







Model of Cyber Conflict Resolution in Indonesia

Qoriah Qoriah , Prima Roza , Agus Syihabudin , and Ade Engkus Kusnadi 

Fakultas Seni Rupa dan Desain, Institut Teknologi Bandung, Bandung, Indonesia
prima.roza@itb.ac.id

Abstract. There has been a growing concern regarding a recent phenomenon in the Indonesian cyber world, i.e., cyber conflicts among the country's users of communication technology. Internet users in many parts of Indonesia have little or no idea of the social, cultural, and legal effects of using the product of Internet, such as online news and social media platforms, in expressing their opinions. Internet users' lack of awareness or ignorance of the harms they may cause other Internet users are mostly related to hoaxes, fake news, and hate speech. Despite the enactment of the ITE Law (Information and Electronic Transactions) No. 11 of 2008, established to prevent adverse impacts on communities, the lack of its socialization and of the Internet users' awareness of ethics in communicating in cyberspace still cause concerns among Internet users, government, stakeholders, and society. Based on the linguistic behavior of the Internet users, this research, which is the first stage of a three-year study, is aimed at finding out what conflicts generally occur in the Indonesian cyber world by looking at the features of the Internet users and at mapping the patterns of the conflicts to be used in a later stage of study in which we will propose a conflict resolution model appropriate for building and maintaining peace and unity in the Indonesian cyber world. The method that we use for data collection and experimental research is Kozinet' netnography, i.e., ethnography done through internet media; the results will be used for mapping the conflicts. The overall results of this study are expected to produce an application of a language-based conflict resolution model that can curb the social, cultural, and legal problems in the society as a reaction of the development of information and communication technology.

Keywords: Cyber conflict · Language · Communication · Resolution Model

1 Introduction

Cyberspace is a tremendously powerful force with an exponential growth in the number of Internet users and individuals connected by mobile phones (Karatzogianni, 2006, p. 173). Along with the rapid growth of this technology, legal and social issues concerning the use of the Internet and social media are becoming part of the 21st century problem, which has led to a new kind of conflict: cyber conflict (Karatzogianni, 2006; Deutsch, 2006; Ghernaouti, 2013). Cyber conflicts can be interpreted as conflicts that occur in a computer-mediated world or computer-mediated environments (Karatzogianni, 2006), while Wilkinson (2015) defines 'cyber conflict' as a situation or state when there is an

occurrence of cyberattacks – a broad term which refers to a series of threats conveyed through computer networks.

There is a wide variety of cyberattacks. First, attackers can use certain software or algorithms that are deliberately designed to find the weakness of a system. Cyberattacks can also be social engineering (Ventre, 2012). The attacker ‘disguises’ himself or herself as a financial director who sends an email to his or her subordinates to immediately transfer money (usually in large amounts) to a certain account. Such attacks are known as cyber fraud. Another way is to condition a server to become over-loaded hence mal-function of its system. As a result, the website and network become inaccessible. The fourth and most widely reported cyberattack is phishing. Attackers send hundreds or even thousands of emails with attachments or links. If the recipient of the email opens the link or the email attachment, then the attacker will have access to the computer and all the data contained therein.

In addition to the above four ways, attackers also use software such as malware, spyware, ransomware or worms that are often infiltrated in attachments or other programs. If malware succeeds in entering a computer system, it will damage the system and even erase the data. If spyware gets into the system, it will record confidential information (e.g. passwords, credit card numbers, PINs and others). Ransomware will lock the data in a system, and then send a message stating that the owner of the data can have the locked data reopened if he or she pays a ransom. Meanwhile, the worm the attackers have planted will reproduce itself like a virus and send itself to all existing contacts in the computer hence spreading very quickly.

There have been many attempts by governments of various countries and different organizations to counter and reduce the impact of conflicts in the cyber world. For example, as quoted from www.washingtonpost.com, the German government has drafted a law that would impose a fine of up to € 50 million to social networks that fail to remove hate speeches or false news on the Internet platforms such as Facebook and Twitter.

Based on information from the website of the Indonesian Ministry of Communications and Information (Kemenkominfo), there are currently 63 million internet users in Indonesia. Of that number, 95 percent use the internet to access social networks. The most accessed social networking sites are Facebook and Twitter, and this makes Indonesia the 4th largest Facebook user after the United States, Brazil and India, and makes Indonesia the top 5 Twitter users in the world after the United States, Brazil, Japan and the United Kingdom.

Based on the facts mentioned above, with such a significant number of users of communication technology in this century, cyber conflict or conflicts in the cyber world in Indonesia has become inevitable. The problem of cyber conflict frequently found in the Indonesian cyber world has, hitherto, been related to social, cultural and legal aspects. Often the Internet users, especially of social media, have little or no understanding of the legal aspect of using social media as a means of expressing their opinion, that what they do on social media may potentially harm others, such as accidentally or deliberately spreading hoaxes, twisting facts, and spreading false news, or hate speeches. Despite the passing and enactment of the ITE Law (Information and Electronic Transactions) No. 11 of 2008 to prevent adverse impacts on communities, lacks of its dissemination by the government and lack of awareness of legal and ethical aspects of communicating in the

cyberspace are still causing concerns among internet users, governments, stakeholders, and society in general.

In a previous study by Karatzogianni (2006), the use of internet in politics has given rise to new lexicons, such as cyberwar, cyberattack and netwar. The term cyber conflict or 'cyber conflict' (CC) - is a common reference to a particular form of politics in the internet world. The term cyber conflict is now commonly used, though the coined terms are still opened to discussions as there are still problems regarding the definition and categorization of the large number of the incidents that occur in the cyberspace (Karatzogianni, 2006, p. 94). In this current study, the term cyber conflict is used to refer to conflicts in the real world that 'spill' into the cyber world or vice versa.

More specifically, the cyber conflict in this study will be limited to the conflicts that occur in the Indonesian cyber world, i.e. those related to news posted and shared on social media that have potentially contributed to the occurrence of cyber conflicts. The object of research is focused on the elements and the use of language on social media networks that are related to the conflicts. For example, prior, during, and following the Indonesia's 2014 presidential election, the Indonesian social media world had seemingly turned into a scene of conflict between supporters of both presidential candidates Prabowo Subianto and Joko Widodo. Supporters of each president candidate were involved in a 'war' on social media through comments and links that were not only notoriously provocative and potentially provoked verbal disagreements and harassment, but also led to ethnic, group and religious conflicts.

