The Hierarchy of Cyber War Definitions

Daniel Hughes(✉) and Andrew Colarik

Massey University, Palmerston North, New Zealand
daniel.hughes.1@uni.massey.ac.nz, a.m.colarik@massey.ac.nz

Abstract. With the advent of militaries declaring cyberspace as the fifth domain of military warfare, those modern societies that are heavily dependent on its reliable operation need to have a clear understanding of the actors and future activities brought about by this new doctrine. Knowing what is meant by the terms 'cyber war' and 'cyber warfare' is critical to navigating a path forward in preparing for and mitigating the effects caused by such activities. In this paper, the authors identified and analysed 159 documents containing the definitions for these terms in order to discern definitional origins, patterns of usage and the relative trends that emerge as a result. From this analysis, we construct a discourse hierarchy of cyber war and cyber warfare definitions, both as a representation of the findings as well as a basis for incorporating future works into the larger context of the domain.

Keywords: Cyber · War · Warfare · Discourse analysis · Definition · Hierarchy

1 Introduction

Cyberspace is a global Information and Communications Technology (ICT) infrastructure that has rapidly evolved and expanded to become an integral component of modern society. It has facilitated immense increases in the range, reach and volume of communications on a scale never seen before. Cyberspace enables mass communication, global supply chains, shared intelligence, and access to the ideas of a diverse set of cultural norms and customs. Its continued persistence is now integral to everyday life and the functioning of modern States and the broader international system. As a result, cyberspace has attained a strategic significance with both national and international dimensions.

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 those expanses that are open to all nations; international waters and orbital pathways. The data and information flowing through this infrastructure comprises many of the forms of communication that individuals, nation States and sub and supra State organizations use on a daily basis 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 defense - and in some cases the exploitation [1] - of cyberspace.

G.A. Wang et al. (Eds.): PAISI 2017, LNCS 10241, pp. 15–33, 2017.
DOI: 10.1007/978-3-319-57463-9_2

Traditionally military doctrine considered land, sea, and air as operational domains of warfare. The advent of orbital and satellite technologies saw the addition of the operational domain of space. Now militaries have begun to consider cyberspace as the fifth domain of warfare. But just what does this mean? How does a military secure cyberspace? What weapons exist in their arsenal to defend it and what new weapons will need to be developed and deployed to do so? Over the years military scholars and academics have published a plethora of competing discussions envisioning cyber war, cyber warfare, and how best to prepare for it. However, in an initial exploration of military and academic literature pertaining to cyber war and cyber warfare, the authors discovered significant variations in how these terms have been defined. In an emerging field of study concerned with both the security and military exploitation of cyberspace - of such criticality to modern societies - the authors believe that definitions do matter. As such, we embarked on an extensive examination of competing definitions. Our aim was to better understand their uses, clarify their scope, and identify any patterns, categories and trends emerging from their application within the body of literature relevant to this domain. In the proceeding sections of the paper we articulate the methodological design used in selecting the body of literature, before providing a detailed analysis of our findings. We then used the results of our research to construct a discourse hierarchy of the definitions of cyber war and cyber warfare we have encountered. Finally, we present our conclusions and identify opportunities for future research.

2 Methodology

The methodological design of our examination was founded on the theory and practice of a social constructivist application of discourse analysis. Our methodology utilized the concept of an 'order of discourse' [2, 3], which we understand as a terrain in which competing discourses attempt to disseminate their claims to authoritative knowledge. In this case the competing discourses are the contrasting definitions of 'cyber war' and 'cyber warfare' that have been identified in the literature survey. Competition between discourses can be seen operating at two levels: textual – the competition between definitions set out in individual texts, and disciplinary, the competition between different academic disciplines. The texts upon which discourse analysis was performed were articles and papers that include the terms 'cyber war' or 'cyber warfare' in their title or abstract, as key words, or at least five times in the main body of text. Slight lexical variations of these terms, such as 'cyberwar', or 'cyber-war', were considered to be synonymous for the purposes of determining qualifying literature. Furthermore, to qualify as a text, a document must have been published on or before 31 July, 2016, and be either:

1. A peer reviewed article from an academic journal;
2. A peer reviewed paper from a published conference proceeding; or
3. A publicly available military document that has been published for internal or external use.

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

Fig. 1. Use of terms in articles

The body of literature was generated through a series of searches on Google Scholar, using the terms cyber war, cyberwar, cyber-war, cyber warfare, cyberwarfare, and cyber-warfare. Qualifying articles were extracted from the first twenty pages of search results for each term. An important consideration of this approach was to ensure other scholars had the means to replicate and verify this process.

