PREVENTATIVE MEASURES AGAINST ONLINE HATE SPEECH: A CASE STUDY OF POLITICAL CONFLICT

POL.MAJ. WANPADEJ HONGTHONG

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
(CRIMINOLOGY, JUSTICE ADMINISTRATION AND SOCIETY)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
2016

COPYRIGHT OF MAHIDOL UNIVERSITY

Thesis
entitled

PREVENTATIVE MEASURES AGAINST ONLINE HATE SPEECH: A CASE STUDY OF POLITICAL CONFLICT

Wanpadej Hongthong
.....
Pol.Maj. Wanpadej Hongthong
Candidate

Punchada Sirivunnabood
.....
Asst. Prof. Punchada Sirivunnabood,
Ph.D.(Political Science)
Major advisor

.....
Pol.Col. Sanya Niampradit,
Ph.D.(Public Policy Analysis-Urban Planning and Policy)
Co-advisor

Veenunkarn Rujiprak
.....
Asst. Prof. Veenunkarn Rujiprak,
Ph.D.(Social Psychology)
Co-advisor

.....
Prof. Patcharee Lertrit,
M.D., Ph.D.(Biochemistry)
Dean
Faculty of Graduate Studies
Mahidol University

Sunee
.....
Assoc.Prof.Sunee Kanyajit,
Ph.D. (Criminology, Justice Administration and Society)
Program Director
Doctor of Philosophy Program in Criminology, Justice Administration and Society
Faculty of Social Sciences
Mahidol University

Thesis
entitled

PREVENTATIVE MEASURES AGAINST ONLINE HATE SPEECH: A CASE STUDY OF POLITICAL CONFLICT

was submitted to the Faculty of Graduate Studies, Mahidol University
for the degree of Doctor of Philosophy
(Criminology, Justice Administration and Society)
on
March 4, 2016

Wanpadej Hongthong
.....
Pol.Maj. Wanpadej Hongthong
Candidate

.....
Pol.Col. Sanya Niampradit,
Ph.D.(Public Policy Analysis-Urban Planning and Policy)
Member

.....
Lect. Anusorn Payakkakom,
Ph.D.(Counseling Psychology)
Chair

.....
Pol.Maj.Chavanut Janekarn,
Ph.D.(Criminology)
Member

Punchada Sirivunnabood
.....
Asst. Prof. Punchada Sirivunnabood,
Ph.D.(Political Science)
Member

K. Phollawan
.....
Prof. Emeritus Kullaphol Phollawan,
Ph.D.
Member

Veenunkarn Rujiprak
.....
Asst. Prof. Veenunkarn Rujiprak,
Ph.D.(Social Psychology)
Member

.....
Prof. Patcharee Lertrit,
M.D., Ph.D.(Biochemistry)
Dean
Faculty of Graduate Studies
Mahidol University

.....
Assco.Prof. Wariya Chinwanno,
Ph.D. (American Studies)
Dean
Faculty of Social Sciences and Humanities
Mahidol University

ACKNOWLEDGEMENTS

This research was well accomplished with the contributions of Asst. Prof. Dr. Punchada Sirivunnabood, Ph.D., that the researcher got the title and accepted to be the advisor, which was the highest benefit to the researcher, even the dissertation structure and preparation of the content and analysis as well as scoped the time of the research. Asst. Prof. Dr. Punchada Sirivunnabood, Ph.D. has sacrificed her precious time to check the validity of the work without fail and her sacrifice would never be forgotten.

Gratitude was extended to Anusorn Payakkakom, Ph.D., Chairman of Examiner Committee, Asst. Prof. Dr. Veenunkarn Rujiprak, Ph.D, Prof. Emeritus Kullaphol Phollawan, Ph.D., Pol. Col. Dr. Sanya Niampradit, Ph.D., and Pol. Maj. Dr. Chavanut Janekarn, Ph.D., the dissertation examiners who have guided, recommended and observation, which allowed the researcher to develop ideas and the new conceptual framework until this dissertation has been accomplished.