The potentials for conflict in the cyberworld did not stop with the fact that Joko Widodo won the election. The election of the Governor of Jakarta, which was left vacant after Joko Widodo was declared president-elect, posed a similar conflict in the world of social media in Indonesia, between the supporters of the then Jakarta deputy governor turning governor candidate Basuki Tjahaya Purnama and those against him. This incident even turned into one big legal case that have invited not only nation-wide but also international attention, i.e. the case of the Al Maidah verse 51 case. The case was triggered by the speech Basuki Tjahaya Purnama delivered, which was considered to have harassed the Surah Al Maidah verse 51. During the time of the trial of the prospective governor, the world of social media turned into an arena of cyberwars between the two opposing sides, those who considered him guilty and those not guilty. Scholars and linguists were summoned to testify as experts and to give their scientific and objective professional opinion as to whether the suspect, the governor candidate Basuki Tjahaya Purnama, has harassed the verse and committed blasphemy towards Islam.

There are still many cases that stem from verbal expressions in the world of social media which have been linked to legal aspects, even though not all of them ended in court. This fact, however, has raised concerns about conflicts that may potentially lead to national disintegration and threaten the unity of the nation of Indonesia.

2 Method

This research is a three-year qualitative study that focuses on the problem of conflicts in the cyber world with research questions formulated as follows: 1) what conflicts generally occur in the Indonesian cyber world, 2) What is the pattern or mapping of

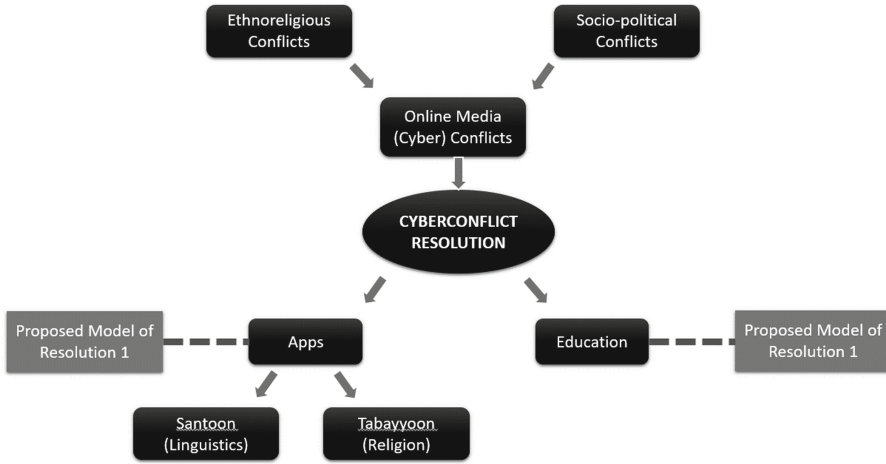


Fig. 1. Basic scheme of Research

conflicts that occur in the Indonesian cyber world, 3) which conflict resolution model is appropriate to build and maintain peace and unity in the cyber world as well as real world in Indonesia. To answer the questions, we have designed a basic scheme of the three years’ research as depicted in Fig. 1.

In terms of methodology, for the first year of study, this current year, this research follows Karatzogianni (2006).

- a. Textual: review of social media platforms, conflicts, literatures on media theory and information, studies in religion and culture.
- b. Theoretical: the use of cyber conflict theory, cyberpragmatic approach, and Applied Linguistic for Peace (Constructive Communication) approach that will be integrated into a single resolution model.
- c. Empirical level of the first year’s stage of study (out of three), for the purpose of mapping the cyber conflict, this research has used Kozinet’s netnography, i.e. by collecting data using internet. The data were collected from more than 2020 mentions of keywords in articles published by 4 Indonesian online media for the period between 1 January 2018 until 2 July 2018 and shared on social media and other web sources with details as follows.
 - i. Firstly, researchers set specific keywords to locate articles related to cyber conflicts based on preliminary data collected using Buzzsumo search engine. The researchers have tried to find out which online media in Indonesia and what topics have the highest engagements with internet users, i.e. users of social media platforms such as Facebook and Twitter, which have been linked to cyber conflicts.
 - ii. Based on the results of the search using Buzzsumo, the researchers, then, used another search engine <http://dashboard.nolimit.id> to collect the information of the articles with details covering:

- Name of online media as sources of articles
 - Date of articles published
 - URLs
 - Titles of articles
 - Contents of articles
 - Geographical location of articles
 - Keywords used for searching articles
- iii. The results were then processed into a readily available data that serve the purpose of identifying and mapping of the cyber conflicts on this research website: <http://www.demosof.com/konflik>.
- d. Analytical: the components comprising the integrated theories and the proposed resolution model are linked with the empirical evidence; this research also attempts to develop the model to become applicable for resolving the cyber conflicts.
1. For the upcoming stages of research, i.e. the second year (2018–2019), the researchers have planned to use the following methods:
- a. Theoretical: uses of studies and theories related to society and behavior of social media and or Internet users, as well as elements considered crucial for cyber conflict analysis. Critical Discourse Analysis (CDA) method will be used to analyze the data collected by using virtual ethnography, both primary data in the form of interviews and experiments, as well as secondary data available in cyberspace. CDA is an inter-disciplinary approach for researching discourse that views language as a form of social practice. The purpose of CDA analysis is to provide an explanation of the linguistic-discursive dimension of social and cultural phenomena as well as the process of changing modernity at this time, “(Jorgensen, & Phillips: 2002). One type of analysis that can be used on CDA is multimodality, an interdisciplinary approach that defines communication and representation beyond more than just language. This method has been developed in the last decade to systematically answer the much-debated questions about changes in society, for example in relation to new media and technology (C. Jewit, 2009).
 - b. Empirical: creating an application or a feature as a tool to avoid or resolve cyber conflicts. A model of verbal and visual means of communication of social media users to build and maintain peace and reduce/prevent cyber conflicts. The cyber conflict resolution model is based on language with the purpose of improving constructive communication skills. At this research stage, this conflict resolution model is more than just a concept; it has become a model modified according to Ventre’s OODA conflict resolution model (Observe, Orient, Decide, Act) loop (2011).
2. The method used for the third year (2019–2020) research will be

- a. Theoretical: uses of Ventre's Cyberpragmatic and de Matos' Applied Linguistics for Peace approaches, i.e. Constructive Communication.
- b. Empirical, deemed suitable for disseminating/socializing the feature/application of the cyber conflict resolution model among internet users, i.e. by conducting experiments among Internet users. The application/feature as the cyber conflict resolution model resulted from the second-year research will be used in the experiment. In its future development, this cyber-conflict resolution model can be realized as an application model that can be used on word processor or entry/post system on social media, either through computers or on mobile phone gadgets.