The key metrics extracted from each article for detailed analysis were definition, academic discipline, publication date, times cited, and terms used (e.g. cyber war or cyber warfare). In light of the diverse spectrum of cyber war and cyber warfare definitions we encountered, definitions were distilled into two categories – explicit and 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 included uses of the term where a reasonably precise definition could be inferred from the text, through to uses of the terms in a 'purely descriptive, non-normative sense' [4] such as in The Tallinn Manual on the International Law Applicable to Cyber Warfare, through to uses of the terms that we regarded as largely superficial.

3 The Discourse of Definitions: Cyber War and Cyber Warfare

The research presented in this paper ultimately examined 159 publications as both a survey and a comparative analysis of definitions of cyber war and cyber warfare. We wish to emphasize that this was a descriptive, rather than a prescriptive activity. It was not our intent to argue for the indisputable validity of any one definition. Indeed, we believe that in a contested domain such efforts are more likely to confuse, rather than to clarify the discourse.

Our first task was to clarify the use of the terms cyber war and cyber warfare in discourse. We began with an assumption that differences between the terms could be understood by a traditional military distinction, where 'war' is held to be the act of war, while 'warfare' is the means. Accordingly, cyber warfare could be understood as the means of cyber war, and cyber war the act. However, this assumption was not borne out in our analysis. Figure 1 demonstrates the prevalence with which the terms were used in our methodological sample.

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 85 articles that made use of both terms 35 used cyber warfare as a dominant term, 20 used cyber war as a dominant term, while 20 articles used both terms with comparable frequency. The authors considered a term to be dominant if it was used at least twice as often as the competing term.

The authors did note that in 12 out of the 35 articles including both terms, with cyber warfare as the dominant term, that cyber war was used to denote a particular act or event, which aligned with our original assumption regarding the distinction between 'war' and 'warfare'. A similar pattern was used in articles that used both terms with comparable frequency; five out of 20 such articles used cyber war to indicate an act or event. While these trends are notable, we did not feel that they were of sufficient weight to alter the key conclusion we drew from this information – that the current discourse does not provide sufficient evidentiary basis to definitively distinguish between the terms cyber war and cyber warfare. In accordance with our descriptive analytical approach, we therefore concluded that the current state of the discourse necessitates that we consider cyber war and cyber warfare as synonymous terms. This is not to say that we believe this lack of distinction between the terms is desirable; indeed we regard the state of ambiguous equivalence between the terms as an impediment to focused research.

For our next task, we focused on 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 illustrated in Fig. 2, out of the 159 articles examined we found that only 56 offered explicit definitions, versus 103 articles that based their analysis on generally weaker, implicit definitions of cyber war or warfare.

Explicit vs Implicit	Quantity
Explicit Defintions	56
Implict Defintions	103
Total	159

Fig. 2. Explicit vs. Implicit

The abundance of articles that base analysis on implicit rather than explicit definitions leads us to agree with the observations presented by Lewis [5] and Raboin [6], that ambiguous terminology weakens the analytical utility of the cyber war and warfare discourse. We further agree that the information we have uncovered lends credence to Liff's [7] observations, that '[W]ritings on cyberwarfare have long been plagued by major definitional problems, one consequence of which has been a lack of analytical coherence', and that the meaning of 'cyberwarfare' has become extremely convoluted in popular discourse. We do acknowledge that some articles instead offer an explicit definition of related terms such as 'cyber-attack' [4, 8], or 'cyber conflict' [9]. We believe, however, that unless the relationship of such ancillary terms to cyber war and cyber warfare is clearly articulated, the definition of further competing terms does little to clarify the discourse.

To develop a deeper understanding of the discourse we thought it essential to trace its emergence over time. Our sample begins in 1993 with Arquilla and Ronfeldt's seminal article 'Cyberwar is Coming!' [10]. Our data, shown in Fig. 3, 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.