Thanks were extended to all informants from TCSD, MICT and NBTC.

Gratitude was extended to all lecturers who have taught and transferred knowledge to the researcher. Thanks to all the personnel of Faculty of Social Sciences and Humanities, Mahidol University who never failed in their helps.

Finally, deepest gratitude is extended to my parent (Nuanjan and Thatchai Hongthong) who have educated the researcher since early age with loving care and spiritual supports and drove the accomplishment of this dissertation.

Pol. Maj. Wanpadej Hongthong

PREVENTATIVE MEASURES AGAINST ONLINE HATE SPEECH: A CASE STUDY OF POLITICAL CONFLICT

POL.MAJ.WANPADEJ HONGTHONG 5436997 SHCJ/D

Ph.D. (CRIMINOLOGY, JUSTICE ADMINISTRATION AND SOCIETY)

THESIS ADVISORY COMMITTEE: PUNCHADA SIRIVUNNABOOD, Ph.D., VEENUNKARN RUJIPRAK, Ph.D., POL.COL.SANYA NIAMPRADIT, Ph.D.

ABSTRACT

This research aimed to investigate the public sector agencies' measures against online hate speech. This was a case study of currently active political conflict. The objectives were 1) to investigate the public sector agencies' measures against online political conflict hate speech, and 2) to investigate remedial approaches and to develop preventative measures for public sector agencies against online political conflict hate speech. This research employed a qualitative approach through in-depth interviews conducted with 24 informants from three agencies, including 1) Technology Crime Suppression Division (TCSD), 2) Ministry of Information and Communication Technology and 3) the National Broadcasting and Telecommunications Commission (NBTC). The results showed that the existing law enforcement against online political conflict hate speech met problems and practical limitations, which make it impossible to prevent hate speech behaviors. These include (1) the problems of accumulating information, witnesses and evidence by the officers, (2) the problems of attribution, (3) the problems of retaliation, and (4) the absence of integration missions among various agencies. All these problems weaken the efficiency of prevention and hate-speech behavioral controls. It is recommended that there should be amendment approaches to control the dispersals of online hate speech in the case of political conflict for the agencies involved to take action. These are (1) set criteria to identify the social online users, (2) redirect political attitudes, (3) campaign for the legal use of online social media, (4) amend violence and penalty enforcement to make it appropriate, (5) develop personnel potentials and keep abreast with modern IT.

KEY WORDS: PREVENTATIVE MEASURES / ONLINE HATE SPEECH / POLITICAL CONFLICT

107 pages

มาตรการการป้องกันการใช้ถ้อยคำที่ก่อให้เกิดความเกลียดชังในสังคมออนไลน์: กรณีศึกษาความขัดแย้งทางการเมือง

PREVENTATIVE MEASURES AGAINST ONLINE HATE SPEECH: A CASE STUDY OF POLITICAL CONFLICT

พันตำรวจตรี วันเผด็จ หงษ์ทอง 5436997 SHCJ/D

ปร.ด. (อาชญาวิทยา, การบริหารงานยุติธรรมและสังคม)

คณะกรรมการที่ปรึกษาวิทยานิพนธ์: พรรณชฎา ศิริวรรณบุศย์, Ph.D, วีนันท์กานต์ รุจิภักดิ์, Ph.D., พ.ต.อ.สัญญา เนียมประดิษฐ์, Ph.D.