By conducting the overall three-year research scheme, it is expected that the result of this research will provide positive impacts of social and scientific benefits as follows:

1. Improved awareness/learning about ethics and law concerning behavior in the cyber world.
2. More discussions (discourses) related to conflicts in the cyber world.
3. Actual actions for conflict resolution by users and providers of Internet services, government, or other relevant institutions.
4. Educational, cultural, and social programs that can curb the problems related to the internet world in Indonesia.

2.1 Theory of Conflict

A lot of research related to conflict, language, and conflict resolution has been conducted in various countries. The aim is to improve understanding of the relationship between language, peace, and conflict resolution through various approaches, insights, and interdisciplinary practices. Research on conflict resolution through linguistic approach aims to integrate languages, peace, and conflict resolution as an approach to understanding, preventing, monitoring, overcoming, and, if possible, eliminating forms of communicative violence from individuals and the society.

Another scholar, a researcher from Portugal, Gomes de Matos (2001), has undertaken numerous studies using Applied Linguistics for Peace (ALP) approach. One of his researches focuses on the relation between conflict, resolution, language, and education (pedagogy of positiveness) applied to diplomatic communication. In 2005, Gomes de Matos conducted more specific research on the use of language of peace or peaceful language, which resulted in what he calls Constructive Communication (CC).

Gomes de Matos (2002) has posed an empirical question as to whether such efforts can be effective as a tool of social change. The implications lead to the use of the language of peace in human rights education and responsibility - a dimension that still requires extensive exploration. de Matos' formulation is the most fundamental integration of three basic human rights, namely, the right to live in peace, the right to study, and the right to communicate. From this concept comes the interpretation and addition of the concept of conflict resolution: humans must have the right/responsibility to learn to communicate peacefully in various social contexts, especially in challenging and life-threatening situations. The right to constructively communicate is largely ignored in

schools and other educational institutions. This negligence can be dangerous for social life and requires immediate change.

This research is a linguistic study that addresses the issue of cyber conflict as explained above, while applying several theories to serve the purpose. Conflict Theory is one of the main foundations in this study. The conflict theory used in this is neither that of Marxist conflict that focuses on political-economic aspect nor modern conflict theory as a result of the development of Marxism which includes Critical theory, feminism theory (approach with gender equality focus on politics, social, and economy), Postmodern theory (approach which is a criticism of modernism) Postcolonial theory, etc.

Instead, the conflict theory used in this study departs from the specific theory of cyber conflict by Karatzogianni (2006) who has classified cyber conflict into two major categories: (1) Socio-political conflicts and (2) ethno-religious conflicts. In cyber conflict, the political environment of the Internet is analyzed not in the Internet corridor as a mass media in the traditional sense, but rather as a significant new resource used by opposing parties in a conflict. Until now there has been no theoretical model that can be a conceptual tool for analyzing the use of the Internet by actual or real parties involved in an endogenous conflict, but following Karatzogianni, this research is an attempt to prove and develop theories about how media influence - or not - the outcome of a conflict in the two categories of cyber conflict.

1. Socio-political Conflict

This conflict has a major issue about netwar conflict or warfare networks of hacktivists who are concerned with global issues such as the environment and those who are less willing to negotiate with the government. The primary objective of hacktivists is to influence or invite/challenge public opinion, or opponents, and fight for control of media access and coverage. What hacktivists do are usually in the form of cyber-attacks, usually an attack of denial of service and damage to a certain web or web defacements.

Another researcher, Jordan (2001) has mapped cyber conflicts into the Mass Virtual Direct Action (MVDA): the simultaneous use of many Internet users to create electronic civil disobedience. This action, hacktions, is not intended to permanently stop a target, but for something symbolic. The perpetrators of hacktion rarely hide their identity; they tend to seek opportunities for general debate and discussion. Secondly, Individual Virtual Direct Action (IDVA) is a hacking action perpetrated by an individual and does not depend on mass protests. These actions can be semiotic or semiotic attacks (defacement), computer intrusion, or network security or network security.

2. Ethno-religious Conflict

The increasing importance of cyber conflict becomes more significant when cyber conflicts reflect real-world conflicts (real world as opposed to cyberspace), for example, the Palestinian-Israeli conflict. Hackers from both sides attack each other's website. They send racist messages, disrupt the computer systems of others and spread propaganda. Another example is the cyber conflict that occurred after an international diplomatic incident between the Chinese government and the American government over the landing of an unmanned US spy plane on Chinese soil. The parties involved

in ethno-religious cyber conflicts rarely use the internet as an effort to mobilize or influence public support. Instead, they use it as a weapon hence the term net warriors; they usually consist of cyber activists that tend to commit acts of violence, i.e. terrorists and criminals, or social activists who can be militant but can also be reconciled. Another researcher, Gadi Wolsfeld (*Media and Political Conflict, 1997*) mentions that there are three variables that drive the ability of antagonists to control the political environment and, in turn, increase the opponent's ability to dominate public discourse on certain issues, for example:

- ability to start and control
- the ability to regulate the flow of information
- ability to provide support

Socio-political cyber conflicts start a newsworthy event by placing others to defensive, sending stories around the world, spreading information out of control and mobilizing support through frames or frame formations as alternate frames for an event. On the other hand, in ethno-religious conflict, conflicting parties tend to use the internet as a weapon. Although they can initiate an action, they fail to understand the effort to promote an alternative. Not infrequently they also conduct attacks against the enemy or defend themselves over their electronic territory.

2.2 Cyberpragmatics

How information is produced and interpreted within the internet environment is the main interest of cyberpragmatics. In addition, how users access contextual information, which is often limited compared to face-to-face conversations, to complete the gaps of information between what users type in to the computer and what they really intend to communicate (Yus, 2011. P. 13).

Communicative exchanges occurring among internet users through the use of various cyber-media are analyzed in cyberpragmatics. By accessing the necessary contextual information "sender-users" can foresee that speakers will make the right conclusions. Likewise, "addressee-users" will seek for relevance in various form of communication (utterances, images, voices and sounds, etc.) that they process. Thus, context is deemed equally essential in both the production and interpretation of information on the internet and in face-to-face interactions (Yus, 2011, p 14). The scheme can be seen in Fig. 2.