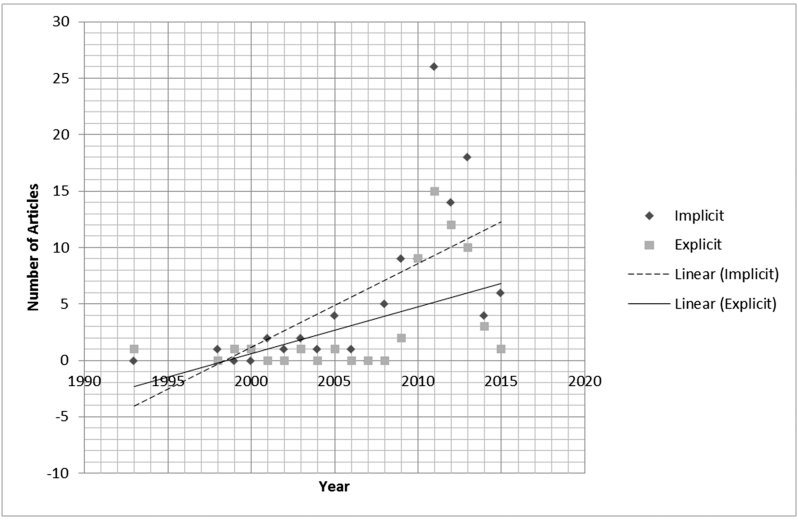

Fig. 3. Implicit/Explicit definitions by year

It is our contention that the number of articles published in the discourse peaks in response to what we consider to be 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. We believe that the 'lag' between the incidents of 2007 and 2008 and the marked increase in publications within the discourse can be attributed 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 our observations of the waxing and waning of the discourse over time, we believe that the discourse will once again expand in response to further empirical incidents of cyber conflict. For example, while we believe that most researchers whose work we have studied would not consider the recent Russian cyber-attacks against the US Democratic Party and alleged interference in the 2016 US election as cyber war or warfare, we nonetheless believe that this event may generate a considerable body of academic work of relevance to the discourse of cyber war and warfare definitions.

As our survey of the cyber war and cyber warfare domain progressed, the interdisciplinary nature of the discourse soon became apparent. As part of our analysis we categorized articles into different academic disciplines, based on the discipline the publication the article appeared in which it was most closely associated with. The results of this process are captured at Fig. 4. Four disciplines dominate the discourse: Information and Communication Technology (ICT), Law, Military Studies, and Strategic and Security studies. These four disciplines accounted 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 Defense Centre of Excellence (CCDOE) and includes submissions relevant to cyber security from a wide range of academic disciplines. Accordingly, the authors felt that articles published from conference proceedings could not accurately be categorized under a single academic discipline; indeed the diverse backgrounds of researchers participating in this conference is representative of the multidisciplinary 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.

Implicit/Explicit Definitions by Discipline					
Discipline	Implicit	Implicit %	Explicit	Explicit %	Total
Law	27.00	16.88%	14.00	8.75%	41.00
Military	22.00	13.75%	15.00	9.38%	37.00
Information and Communications Technology	22.00	13.75%	10.00	6.25%	32.00
Strategic Studies & Security Studies	15.00	9.38%	8.00	5.00%	23.00
Other	8.00	5.00%	3.00	1.88%	11.00
International Conference on Cyber Conflict	4.00	2.50%	4.00	2.50%	8.00
International Relations	5.00	3.13%	3.00	1.88%	8.00
Total	103.00	64.38%	57.00	35.63%	160.00

Fig. 4. Implicit/Explicit definitions by discipline

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 our sample was associated with ICT. We considered that this was the most fragmented discipline, both in the range of divergent positions advanced and the ambiguity with which the terms cyber war and warfare were used. While it included articles that we felt made valuable contributions to the discourse [5, 11], we also encountered articles where we considered the terms cyber war or cyber warfare were used with a significant degree of ambiguity and superficiality [12, 13].

The discipline of Military Studies made the third largest contribution of articles to the discourse. Unsurprisingly articles associated with the military discipline predominantly focused on how cyber war and warfare capabilities could be used to achieve military advantage. In addition, there discussion of the ramifications of cyber war and

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

Fig. 5. Average impact by article

warfare for military ethics, ethos, and force development. Readers should note that this category includes publications from Military Law journals, which we included in the category because of our belief that their primary focus was on military, rather than purely legal matters.

The final dominant discipline we 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, we have elected to represent them as a single discipline for the purposes of our analysis. 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.

To deepen our analysis, we then examined the influence of the articles associated with each discipline. Our measure of influence was the number of times an article had been cited. This data was extracted from Google Scholar during the collection of our sample in July and August 2016. We calculated the average citations per article in each discipline by adding together 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.

As shown in Fig. 5, the most influential discipline in the discourse by citation count is Strategic and Security Studies, followed by ICT, Law, International Relations, Other, Cyber Conflict Conference, and finally, Military. However, if we discount citations from articles with implicit definitions, the rankings change to Strategic and Security Studies, International Relations, ICT, Law, Military, Cyber Conflict Conference, and Other. This allows us to draw several conclusions. Despite having the lowest number of articles out of the major disciplines active in the discourse, the fields of Strategic and Security Studies have had the greatest impact on the discourse. Conversely Military Studies, which has the second highest number of articles in our sample has had a low degree of influence on the discourse.

While the average citations count for articles featuring explicit definitions was slightly greater than that for articles featuring implicit definitions (34.31 to 31.51), we were surprised that this was not higher - we had assumed that articles with explicit definitions would be more influential in the discourse. In line with this observation we note that articles in the Law, ICT and Other categories with implicit definitions have

been more influential than articles with explicit definitions. In the ICT category, we ascribe some of this phenomenon to an outlying article – Wang and Wang's 'Cyber Warfare: Steganography vs. Steganalysis' [12]. 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 our 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 in with implicit definitions in our sample is reduced from 31.51 to 28.91. We have observed a similar pattern 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 have exerted considerably greater influence than those with explicit definitions, is also worthy of further consideration. We contend 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 the Charter of the United Nations. The majority of this type of analysis does not require a perennial definition of cyber war or warfare, as it is focused more on whether individual acts would cross thresholds established in international law.