บทคัดย่อ

งานวิจัยนี้มุ่งศึกษามาตรการของหน่วยงานภาครัฐต่อการป้องกันและปราบปรามพฤติกรรมการใช้ข้อความที่ก่อให้เกิดความเกลียดชังในสังคมออนไลน์ ในประเด็นความขัดแย้งทางการเมือง ที่ดำเนินการอยู่ในปัจจุบัน ซึ่งมีวัตถุประสงค์ 1) เพื่อศึกษาถึงมาตรการที่มีในปัจจุบันของหน่วยงานภาครัฐในการป้องกันและปราบปรามพฤติกรรมการใช้ข้อความที่ก่อให้เกิดความเกลียดชังในสังคมออนไลน์ เกี่ยวกับประเด็นความขัดแย้งทางการเมือง และ 2) เพื่อศึกษาหาแนวทางแก้ไขและพัฒนามาตรการในการป้องกันและปราบปรามของหน่วยงานภาครัฐต่อการใช้ข้อความที่ก่อให้เกิดความเกลียดชังในสังคมออนไลน์ เกี่ยวกับประเด็นความขัดแย้งทางการเมือง การวิจัยฉบับนี้จะใช้รูปแบบของการวิจัยเชิงคุณภาพ โดยใช้วิธีสัมภาษณ์เชิงลึก จากกลุ่มตัวอย่าง จำนวน 24 คน ที่มาจาก 3 หน่วยงาน ประกอบไปด้วย 1) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี 2) กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และ 3) คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ ผลการวิจัยแสดงให้เห็นว่ามาตรการที่ดำเนินการอยู่ในปัจจุบันสำหรับการป้องกันปราบปรามพฤติกรรมการใช้ถ้อยคำที่ก่อให้เกิดความเกลียดชังในสังคมออนไลน์ ในประเด็นความขัดแย้งทางการเมือง ยังมีปัญหา ข้อขัดข้องในการปฏิบัติทำให้ไม่สามารถป้องกันพฤติกรรมลักษณะดังกล่าวได้ตามที่ควรจะเป็น ได้แก่ 1)ปัญหาในการรวบรวมข้อมูลพยานหลักฐานของเจ้าหน้าที่ 2) ปัญหาในการระบุตัวตนผู้กระทำความผิด 3) ปัญหาด้านของบทลงโทษ และ 4) การขาดการบูรณาการในการทำงานของหน่วยงานต่างๆ ปัญหาทั้งหมดนี้ ส่งผลโดยตรงต่อประสิทธิภาพในการป้องกันและควบคุมพฤติกรรมดังกล่าว ดังนั้น จึงควรต้องมีการนำเสนอแนวทางปรับปรุงแก้ไข เพื่อเป็นการควบคุมการแพร่จายของพฤติกรรมดังกล่าว ซึ่งผลการวิจัยได้เสนอแนะแนวทางในประเด็นต่างๆ เพื่อเป็นให้หน่วยงานที่เกี่ยวข้องนำไปใช้เพื่อการป้องกันและควบคุมพฤติกรรมการใช้ข้อความที่ก่อให้เกิดความเกลียดชังในสังคมออนไลน์ ในประเด็นความขัดแย้งทางการเมือง ได้แก่ 1) การกำหนดหลักเกณฑ์ในการระบุตัวตนของผู้ใช้บริการสังคมออนไลน์ 2) การปรับทัศนคติทางการเมือง 3) การรณรงค์ในการใช้สื่อสังคมออนไลน์ให้ถูกต้องให้กับคนในสังคม 4) การแก้ไขความรุนแรงหรือแนวทางการลงโทษให้มีความเหมาะสมมากขึ้น และ 5) การพัฒนาศักยภาพของบุคลากรและวัสดุอุปกรณ์ให้ทันสมัยตามเทคโนยีการสื่อสาร

107 หน้า

CONTENTS

CONTENTS (cont.)

CONTENTS (cont.)

LIST OF FIGURES

LIST OF ABBREVIATIONS

TCSD	Technology Crime Suppression Division
MICT	Ministry of Information and Communication Technology
NBTC	The National Broadcasting and Telecommunications Commission
ISP	Internet Service Provider

CHAPTER I
INTRODUCTION

1.1. Background and Significance

"Scission, if only shootout the Red but protecting the Yellow...
…If not kill now, killing will come …Just die then now…"

Political actions in any regimes must unavoidably meet the agreed and disagreed parties on the practices and administration. Such conflicts are relied on many factors such as economy, social and even personal attitudes. These lead to an association of the same ideal and this grouping could even be political parties to object the normal regime or grouping of the media to express opinion in various forms. However, whatever actions any groups perform, they perform by using media as the driving tool. And the contents in actions involve the politics, public affairs administration, and agencies' missions; these can be formal such as the government manifesto or communiqué, the interview of different political parties. Moreover, these can be informal such as specialists' opinions, information collections and published in media or other people through various channels. The objectives of political dissemination are to launch public relation of the group's performance, supporting one's group, persuasive others to join group and discredit the oppositions (Kanjana Kaewthep, 1977). With the contradiction of political view, it creates schism in Thai society. Often, political rifts are heated into unrest within the country such as rally, protest and closing down the government workplaces and so forth.