Another important aspect in cyberpragmatics is politeness, a conventional strategy used by human beings to nurture their relations with other human beings as well as to soften the impact of certain deeds on other people. Every culture, according to Yus (2011), has its own unique expression of politeness, implying that every language also has a different means of conceptualizing the world and the relationships among individuals within speech communities (which includes virtual communities and networks).

Politeness is, therefore, a social behaviour that specifies the existence the community. It is a strategy used by the community to reveal which speakers do not belong to them and which disregard. The inherent rules of politeness which are commonly adopted and shared by its members (Yus, 2011, p. 255). The expression of politeness on the internet is deemed common and essential. It shows the importance beyond face-to-face

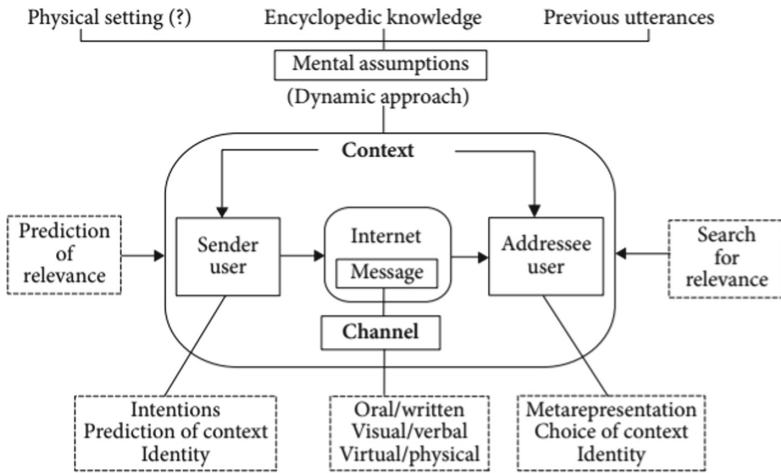


Fig. 2. Internet-mediated communication according to cyberpragmatics (Yus, 2011, p. 15)

interactions. Politeness on the Net is called netiquette (from net and etiquette), and it is applicable to internet-mediated communication as well. The politeness is also important in the interactions using electronic messages and utterances in environments such as chat rooms in which users can choose the strategies of politeness to comply with the official standards of social etiquette (Yus, 2011, pp. 256–258).

2.3 Applied Linguistics for Peace (ALP): the Relationship Between Language, Conflict Resolution, and Peace

According to Paul A. Chilton in Sue Wright’s book, *Language and Conflict: A Neglected Relationship* (1998) network-based conflicts will be a major phenomenon in the future as a result of dysfunction in communication. In other words, this cyber-conflict also includes conflicts in language usage: textual, visual, audio, and gestural. In term of the use of textual languages, for instance, Gomes de Matos (2001) has conducted many studies using Applied Linguistics for Peace (ALP) that sees the importance of the relation between conflict, resolution, language, and education (pedagogy of positiveness) applied to diplomatic communication. In 2005, Gomes de Matos conducted more specific research on the use of the language of peace or peaceful language, which then produced Constructive Communication or Constructive Communication (CC).

Crystal and Crystal (2000) argue that the field of linguistics can be very diverse, ranging from the nature of language-analysis of structure, diversity, function, meaning, form-through usage and consequently (friendly/unfriendly). Language as the main study of Linguistics is the way humans convey ideas, emotions, and desires through a consciously generated symbol system (Sapir, [1921] 2001). Language is a cognitive system that is part of the mental and psychological structures of humans. It is a mental power to create meaning of peace and solve problems. This reflects that we are cognitive, communicative, creative, and peace-building users (Deutsch, 2016). Conversely, language can also be used as a weapon (Crystal and Crystal, 2000).

Linguistics is the science of language. Applied Linguistics (AL) is an interdisciplinary field of study that examines language-related issues such as language learning and literacy, literature, language contact, language policy and planning, language pathology, and language usage. The interest of linguistics on the aspects of conflict-related language use and peace has grown and evolved with the increasing importance of issues of peace and conflict in the field of social and political sciences and along with the diversity of approaches in the scientific research of Applied Linguistics. Linguistics for peace is a growing approach focusing on the use of language to build peace/nonviolence and an emphasis on “respect for the dignity of individual and community language users” (Crystal, 1999). As part of Applied Linguistics, Applied Peace Linguistics (APL) is defined as an interdisciplinary approach aimed at helping the educational system create conditions that can prepare humans as the language-builder of peace.

2.4 Nonviolent Communication (NVC): Constructive Communication

Gomes de Matos (2005) states that one of the first known Conflict Resolution Approaches or CRA is Nonviolent Communication (NVC), based on a conceptual repertoire: appreciation, compassion, conflict, feeling/not feeling, judgment, need, positive action, responsibility, and vocabulary (concerning feeling).

The core concept of NVC is translated through a simple way of bringing the two approaches closer, i.e., by adding the adjective “communicative” to each of the concepts in the NVC system. The addition of the word ‘communicative’ adds a special meaning to the NVC and becomes a reminder for language users that peace in/through language is a wide and varied area.

Another contribution from NVC to APL is two vocabulary lists to describe feelings (Rosenberg, 2003). The first list contains adjectives that represent positive feelings (needs fulfilled) that serve as a list of communicative responsibilities. Language users are challenged to be communicative, affectionate, cheerful, free, friendly, kind, loving, optimistic, peaceful, fun, gentle, and warm.

The second list of Rosenberg is focused on negative feelings (needs are not met). Thus, language users can use it as a reminder of what they should avoid in interacting with their fellow human beings. Such a list of preventive/self-monitoring checklists includes, among others, communicative: anger, bitterness, despair, sadness, hostility, impatience, irritation, pessimism, resentment, surprise, and misery (Gomes de Matos, 2005).

The third inspirational insight from NVC that linguists can apply to peace is the translation of vocabulary and judgmental expression into a non-judgmental vocabulary and promoting peace. Provocatively, Rosenberg made a case against the use of the word “should” that caused embarrassment or guilt. He argues that “these violent words, which we normally use to evaluate ourselves, are so deeply embedded in our consciousness that many of us cannot live without those words” (Rosenberg, 2003). Whitney and Trosten-Bloom (2003) argue that from a linguistic perspective of peace, words can create the world of words create worlds and that language has the power to create social change and reality.

Good communication is a communication that is aimed at the good of mankind. Gomes de Matos (1996) lists and instructs on how to communicate constructively (in Portuguese) (Table 1).