4 Explicit Definitions of Cyber War and Cyber Warfare

Until this point our analysis had been focused on the totality of definitions we have encountered – both implicit and explicit. While consideration of implicit definitions has provided valuable information as to the shape of the discourse, we believed that further insight could be achieved through a more comprehensive analysis of the explicit definitions encountered in our survey. We began by more effectively ordering explicit definitions by consolidating duplicated definitions. We achieved this by counting each duplicate definition once, then associating it with the discipline of the article using that definition which had the highest citation count. This resulted in the total number of 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 Fig. 6.

Our next action was to shift our analysis down to the level of individual explicit definitions, then to rank these according to influence (by citation count). The top five definitions are captured in Fig. 7.

Explicit Definitions (Duplicates Removed)		
Discipline	Explicit	%
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	100.00%

Fig. 6. Explicit definitions

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

Fig. 7. Top definitions by influence (citation count) [10, 14–17]

The five definitions listed in Fig. 7 have had the greatest influence by citation count out of individual articles encountered in our sample. As we have previously noted, however, we encountered several definitions that were repeated in several articles across several disciplines. While we regard this as further evidence of the cross-disciplinary nature of the cyber war and warfare discourse, we also believed that a more in depth examination of these 'cross-disciplinary definitions' provided another viable method to explore the influence of competing definitions. This led us to construct the table at Fig. 8, where we identified: (a) each cross-disciplinary definition; (b) the references for the articles in which the definition appeared; (c) the discipline of each article in which

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 controlling processes within an opponent's system.	Alford, L. D. (2000).	Military	9	Alford, L. D. (2000)	9	20
	Cahill, et al. (2003)	ICT	11			
"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. It is engaged with the informational environment, agents and targets ranging both on the physical and non-physical domains and level of violence completely depends on the situation	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			

Fig. 8. Breakdown of cross-disciplinary definitions [18–36]

the definition appeared; (d) the number of citations arising from each article; (e) the original source of the definition; (f) the citations arising from the source article; and (g) the total number of citations associated with the cross-disciplinary definition.

Out of the five cross-disciplinary definitions captured in Fig. 8, only the Arquilla and Ronfeldt definition is present in Fig. 7 - the initial table we constructed to demonstrate definition influence. We do note that Arquilla had 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' [21].

Out of the remaining four remaining cross-disciplinary definitions, we considered neither Alford's nor Taddeo's definitions to be sufficiently influential to warrant detailed analysis at that stage. Both definitions encountered were in only one other article and have generated minimal citations. 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' [36] - 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 US Department of Defense – is more complex and worthy of further explication.

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' [30]. CND is defined as '[a]ctions taken to protect, monitor, analyze, detect, and respond to

unauthorized activity within the Department of Defense information systems and computer networks' [30]. 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' [30]. Notably, the Department of Defense source document does not explicitly equate CNO to cyber war or cyber warfare. However, this equation is made in the works of Turns [29], Kirsch [28], Leblanc et al. [26], and Chappelle et al. [27]. We regard the equivalence these authors assert between the terms CNO and cyber war or cyber warfare as valid, particularly when the concept of CNO is considered in light of the Department of Defense's (DoD) Strategy for Operating in Cyberspace [1]. 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 authors 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'. 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' [1].

Neither of the original source documents from which the Clarke and Knake or US Department of Defense definitions arose were included in our sample. Clarke and Knake's definition was not originally published through an academic venue, while the source document for US Department of Defense's concept of Computer Network Operations was not returned in search results – presumably because it does not include the terms cyber war or cyber warfare. Our analysis shows, however, that both works have had considerable influence on the discourse. Indeed, as we have noted, Clarke and Knake's work has generated more citations than any other publication.

Based on our analysis of cross-disciplinary definitions we combined Fig. 7 – the most influential definitions by citation count from a single article, with Fig. 8 – the breakdown of cross-disciplinary definitions. The results are captured in Fig. 9. For reasons previously stated concerning low citations, we omitted Alford's 2000 definition and Taddeo's 2012 definition.

Figure 9 contains the seven most influential definitions that we encountered. However, under further analysis we regard only five of these 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 we have identified are Clarke & Knake [37], Arquilla and Ronfeldt [10], Rid [14], US Department of Defense [30], and Nye [17]. We contend that the definitions offered by Nicolson et al. [15] and Schaap [16] are more correctly viewed as being derived from the definitions offered by Clarke and Knake and the US Department of Defense. Both definitions utilize the State-centric conception of cyber war and cyber warfare found in Clarke and Knake, in addition to the emphasis on CNO that is the focus of the Department of Defense definition. We further justify this action by noting that Schaap's definition uses the language from the Department of Defense definition – 'the use of computer networks

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. (1993)	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

Fig. 9. Most influential definitions by citation count

to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves' – verbatim.