However, even with any groups; all their actions since 2005 until 2014 the peace and order of Thailand met critical crises because of chained political conflicts. Be it the coup in 2006, the emergency announcement in 2010 and the latest one was the coup in May 2014. These hindered the national development regardless economy or social but the critical one was the national security. These political conflicts split

the Thais because of just different political opinions. However, the rift from different political viewpoints is not ended at the opinion expression or legal expression, but growing wild with violence and assaults the oppositions, even death or taking violating action such as intrusion of the government offices or destroying public properties and so on. Such deeds so much damage the country.

The phenomena under the domestic unrest caused by social schism are just the incompliance of political opinion. Questions are then raised: On what point, why people strongly and violently feel about politics? Why people politically behaved with various violent deeds and violating law in their political expressions? It is unavoidable to express their opinion in order to discredit the oppositions (Thairath Online, 2014). On account of humans own rights to express opinion enacted in the Constitution, but such opinions must be subject to law without the characteristics of incitement or instigation to use violence or taking any law violation acts. However, in the past, either there were incitements or instigation by rebukes, accusation, rude and such behaviour incited hatred against the opposite individuals or groups with contradictory opinions or it may be called “hate speech”.

The provocation or incitement for political participation with rudeness or hate speech is common in political expression in any era (Thairath Online, 2014). Nevertheless, the consequences arouse common political moods and diffuse into violence and violating the law. The mediums to express hate speech are many by IT development, beginning from radio, TV and social media to be the medium of opinion expressions.

The relationship between media and politics

In democracy, media has an influence in politics since the past until today because media is the governments’ channel of public relation for people to realize the political activities and the government’s action, which may lead to the involvement of people either the conventional or unconventional political participation, temporally or permanently. The objectives are to have influence on public policy decision making and to check the governments’ using power and any affairs. Political participation is the key to develop democracy, which leading to the national development in other areas (Inglehart and Catterberg, 2002; Office of the Parliament Secretary, 2011).

There are two characteristics of the relationship between media and politics. First, one-way communication – the government or the political powerhouses convey messages through media to mass only. Second, two-way communication – or being both being senders and receivers at the same time: besides the political messages are disseminated from the political powerhouses but the people can express their opinions or claims through various channels back to the political powerhouses (McNair, 2003).

The model of political communication in the past was characterized as disseminating messages and opinion in one-way communication. Meaning, the government convey messages to people through communication devices to convince them to accept and trust its administration, but the people cannot provide feedbacks because the communication channels were owned by the government and people unlikely know much about politics (Brian, 2003; Nattakan Kulnarong, 2007). However, communication allows people to perceive and learn about various political experiences, which demand political participation. In associated with the communication development, it allows political communication changes into two-way communication (Kanjana Kaewthep, 1998; Nattakan Kulnarong, 2007). At present, when the internet turns the communication between politics and media could be done all the time through social media because the attributes of the social media are popular to be the medium. Alternatively, it could be said that communication through social media today has become the tool for political parties. For example, Barak Obama, US President, has used Twitter in his election campaign or David Cameron, the UK Prime Minster, has used facebook for his campaign.

The influence of social media

At present, the internet is the most influential device and used in human communication. This makes the world becomes borderless because the internet can help humans to communicate all the time, to present information, pictures, sounds and motion pictures. In addition, the internet users can interact with other or websites and with this interaction, it becomes the strength, which leads to social media.