Table 1. De Matos' List of How to communicate constructively

A. How to interact positively	
1	Help integrate potentially conflicting perspectives
2	Be nice to linguistic neighbors.
3	Giving reactions with responsibilities
4	Interact for the common good
5	Find out as much as you can about the values and beliefs of the neighbors
6	Ask for constructive feedback.
7	Make a positive question

Table 2. de Matos' List of How to write constructively

B. Questions to consider when writing constructively	
1	What constructive knowledge do I have about the reader who reads my writing?
2	How can I contribute to individual groups?
3	What constructive values do I communicate / enhance / prioritize? How to?
4	What constructive vocabularies should I change in order to communicate more constructively? How to?
5	What contributions can my writing give to the communicative, cultural, ecological, economic, ethical, moral, political, social, and spiritual conditions of the readers and myself?

De Matos (1996) also proposes constructive writing. The underlying constructive written communication guide is the belief that good writing is writing for the benefit of authors and readers, and more broadly, the good of national or regional, or international groups or communities. He lists the following questions used in a Constructive Writing workshop material that attracts the attention of Peace Linguists (Table 2):

The constructive communication approach (CC) of Gomes de Matos (1996 and 2002) also contains guidance on how to read and listen in a positive (or constructive) way, how to positively criticize, how to interact with positively older people, and how to use linguistics as a tool positive communication. This suits our research purpose to propose a conflict resolution model that is based on language as an effective tool for communicative communication, both verbally and written.

2.5 The Concept of Tabayyun in Islam

The term *tabayyun* is derived from the Arabic word *bana-bayanan-tibyanan* which, according to Al-Munawwir Arabic-Indonesian dictionary, literally means 'visible, clear, and bright'. According to Shihab, the word *fatabayyanu* means 'thoroughly examine' (2002, p.678). Mushthafa defines *tabayyun* as 'seeking clarity' (1986, pp. 209), while

Wahid defines *tabayyun* as ‘to make clear and clarify a case or to seek for the origin of an event before arguing in disagreement (1998, p.xiv). According to Kamus Besar Bahasa Indonesia *tabayyun* is an understanding or explanation.

The term *tabayyun*, therefore, semantically means seeking the clarity about something until it is proven clearly true. In relation to the new phenomenon of the spreads of hoaxes, fake news, and hate speech, the term *tabayyun* means conducting research and being selective in responding to news, while being wise and not rushing into making a decision in curbing a problem, and at the same time taking into consideration the aspects of law and policy until the news is clearly true hence no one should feel tarnished or hurt (Anwar 2018 on <http://Discourse in Anwar>” Blog, Saturday 5 September 2009).

Tabayyun is a noble *Akhlaq* which is an important principle in upholding the purity of Islamic teachings and maintaining the harmony. The authenticity of hadiths, the words of the Messenger of Allah, for instance, can be validated among others because the Islamic scholars have applied the principle of *Tabayyun* in receiving news. Similarly, in the social life of the society, one will avoid misunderstanding or enmity and even bloodshed, among others, because he or she performs the *Tabayyun* well. Therefore, Allah commands the believers to keep *Tabayyun* in receiving and responding to news conveyed to them hence no regret in the future.

In Alquran Surah al-Hujurat/49:6 it is stated:

يَا أَيُّهَا الَّذِينَ آمَنُوا إِن جَاءَكُمْ فَاسِقٌ بِنَبَأٍ فَتَبَيَّنُوا أَن تُصِيبُوا قَوْمًا بِجَهَالَةٍ فَتُصِبُوا عَلَىٰ مَا فَعَلْتُمْ نَادِمِينَ

‘O ye who believe! If a wicked person comes to you with any news, ascertain the truth, lest ye harm people unwittingly, and afterwards become full of repentance for what ye have done.’

Based on the explanation above, this research uses the *tabayyun* principle in creating one of the applications/features to resolve cyber conflicts, especially those on social media, taking into account the following rationale:

1. This verse is an *adab* lesson for believers in receiving and responding to an issue or news that is not yet clear.
2. The implementation of performing *tabayyun* following the command is an *ibadah* or service that can increase one’s faith, and therefore ignoring *tabayyun* can reduce faith.
3. The obligation to perform *tabayyun* shall be borne by the person receiving the news and who will pass judgement to the suspected or accused.
4. Violation to the command to perform *tabayyun* can lead to ruining personal relationships and the society. Neglecting the obligation to perform *tabayyun* can cause people to act stupidly.
5. Violation to the command to perform *tabayyun* can lead to ruining personal relationships and the society or social relationships and the entire community.
6. Regrets in the world and the hereafter life will be inflicted on the person who receives and spreads the negative issue and to the person who passes judgements without performing *tabayyun* beforehand.

3 Results and Discussion

As mentioned before, this current research is part of a three-year study. In the first year, the result expected is a mapping of the cyber conflict data in Indonesia, as depicted on online media and the online media users' internet engagements related to the keywords used as the criteria for obtaining the data. Based on the data collected using Buzzsumo from 1 January 2018 until 2 July 2018, it was found that there are four main online media that have shown the highest number of Internet engagement among users, which were deemed to have led to cyber conflicts. i.e. detik.com (approx. 30%), tribunews.com (approx. 26%), kompas.com (approx. 23%), and viva.co.id (approx. 21%). The result can be seen in Fig. 3.

The data from these media are then categorized using a prototype of web-based application which has a user-friendly interface to make it easier for researchers to take maximum advantage of this database resource (Fig. 4).