5 A Discourse Hierarchy

Our analysis leads us to contend that the five core definitions we have identified form the foundations for a 'discourse hierarchy' of cyber war and cyber warfare definitions. We believe that out of the 44 explicit definitions we encountered in our analysis, 43 can be logically placed in the structure of our hierarchy. Each definition in the hierarchy either has a one to one relationship with a core definition. Alternatively, in cases where we have perceived that the definition in question included components from two distinct core definitions, a one to two relationship with two core definitions. Our discourse hierarchy is presented at Fig. 10. To explicate the underlying logic of the relationships within it, is necessary to expand upon each of the five core definitions that form its basis.

Rid's definition is presented in his provocatively titled article 'Cyber War Will Not Take Place'. Taking as his starting point the conception of war presented by Clausewitz [66], Rid states that cyber war is 'a potentially lethal, instrumental, and political act of force conducted through malicious code' [14]. This places an extremely high threshold on what would constitute cyber war or cyber war; 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' [14]. No other authors we have 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 be grouped under him in the discourse hierarchy. Alford's 2000 definition, which we have previously encountered in our analysis of cross-disciplinary definitions, is a useful example. Alford's defines cyber warfare as 'any act intended to compel an opponent to fulfil our national will, executed against the software

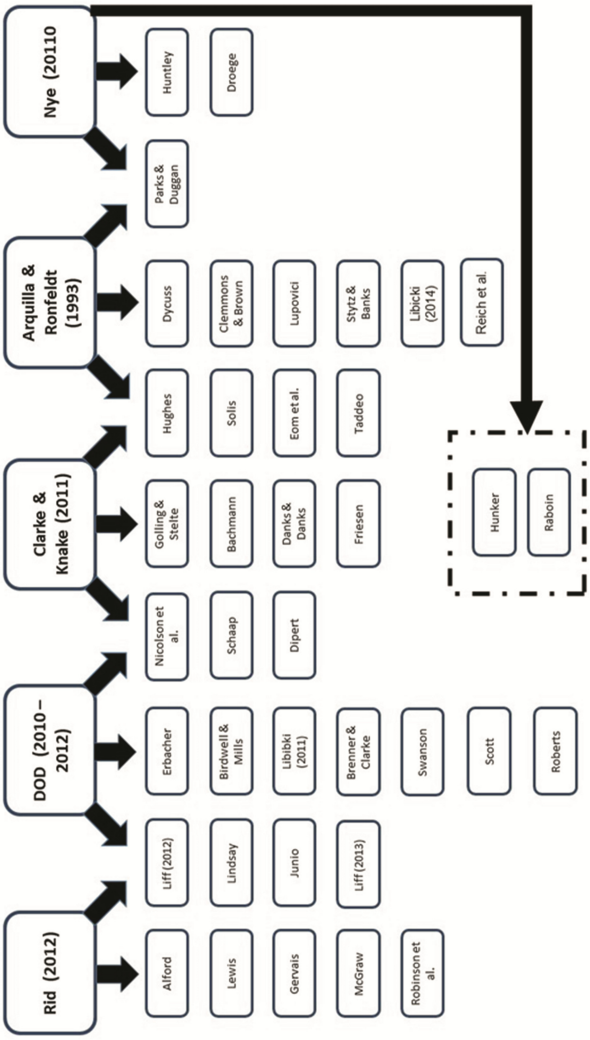

Fig. 10. Discourse hierarchy of cyber war and cyber warfare definitions [7, 15, 37–65]

controlling processes within an opponent's system.' [22] While it omits Rid's criterion of potentially lethal violence, we contend that this Alford's definition shares Rid's conception that cyber war and cyber warfare must involve an instrumental and political act of force. Lewis's 2012 definition – 'the use of cybertechniques to cause, damage, destruction, or casualties for political effect by States or political groups' [5] 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. In addition, 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. In effect McGraw defines cyber war as the application of violent, physical

force via virtual means by groups for 'political, economic, or ideological reasons' [38]. Once again McGraw's definition does not maintain Rid's threshold of potential lethality, but does emphasize that cyber war should be conceived of as a means to achieve a political end.

We consider the above definitions to have a one to one relationship with Rid's definition in the discourse hierarchy. There are other definitions, however, that utilize components of both Rid's definition and the Department of Defense's conception of CNO. An example is the definition offered by Junio [41], where cyber war is defined as a coercive act (using force to change or preserve a political status quo) involving Computer Network Attack (where information is disrupted, degraded, or destroyed). The emphasis on cyber war as a coercive act ties back to Rid, while the reference to Computer Network Attack and the disruption, degradation, or destruction of information is sourced from the Department of Defense's concept of Computer Network Operations. A similar combination of definition components is evident in Liff's 2012 definition where 'cyberwarfare is conceptualized 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 defense (CND)' [7].

