare Convention. Wake Forest Law Review Online, 5, 5-12.	Implicit	2011	6	Cyber War and Cyber Warfare	Law
Eichensehr, K. E. (2015). Cyberwar & International Law Step Zero. Tex. Int'l LJ, 50, 357.	Implicit	2015	6	Cyber War and Cyber Warfare	Law
Dinstein, Y. (2013). Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference. Int'l L. Stud. Ser. US Naval War Col., 89, i. DOI: 10.1093/jcsl/krs016	Implicit	2013	3	Cyber War and Cyber Warfare	Law

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Azzopardi, M. (2013). The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Brief Introduction on Its Treatment of Jus Ad Bellum Norms. Elsa Malta Law Review, 3.	Implicit	2013	3	Cyber Warfare	Law
Korns, S. W., & Kastenberg, J. E. (2008). Georgia's cyber left hook. Parameters, 38(4), 60.	Implicit	2008	67	Cyber War and Cyber Warfare	Military Studies
Antolin-Jenkins, V. M. (2005). Defining the parameters of cyberwar operations: looking for law in all the wrong places. Naval L. Rev., 51, 132.	Implicit	2005	47	Cyber War	Military Studies
Dunlap Jr, C. J. (2011). Perspectives for cyber strategists on law for cyberwar. Strategic Studies Quarterly, Spring 2011	Implicit	2011	41	Cyber War and Cyber Warfare	Military Studies
Allen, P. D., & Demchak, C. C. (2003). The Palestinian-Israeli Cyberwar. Military Review, 83(2), 52.	Implicit	2003	27	Cyber War	Military Studies
Crosston, M. D. (2011). World Gone Cyber MAD. Strategic Studies, 100.	Implicit	2011	25	Cyber War	Military Studies
Tabansky, L. (2011). Basic concepts in cyber warfare. Military and Strategic Affairs, 3(1), 75-92.	Implicit	2011	18	Cyber War and Cyber Warfare	Military Studies
Kallberg, J. (2013). Cyber Operations–Bridging from Concept to Cyber Superiority. Joint Forces Quarterly, (68).	Implicit	2013	16	Cyber Warfare	Military Studies
Denning, D. E. (2009). Barriers to entry: are they lower for cyber warfare?.	Implicit	2009	15	Cyber War and Cyber Warfare	Military Studies
Arquilla, J. (2013). Twenty years of cyberwar. Journal of Military Ethics, 12(1), 80-87. DOI: 10.1080/15027570.2013.782632	Implicit	2013	11	Cyber War	Military Studies
Miller, R. A., Kuehl, D. T., & Lachow, I. (2011). Cyber War: Issues in Attack and Defence. Joint Force Quarterly, 61(2), 18-23.	Implicit	2011	11	Cyber War	Military Studies

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Franz, T. (2011). The cyber warfare professional: realizations for developing the next generation. Air and Space Power Journal Maxwell AFB AL.	Implicit	2011	8	Cyber War and Cyber Warfare	Military Studies
Conti, G., & Raymond, D. (2011). Leadership of cyber warriors: Enduring principles and new directions. Military Academy West Point NY Dept of Electrical Engineering and Computer Science.	Implicit	2011	8	Cyber Warfare	Military Studies
Kallberg, J. (2012). Designer satellite collisions from covert cyber war. Strategic Studies Quarterly, 124.	Implicit	2012	8	Cyber War and Cyber Warfare	Military Studies
Kanwal, G. (2009). China's Emerging Cyber War Doctrine. Journal of Defence Studies, 3(3), 14-22. DOI: 10.1080/15027570.2013.782638	Implicit	2009	7	Cyber War and Cyber Warfare	Military Studies
Farmer, D. B. (2010). Do the principles of war apply to cyber war?. Army Command and General Staff College Fort Leavenworth KS School of Advanced Military Studies.	Implicit	2010	7	Cyber War and Cyber Warfare	Military Studies
Eberle, C. J. (2013). Just War and Cyberwar. Journal of Military Ethics, 12(1), 54-67. DOI: 10.1080/15027570.2013.782638	Implicit	2013	7	Cyber War	Military Studies
Dunlap Jr, C. J. (2013). Some reflections on the intersection of law and ethics in cyber war. Air & Space Power Journal, 27(1), 22.	Implicit	2013	6	Cyber War	Military Studies
Dombrowski, P., & Demchak, C. C. (2014). Cyber war, cybered conflict, and the maritime domain. Naval War College Review, 67(2), 70.	Implicit	2014	6	Cyber War and Cyber Warfare	Military Studies
Kan, P. R. (2013). Cyberwar to Wikiwar: battles for cyberspace. Army War College Carlisle Barracks PA.	Implicit	2013	4	Cyber War	Military Studies