Following the result of the sources of data of online media, detailed data of the articles were obtained using <http://dashboard.nolimit.id> with details as follows:

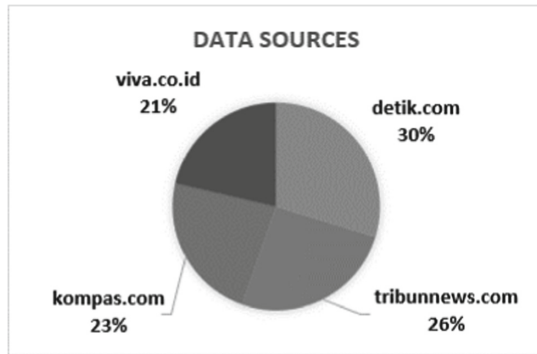


Fig. 3. Sources of Online Media Articles

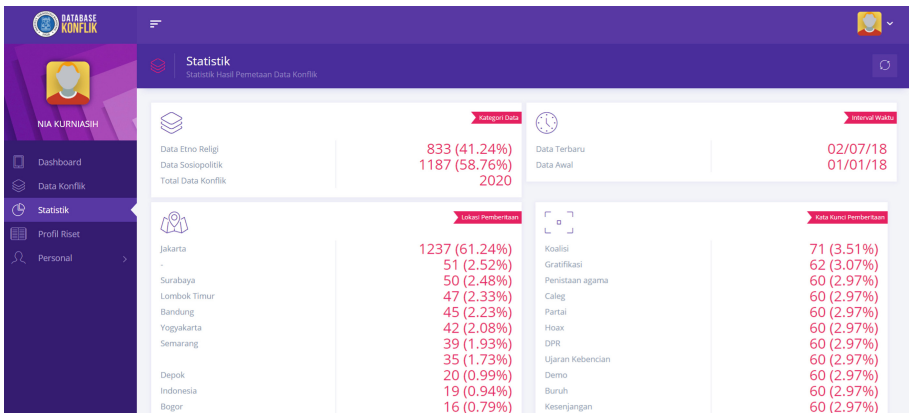


Fig. 4. Web of research data collection results

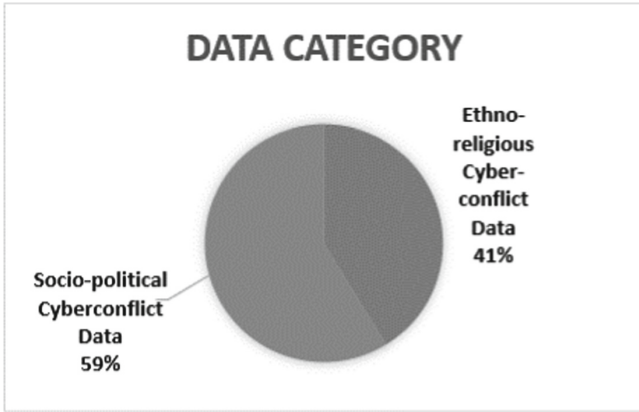


Fig. 5. Data Category of Cyber conflict

3.1 Category of Cyber Conflicts

Based on the category of cyber conflict, as can be seen in Fig. 5, the frequency of mention or internet engagement on online media related to ethno-religion cyber conflicts comprises 833 or 41.24% out of the total 2020. The frequency of mention of 1187 or 58.76% out of the total 2020 mentions or Internet engagements by Internet users on the online media. This shows that the socio-political issues have a bigger proportion of mentions in the cyber world in Indonesia.

3.2 Location of Articles Published on Online Media

Based on the location mentioned in the articles, it can be seen in Fig. 6 below that the city with the highest mention in the articles posted on online media in Indonesia that have potentially led to cyber conflicts are Jakarta: 1237 mentions or 61.24% of the total 2020 total data, plus 51 implicit mention, which comprises an additional 2.52% to it. The other locations that come after Jakarta in the frequency of mentions are Surabaya with 50 (2.48%) mentions; East Lombok (Lombok Timur) with 47 (2.33%) mentions, Bandung 45 (2.23%) mentions, Yogyakarta 42 (2.08%), Semarang with 39 (1.93%) plus 35 (1.73%) implicit mentions. The rest of the locations comprise a respective percentage below 1, with a total of 259 mentions. There are some locations geographically out of Indonesia, but the data shown these places were parts of the cyber conflicts in Indonesia, such as Kuala Lumpur, Washington, Gaza, overall comprising 128 mentions. It is evident that in terms of cyber conflict, the issues can invite comments and Internet engagements beyond geographical borders.

3.3 Frequency of Keywords Mentioned on the Online Media

Based on the frequency of keywords mentioned in the articles, it can be seen in Table 3 that the keywords with the highest mention in the articles posted on online media in Indonesia that have potentially led to cyber conflicts are *koalisi* 'coalition': 71 mentions

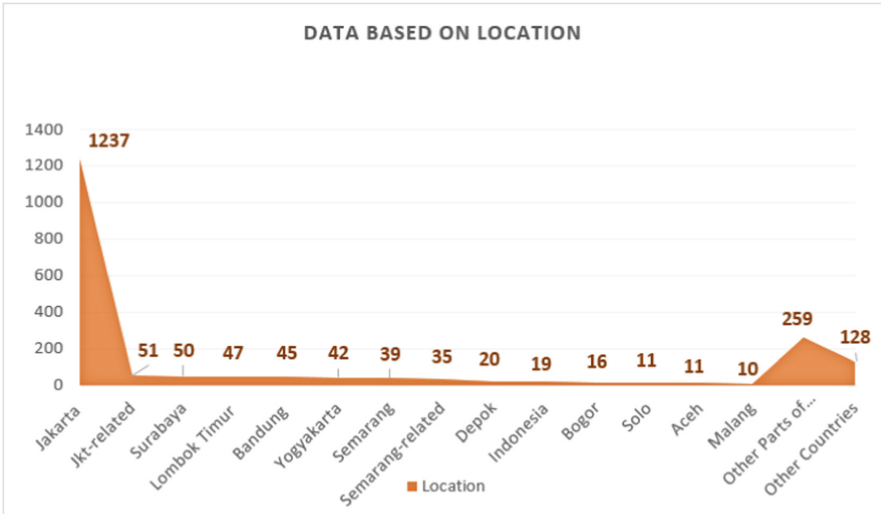


Fig. 6. Location Mentioned in the Articles of Online Media

or 3.71% of the total 95 total data of keywords. It is followed by the keyword *gratifikasi* 'gratification' with 62 mentions or 3.07%; next are keywords that have a frequency of respectively 60 (2.97%) mentions: *penistaan agama* 'blasphemy', *caleg* 'legislative candidate', *partai* 'party', hoax, DPR 'House of Representatives', *ujaran kebencian* 'hate speech', *demo* 'demonstration', *buruh* 'labour', *kesenjangan* 'discrepancy', and *provokasi* 'provocation'. The rest of the data can be seen in Table 3.

Based on the theories and approaches we have explained above, i.e., cyberpragmatics, the concept of *tabayyun*, and Applied Linguistics for Peace or Constructive Communication, and the empirical data obtained from the internet, this research proposes the following Model for Cyber conflict Resolution:

As can be seen in Fig. 7 the data of both ethno-religious cyber conflicts and socio-political cyber conflicts will be analyzed using virtual ethnography prior to designing the resolutions, i.e. applications (both linguistic apps and religious apps) and a form of education for internet users.