While the above definitions are the result of the interaction of the definitions offered by Rid and the Department of Defense, numerous other definitions can be traced solely to the Department of Defense. Birdwell and Mills's define 'cyber war-fighting actions as CNA plus a subset of CND called CND-response actions (CND-RA)' [44], notably omitting Computer Network Exploitation (CNE) from their definition. A similar definition is offered by Scott et al.: 'Cyber warfare is typically associated with the fields of Computer Network Attack (CNA) and Computer Network Defense (CND)… CNA attempts to create tactical and strategic effects through the control and exploitation of network resources, whereas CND defends against these same objectives' [48]. Related definitions are observed through the combination of the Department of Defense definition and the Clarke and Knake definition. The definitions by Schaap [16] and Nicholson et al. [15] are useful examples; the definition offered by Dipert [50], 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 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' [51]. Danks and Danks's definition does not have a strict criterion that cyber war or warfare either originates from or is targeted at a State. Instead 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 [53]. They further note that State backed groups 'typically have a goal that serves the interest of a particular State or state-like group' [53]. Conversely Bachmann's

2012 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' [52].

In a pattern similar to that observed elsewhere in the hierarchy, a number of definitions are constituted according to a dual relationship with both the Clarke and Knake and Arquilla and Ronfeldt definitions. Definitions such as those offered by Hughes [56], and Taddeo [24] utilize Arquilla and Ronfeldt's conception of cyber war and warfare – conducting military operations according to information-related principles – but add the additional criterion that cyber war and cyber warfare is 'waged by states and significant non-state actors' [56], or used 'within an offensive or defensive military strategy endorsed by a state' [24]. Other definitions grouped solely under Arquilla and Ronfeldt focus more exclusively on operational warfare and the furtherance of traditional, kinetic combat (see Libicki [63], Clemmons and Brown [60], and Lupovici [61]).

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' [17]. We regard Nye's definition as particularly useful as it provides a mechanism to group those definitions that make reference to the concepts of 'use of force' and 'armed attack', as they appear in international law. A considerable amount of the legal discourse pertaining to cyber war and cyber warfare discusses how these concepts, enshrined in the UN 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 our hierarchy, we have aligned definitions such as those offered by Huntley [64], and Droege [65], with Nye's definition.

We have represented Hunker's 2012 definition [55] as the result of the 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. We have categorised Raboin's definition in a similar manner, as he states that 'cyber warfare … has come to symbolize a state sponsored use of weapons functioning within the cyberspace domain to create problematic and destructive real world effects' [6]. The final definition associated with Nye, that proposed by Parks and Duggan, has a relationship 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' [11]. From the context of their paper 'The Principles of Cyber-warfare', we interpret this to primarily mean kinetic military effects.

6 Conclusions

Through our application of discourse analysis, we have deduced several conclusions regarding the nature of the discourse of cyber war and warfare definitions. First, the discourse provides no basis to definitively distinguish between the terms 'cyber war' and 'cyber warfare'; extensive synonymous use of the terms in the literature relevant to the domain precludes this. Second, despite location in a domain ostensibly concerned

with the explication and implications of newly emerged technologies and modalities, a majority of articles do not offer explicit definitions of either cyber war or cyber warfare from which to base their analysis. Third, the expansion (and recession) of the discourse correlates with major international cyber incidents. 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. The inter-disciplinary nature of the discourse is further illustrated by the frequency with which definitions migrate across articles arising from different disciplines.

We have further concluded that the domain is characterized by both intra and inter-disciplinary competition between dozens of definitions, most of which 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. We contend that this is indicative of a domain contested by a multitude of stakeholders with differing agendas; and that this is a factor in the failure of the domain to produce a dominant functional definition.

While some element of fragmentation within the domain may be inescapable, we have nonetheless shown that almost all definitions we have encountered can be deduced from five core definitions - those identified through our application of discourse analysis methodology. The identification of these core definitions has in turn allowed us to construct a discourse hierarchy of cyber war and warfare definitions. While we believe that this hierarchy has value in its ability to represent a spectrum of disparate definitions under a single model, we have primarily constructed it in the hope that it may be expand upon and refined as the domain solidifies its use of definitions and associated outcomes.