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Cobb, J. (2011). Centralized execution, decentralized chaos: how the Air Force is poised to lose a cyber war. Air and Space Powere Journal Maxwell AFB AL.	Implicit	2011	3	Cyber War and Cyber Warfare	Military Studies
Gregory, D. (2011). The everywhere war. The Geographical Journal, 177(3), 238-250. DOI: 10.1111/j.1475-4959.2011.00426.x	Implicit	2011	158	Cyber Warfare	Other
Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. Journal of International Management, 11(4), 541-562. DOI:10.1016/j.intman.2005.09.009	Implicit	2005	78	Cyber War	Other
Barnard-Wills, D., & Ashenden, D. (2012). Securing virtual space cyber war, cyber terror, and risk. Space and Culture, 15(2), 110-123. DOI: 10.1177/1206331211430016	Implicit	2012	20	Cyber War and Cyber Warfare	Other
Rosenfield, D. K. (2009). Rethinking cyber war. Critical review, 21(1), 77-90. DOI: 10.1080/08913810902812156	Implicit	2009	15	Cyber War	Other
Cullather, N. (2003). Bombing at the speed of thought: intelligence in the coming age of cyberwar. Intelligence and national security, 18(4), 141-154. DOI: 10.1080/02684520310001688907	Implicit	2003	12	Cyber War and Cyber Warfare	Other
Kaiser, R. (2015). The birth of cyberwar. Political Geography, 46, 11-20. DOI:10.1016/j.polgeo.2014.10.001	Implicit	2015	8	Cyber War and Cyber Warfare	Other
Bringsjord, S., & Licato, J. (2015). By Disanalogy, Cyberwarfare is Utterly New. Philosophy & Technology, 28(3), 339-358. DOI: 10.1007/s13347-015-0194-y	Implicit	2015	3	Cyber War and Cyber Warfare	Other

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23-40. DOI: 10.1080/00396338.2011.555586	Implicit	2011	238	Cyber War	Strategic & Security Studies
Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. Journal of Strategic Security, 4(2), 49.	Implicit	2011	61	Cyber War and Cyber Warfare	Strategic & Security Studies
Gartzke, E. (2013). The myth of cyberwar: bringing war in cyberspace back down to earth. International Security, 38(2), 41-73.	Implicit	2013	52	Cyber War	Strategic & Security Studies
Stone, J. (2013). Cyber war will take place!. Journal of Strategic Studies,36(1), 101-108. DOI: 10.1080/01402390.2012.730485	Implicit	2013	40	Cyber War	Strategic & Security Studies
Farwell, J. P., & Rohozinski, R. (2012). The new reality of cyber war. Survival, 54(4), 107-120. DOI: 10.1080/00396338.2012.709391	Implicit	2012	38	Cyber War	Strategic & Security Studies
Sharma, A. (2010). Cyber wars: A paradigm shift from means to ends. Strategic Analysis, 34(1), 62-73.	Implicit	2010	36	Cyber War and Cyber Warfare	Strategic & Security Studies
Hjortdal, M. (2011). China's use of cyber warfare: Espionage meets strategic deterrence. Journal of Strategic Security, 4(2), 1. DOI: 10.1080/09700160903354450	Implicit	2011	34	Cyber War and Cyber Warfare	Strategic & Security Studies
Ball, D. (2011). China's cyber warfare capabilities. Security Challenges, 7(2), 81-103.	Implicit	2011	26	Cyber Warfare	Strategic & Security Studies
Gompert, D. C., & Libicki, M. (2014). Cyber warfare and Sino-American crisis instability. Survival, 56(4), 7-22. DOI: 10.1080/00396338.2014.941543	Implicit	2014	18	Cyber Warfare	Strategic & Security Studies

Reference	Implicit/ Explicit	Date	Times Cited[9]:	Terms Used	Discipline
Manson, G. P. (2011). Cyberwar: The United States and China prepare for the next generation of conflict. Comparative Strategy, 30(2), 121-133. DOI: 10.1080/01495933.2011.561730	Implicit	2011	15	Cyber War and Cyber Warfare	Strategic & Security Studies
Rid, T. (2013). More attacks, less violence. Journal of Strategic Studies, 36(1), 139-142. DOI: 10.1080/01402390.2012.742012	Implicit	2013	13	Cyber War	Strategic & Security Studies
Colarik, A., & Janczewski, L. (2015). Establishing cyber warfare doctrine. In Current and Emerging Trends in Cyber Operations (pp. 37-50). Palgrave Macmillan UK.	Implicit	2015	11	Cyber War and Cyber Warfare	Strategic & Security Studies
Meyer, P. (2012). Diplomatic Alternatives to Cyber-Warfare: A Near-Term Agenda. The RUSI Journal, 157(1), 14-19.	Implicit	2012	6	Cyber Warfare	Strategic & Security Studies
Cavaiola, L. J., Gompert, D. C., & Libicki, M. (2015). Cyber House Rules: On War, Retaliation and Escalation. Survival, 57(1), 81-104. DOI: 10.1080/00396338.2015.1008300	Implicit	2015	4	Cyber War and Cyber Warfare	Strategic & Security Studies
Gompert, D. C., & Libicki, M. (2015). Waging cyber war the american way. Survival, 57(4), 7-28. DOI: 10.1080/00396338.2015.1068551	Implicit	2015	3	Cyber War and Cyber Warfare	Strategic & Security Studies
Boylan, M. (2013). Can there be a Just Cyber War?. Journal of applied ethics and philosophy, 5, 10-17.	Implicit	2013	3	Cyber War and Cyber Warfare	Other