The stage of designing and creating the apps and the kind of educational practice will be performed according to the principle of politeness (netiquette) as proposed in cyberpragmatics. The apps will consist of verbal, visual, and auditory linguistic features that will help lessen the impacts of unwanted posts or posts and comments that may potentially violate the politeness principle hence conflicts among Internet users. The elements of local culture and languages will be key points in the design due to the diversity of the Internet users in Indonesia which consist of thousands of ethnicities and local languages. The feature/apps related to religion will be designed according to the principle of *tabayyun*, comprising Islamic teachings, shared values, examples of practices, etc. in the form of verbal, visual, and auditory languages.

Lastly, the result of the data will be used as a subject in character building. It will be based on the principle of the national ideology, social values, and cultural values.

Table 3. Frequency of Keyword Mentions

No.	Keywords	Number of Mentions	Percentage
1.	Koalisi	71	3,51%
2.	Gratifikasi	62	3,07%
3.	Penistaan agama	60	2,97%
4.	Caleg	60	2,97%
5.	Partai	60	2,97%
6.	Hoax	60	2,97%
7.	DPR	60	2,97%
8.	Ujaran Kebencian	60	2,97%
9.	Demo	60	2,97%
10.	Buruh	60	2,97%
11.	Kesenjangan	60	2,97%
12.	Provokasi	60	2,97%
13.	Politik uang	59	2,92%
14.	Pencemaran Nama Baik	59	2,92%
15.	Teroris	57	2,82%
16.	Fitnah	56	2,77%
17.	Syiah	54	2,67%
18.	KKN	53	2,62%
19.	Pencitraan	53	2,62%
20.	HTI	52	2,57%
21.	Jihad	50	2,48%
22.	Perbuatan tidak menyenangkan	50	2,48%
23.	Kafir	49	2,43%
24.	Khilafah	49	2,43%
25.	Islam nusantara	47	2,33%
26.	Legowo	46	2,28%
27.	Manipulasi	45	2,23%
28.	Ahmadiyah	44	2,18%
29.	Persekusi	42	2,08%
30.	Pribumi	37	1,83%
31.	Tabayyun	34	1,68%
32.	Cina	32	1,58%

(continued)

Table 3. (continued)

No.	Keywords	Number of Mentions	Percentage
33.	Bubarkan	32	1,58%
34.	Sesat	30	1,49%
35.	Ekstrim	26	1,29%
36.	Makar	23	1,14%
37.	Pluralisme	21	1,04%
38.	Misionaris	18	0,89%
39.	Bumi Datar	17	0,84%
40.	Sekuler	17	0,84%
41.	Liberal	14	0,69%
42.	Islamofobia	13	0,64%
43.	Wahabi	11	0,54%
44.	Fanatik	11	0,54%
45.	Khilafah#HTI	8	0,4%
46.	Sumbu Pendek	8	0,4%
47.	Aliran sesat	6	0,3%
48.	Kristenisasi	4	0,2%
49.	Ahmadiyah#Aliran sesat#Sesat	3	0,15%
50.	Kafir#Jihad	3	0,15%
51.	Ahmadiyah#Persekusi	3	0,15%
52.	Aliran sesat#Sesat	2	0,1%
53.	Fitnah#Tabayyun	2	0,1%
54.	Tabayyun#Fitnah 2	2	0,1%
55.	Syiah#Jihad 2	2	0,1%
56.	Fanatik#Teroris 2	2	0,1%
57.	Fanatik#Jihad 2	2	0,1%
58.	Kafir#Jihad#HTI	1	0,05%
59.	Khilafah#Jihad 1	1	0,05%
60.	Ahmadiyah#Tabayyun	1	0,05%
61.	Kristenisasi#Jihad	1	0,05%
62.	Kafir#HTI	1	0,05%
63.	Khilafah#Liberal#HTI	1	0,05%
64.	Islamofobia#Ekstrim	1	0,05%

(continued)

Table 3. (continued)

No.	Keywords	Number of Mentions	Percentage
65.	Sekuler#Islam nusantara	1	0,05%
66.	Kafir#Islam nusantara	1	0,05%
67.	Aliran sesat#Teroris#Sesat	1	0,05%
68.	Fitnah#Jihad	1	0,05%
69.	Syah#Wahabi	1	0,05%
70.	Islamofobia#Teroris	1	0,05%
71.	Kafir#Jihad#Islam nusantara	1	0,05%
72.	Tabayyun#Fanatik	1	0,05%
73.	Fitnah#Teroris	1	0,05%
74.	Syah#Sekuler	1	0,05%
75.	Kafir#Islamofobia#Fitnah	1	0,05%
76.	Tabayyun#Penistaan agama	1	0,05%
77.	Syah#Tabayyun#Fitnah	1	0,05%
78.	Teroris#Khilafah	1	0,05%
79.	Kafir#Fanatik	1	0,05%
80.	Wahabi#Syah	1	0,05%
81.	Ekstrim#Liberal	1	0,05%
82.	Teroris#Khilafah#Jihad	1	0,05%
83.	Islam nusantara#Penistaan agama	1	0,05%
84.	Kafir#Ekstrim	1	0,05%
85.	Sesat#Jihad	1	0,05%
86.	Wahabi#Teroris	1	0,05%
87.	Syah#Kafir#Teroris	1	0,05%
88.	Teroris#Khilafah#Islam nusantara	1	0,05%
89.	Sesat#Penistaan agama	1	0,05%
90.	Jenggot Panjang	1	0,05%
91.	Kafir#Penistaan agama#Jihad#HTI	1	0,05%
92.	Ahmadiyah#Aliran sesat	1	0,05%
93.	Sesat#Aliran sesat	1	0,05%
94.	Liberal#Jihad	1	0,05%

The purpose is to raise the awareness of Internet users in maintaining the unity of the Indonesian nation through Applied Linguistic for Peace approach.