References

1. Department of Defense. DoD Cyber Strategy (2015). http://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. Accessed
2. Jørgensen, M.W., Phillips, L.J.: Discourse Analysis as Theory and Method. Sage, London (2002)
3. Fairclough, N.: Critical Discourse Analysis: The Critical Study of Language (1995)
4. Schmitt, M.N.: Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, Cambridge (2013)
5. Lewis, J.: Cyberwar thresholds and effects. IEEE Secur. Priv. **9**(5), 23–29 (2011)
6. Raboin, B.: Corresponding evolution: international law and the emergence of cyber warfare. J. Nat. Assoc. Adm. Law Judiciary **31**, 602 (2011)
7. Liff, A.P.: Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war. J. Strateg. Stud. **35**(3), 401–428 (2012)
8. Nguyen, R.: Navigating jus ad bellum in the age of cyber warfare. Cal. Law Rev. **101**, 1079 (2013)
9. Ottis, R., Lorents, P.: Cyberspace: definition and implications. In: International Conference on Information Warfare and Security, p. 267. Academic Conferences International Limited, April 2010
10. Arquilla, J., Ronfeldt, D.: Cyberwar is coming! Comp. Strategy **12**(2), 141–165 (1993)

11. Parks, R.C., Duggan, D.P.: Principles of cyberwarfare. IEEE Secur. Priv. Mag. **9**(5), 30–35 (2011)
12. Wang, H., Wang, S.: Cyber warfare: steganography vs. steganalysis. Commun. ACM **47**(10), 76–82 (2004)
13. Catuogno, L., De Santis, A.: An internet role-game for the laboratory of network security course. In: ACM SIGCSE Bulletin, vol. 40, No. 3, pp. 240–244. ACM, June 2008
14. Rid, T.: Cyber war will not take place. J. Strateg. Stud. **35**(1), 5–32 (2012)
15. Nicholson, A., Webber, S., Dyer, S., Patel, T., Janicke, H.: SCADA security in the light of Cyber-Warfare. Comput. Secur. **31**(4), 418–436 (2012)
16. Schaap, A.J.: Cyber warfare operations: development and use under international law. AFL Rev. **64**, 121 (2009)
17. Nye Jr., J.S.: Nuclear Lessons for Cyber Security. Air Univ. Press Maxwell, AFB, AL (2011)
18. Cimbala, S.J.: Nuclear crisis management and "Cyberwar" phishing for trouble. Strateg. Stud. Q. **5**(1), 117–131 (2011)
19. Liles, S., Dietz, J.E., Rogers, M., Larson, D.: Applying traditional military principles to cyber warfare. In: 2012 4th International Conference on Cyber Conflict (CYCON 2012), June 2012
20. Reich, P.C., Weinstein, S., Wild, C., Cabanlong, A.S.: Cyber warfare: a review of theories, law, policies, actual incidents–and the dilemma of anonymity. Eur. J. Law Technol. **1**(2), 1–58 (2010)
21. Arquilla, J.: Computer Mouse That Roared: Cyberwar in the Twenty-First Century. Brown J. World Aff. **18**, 39 (2011)
22. Alford, L.D.: Cyber warfare: Protecting military systems. AIR FORCE MATERIEL COMMAND WRIGHT-PATTERSON AFB OH (2000)
23. Cahill, T.P., Rozinov, K., Mule, C.: Cyber warfare peacekeeping. In: Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society, pp. 100–106. IEEE, June 2003
24. Taddeo, M.: An analysis for a just cyber warfare. In: 2012 4th International Conference on Cyber Conflict (CYCON 2012), pp. 1–10. IEEE, June 2012
25. Ganji, M., Dehghantanha, A., IzuraUdzir, N., Damshenas, M.: Cyber warfare trends and future. Adv. Inform. Sci. Serv. Sci. **5**(13), 1 (2013)
26. Leblanc, S.P., Partington, A., Chapman, I., Bernier, M.: 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, April 2011
27. Chappelle, W., McDonald, K., Christensen, J., Prince, L., Goodman, T., Thompson, W., Hayes, W.: 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 (2013)
28. Kirsch, C.M.: Science fiction no more: cyber Warfare and the United States. Denver J. Int. Law Policy **40**, 620 (2011)
29. Turns, D.: Cyber warfare and the notion of direct participation in hostilities. J. Conflict Secur. Law **17**(2), 279–297 (2012)
30. DoD, U. S. JP1-02: Department of Defense Dictionary of Military and Associated Terms. Washington: DoD (2010)
31. Uma, M., Padmavathi, G.: A survey on various cyber attacks and their classification. Int. J. Netw. Secur. **15**(5), 390–396 (2013)
32. Saad, S., Bazan, S., Varin, C.: Asymmetric Cyber-warfare between Israel and Hezbollah: the Web as a new strategic battlefield. In: Proceedings of the ACM WebSci 2011, Koblenz, Germany, 14–17 June 2011 (2011)
33. Caplan, N.: Cyber war: the challenge to national security. Glob. Secur. Stud. **4**(1), 93–115 (2013)

34. Feil, J.A.: Cyberwar and unmanned aerial vehicles: using new technologies, from espionage to action. Case West. Reserve J. Int. Law **45**, 513 (2012)
35. Jolley, J.D.: Article 2 (4) and Cyber Warfare: How do Old Rules Control the Brave New World?. Available at SSRN 2128301 (2012)
36. Clarke, R.A., Knake, R.K.: Cyber war. HarperCollins (2011)
37. Gervais, M.: Cyber Attacks and the Laws of War. Berkeley J. Int. Law **30**(2) (2011)
38. McGraw, G.: Cyber war is inevitable (unless we build security in). J. Strateg. Stud. **36**(1), 109–119 (2013)
39. Robinson, M., Jones, K., Janicke, H.: Cyber warfare: Issues and challenges. Comput. Secur. **49**, 70–94 (2015)
40. Lindsay, J.R.: Stuxnet and the limits of cyber warfare. Secur. Stud. **22**(3), 365–404 (2013)
41. Junio, T.J.: How probable is cyber war? Bringing IR theory back in to the cyber conflict debate. J. Strateg. Stud. **36**(1), 125–133 (2013)
42. Liff, A.P.: The proliferation of cyberwarfare capabilities and interstate war, redux: liff responds to junio. J. Strateg. Stud. **36**(1), 134–138 (2013)
43. Erbacher, R.F.: 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, October 2005
44. Birdwell, M.B., Mills, R.: War fighting in cyberspace: evolving force presentation and command and control. AIR UNIV MAXWELL AFB AL AIR FORCE RESEARCH INST (2011)
45. Libicki, M.C.: Cyberwar as a confidence game. Strateg. Stud. Q. **5** (2011)
46. Brenner, S.W., Clarke, L.L.: Civilians in cyberwarfare: conscripts. Vand. J. Trans. Law **43**, 1011 (2010)
47. Swanson, L.: Era of cyber warfare: applying international humanitarian law to the 2008 Russian-Georgian Cyber Conflict. Loyola Los Angeles Int. Comp. Law Rev. **32**, 303 (2010)
48. Scott, A., Hardy, T.J., Martin, R.K., Thomas, R.W.: 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, August 2011
49. Roberts, S.: Cyber wars: applying conventional laws to war to cyber warfare and non-state actors. Northern Ky Law Rev. **41**, 535 (2014)
50. Dipert, R.R.: Other-than-Internet (OTI) cyberwarfare: challenges for ethics, law, and policy. J. Mil. Ethics **12**(1), 34–53 (2013)
51. Golling, M., Stelte, B.: 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, June 2011
52. Bachmann, S.D.O.V.: 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 (2012)
53. Danks, D., Danks, J.H.: The moral permissibility of automated responses during cyberwarfare. J. Mil. Ethics **12**(1), 18–33 (2013)
54. Friesen, T.L.: Resolving tomorrow's conflicts today: how new developments within the UN security council can be used to combat cyberwarfare. Naval Law Rev. **58**, 89 (2009)
55. Hunker, J.: Cyber war and cyber power. Issues for NATO doctrine (2010)
56. Hughes, R.: A treaty for cyberspace. Int. Aff. **86**(2), 523–541 (2010)
57. Solis, G.D.: Cyber warfare. Mil. Law Rev. **219**, 1 (2014)
58. Eom, J.H., Kim, N.U., Kim, S.H., Chung, T.M.: Cyber military strategy for cyberspace superiority in cyber warfare. In: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), pp. 295–299. IEEE, June 2012
59. Dycus, S.: Congress's role in cyber warfare. J. Nat. Secur. Law Policy **4**, 153 (2010)

60. Clemmons, B.Q., Brown, G.D.: Cyberwarfare: ways, warriors and weapons of mass destruction. Mil. Rev. **79**(5), 35 (1999)
61. Lupovici, A.: Cyber warfare and deterrence: trends and challenges in research. Mil. Strateg. Aff. **3**(3), 49–62 (2011)
62. Stytz, M.R., Banks, S.B.: Addressing Simulation Issues Posed by Cyber Warfare Technologies. SCS M&S Magazine. n (3) (2010)
63. Libicki, M.C.: Why cyber war will not and should not have its grand strategist. AIR UNIV MAXWELL AFB AL AIR FORCE RESEARCH INST (2014)
64. Huntley, T.C.: 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 Law Rev. **60**, 1 (2010)
65. Droege, C.: Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. Int. Rev. Red Cross **94**(886), 533–578 (2012)
66. Von Clausewitz, C.: On war, vol. 1. N. Trübner & Company, London (1873)

http://www.springer.com/978-3-319-57462-2

Intelligence and Security Informatics
12th Pacific Asia Workshop, PAISI 2017, Jeju Island, South Korea, May 23, 2017, Proceedings
Wang, G.A.; Chau, M.; Chen, H. (Eds.)
2017, VII, 151 p. 55 illus., Softcover
ISBN: 978-3-319-57462-2