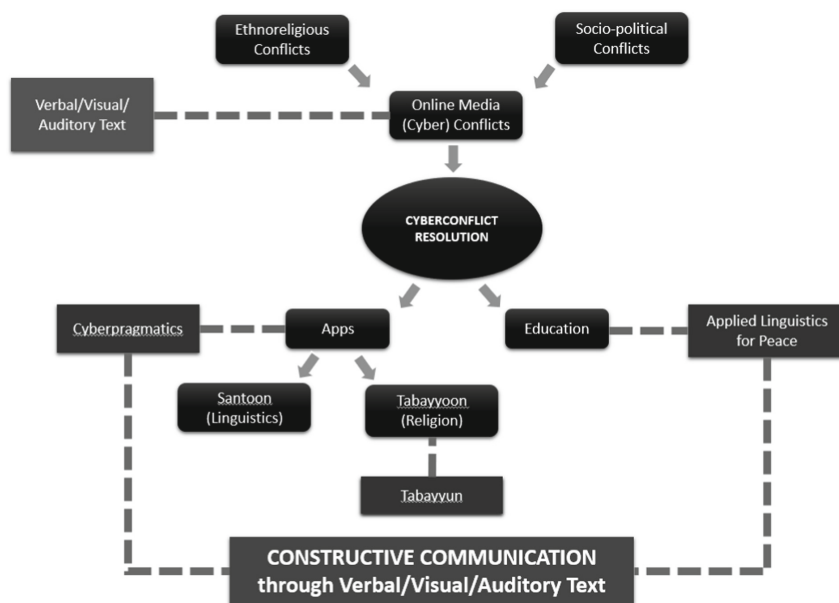


Fig. 7. Language-based Cyber conflict Resolution Model

4 Conclusion

To conclude, this three-year qualitative study is an attempt to curb the problem of cyber conflicts that may potentially harm the unity of the Indonesian people as Internet users. This research has identified and mapped the conflicts that have occurred in the Indonesian cyber world by examining the linguistic behavior of the Internet users. This paper is proposing a new resolution model that is based on language due to the unique and highly diverse characteristics of the Internet users in Indonesia. It follows the notion that the resolution model should be appropriate for improving the constructive communication skills of the internet users and for building and maintaining peace and unity in the cyber world as well as the real world in Indonesia.

References

- Al-Maraghi, Ahmad Mushthafa: Tafsir Al-Maraghi. Semarang: CV Toha Putra (1986).
- Coulthard, Malcolm & Johnson, Alison: The Routledge Handbook of Forensic Linguistics. London: Routledge (2000).
- Deutsch, Morton, Coleman, Peter T., Marcus, Eric C. Ed.: The Handbook of Conflict Resolution Theory and Practice. San Fransisco: Jossey-Bass (2006).
- Gheraouti, Solange: Cyber Power: Crime, Conflict and Security in Cyberspace. Lausanne. EPFL Press. (2013).
- Gomes de Matos, F.: Applying the Pedagogy of Positiveness to Diplomatic Communication in M. Kurbalija and H. Slavik (eds.). Language and Diplomacy. University of Malta: Mediteranean Academy of Diplomatic Studies. . (2001).

- Gomes de Matos, F.: Teaching Vocabulary for Peace Education. *ESL Magazine*, July/August. (2002).
- Gomes de Matos, F.: Using Peaceful Language: From Principles to Practices. In *UNESCO-OELSS Online Encyclopedia*. (2005).
- Gomes de Matos, F.: Language, Peace, and Conflict Resolution in Deutsch, Morton, Coleman, Peter T., and Marcus, Eric C. (eds) *The Handbook of Conflict Resolution. Theory and Practice*. San Fransisco: Jossey-Bass. (2006).
- Halliday, M.A.K.: *An Introduction to Functional Grammar*. London: Edward Arnold. (1985)
- Hine, Christine: *Virtual Ethnography*. London: Sage Publications. (2000).
- Jewitt, C. (ed.) *The Routledge Handbook of Multimodal Analysis*. London: Routledge. (2009)
- Jorgensen, Marianne & Phillips, Louise: *Discourse Analysis as Theory and Method*. London: Sage Publications Ltd. . (2002).
- Jordan, Tim: Mapping Hacktivism, Computer Fraud and Security: Mass Virtual Direct Action (MVDA), Individual Virtual Direct Action (IVDA) and Cyber Wars. *Computer Fraud and Security*. 4. Pp 8-11. . (2001).
- Karatzogianni, Athina.: *The Politics of Cyberconflict*. New York: Routledge. (2006).
- Karatzogianni, Athina & Kuntsman, Adi. (Ed.): *Digital Cultures and the Politics of Emotion: Feeling, Affect, and Technological Change*. New York: Palgrave Macmillan (2012).
- Kelly, Michael and Baker, Catherine: *Interpreting the Peace: Peace Operation, Conflicts and Language in Bosnia-Herzegovina*. London: Palgrave Macmillan. . (2009).
- Kozinet, R.V.: *Netnography. Doing Ethnographic Research Online*. California: Sage Publication. (2010).
- Kress, G.: *Multimodality: a Social Semiotic Approach to Contemporary Communication*. London: Routledge. (2009).
- Masiola, Rosano & Tomei, Renato: *Law, Language and Translation: from Concepts to Conflicts*. New York: Springer. (2015).
- Matoesian, Gregory M.: *Routledge Handbook of Forensic Linguistics*. New York: Routledge. (2010).
- Piliang, Yasraf A.: *Semiotika dan Hipersemiotika: Kode, Gaya, & Matinya Makna*. Jakarta: Matahari (2012).
- Rosenberg, Marshall: *Nonviolent Communication: A Language of Life: Life Changing Tools for Healthy Relationship*. California: PuddleDancer Press. (2003).
- Shihab, M. Quraish: *Tafsir Al-Misbah*. Jakarta: Lentera Hati. (2002).
- Siddiq, Muhammad Rafi: *Peace, Conflict, and Language: Coping with Linguistic Intolerance and Violence* MA TESOL Collection. Paper 715. (2016).
- Ventre, Daniel. Ed.: *Cyberwar and Information Warfare*. New Jersey: John Wiley and Sons. . (2011).
- Wahid, Abdurrahman: *Tabayyun Gus Dur*. Yogyakarta: LKiS Yogyakarta (1998).
- Whitney, Diana Kaplin and Trosten-Bloom, Amanda: *The Power of Appreciative Inquiry: A Practical Guide to Positive Change*. San Fransisco: Berrett-Koehler Publishers. . (2003).
- Wilkinson, David: *The Strategy of Cyber conflict: Quantifying and Reducing Cyber-Risk - Effective Deterrence* . (2015).
- Wolsfeld, G.: *Media and Political Conflict*. Cambridge: Cambridge University Press. (1997).
- Yus, Fransisco: *Cyberpragmatics: internet-mediated communication in context*. Philadelphia: John Benjamins Publishing Company . (2011).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