Social media is similar to virtual community. It allows the internet users with unlimited races, ages, genders and religions to express contents, experiences,

articles, pictures or any communications of various forms for others within one's network that there will be feedback opinion (Wiyada Thitimatchima, 2010). Undeniably, the large numbers of internet users have turned to websites serving on the social media site. With the dispersal and popularity of social media at present, it impact on the internet users' thinking and understanding and people around them (Eid and Ward, 2009).

The prominent point of the modern technology and the popularity of social media allow us too speedily and limitless realize information regardless of distance or time, real time. The information presenters are not restricted only being the news reporters but common people can work as citizen journalism. Had the person known the news by himself/ herself or from others, he/she can broadcast them on social media (Newman, 2009; Newman, Dutton and Blank, 2012). Moreover, social media is also the advertisement tool or election campaign because of its characteristics of two-way communication. It diffuses like word-of-mouth or viral marketing in the real world or in the cyber world (Miller and Lammas, 2010). With this distinctive point, the users who want to disseminate information use social media as a device to achieve their objectives (Wowpailin Chorwichian, 20110. The influence of social media so much affects human's way of life in the society either in education or in economy or in mass communication.

The internet users around the world since June 2012 were more than 2.4 billion. If watching its growth rate since 2000-2012, it was found that it hiked to 566.4% as shown in figure 1.1 (Internet World Stats, 2014). The figure shows the growing popularity of humans on using internet in particular social media, since 1997 when it has been launched for services (Sixsdegrees.com). Today, there are many social-media providers but the popular providers are Facebook, Google +, Twitter, WhatsApp, Line or LinkedIn and so on (see Figure 1.2). The statistic of the social-media users shows that most internet users will sue social media too (Office for National Statics, 2013; Statistic Brain, 2014).

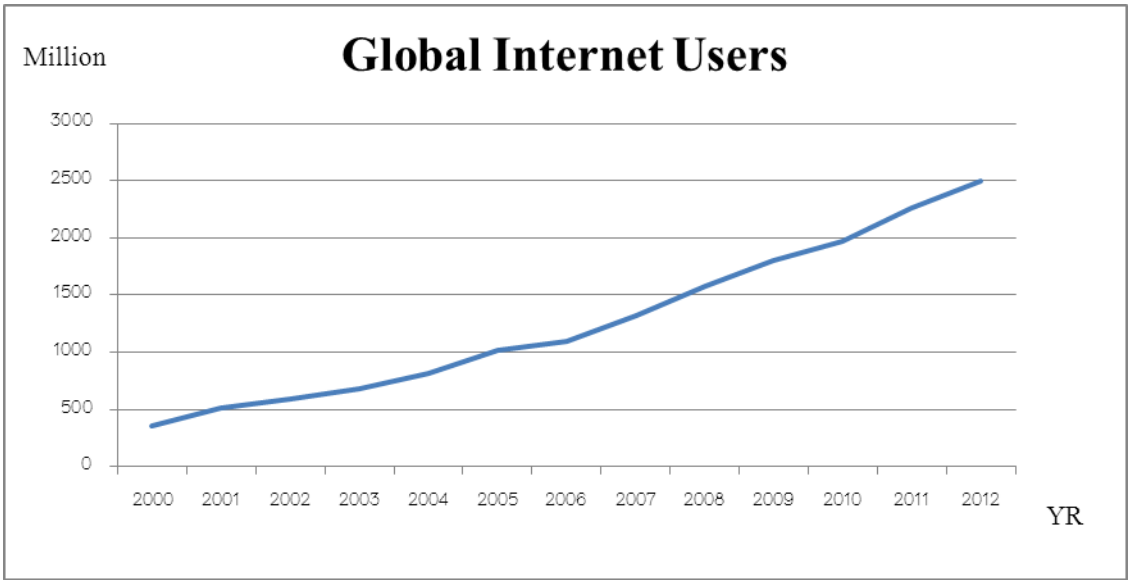

Figure 1.1. Growth rate of internet users worldwide 2000-2012

For Thailand, the growth rate of internet users during 2000-2012 hiked more than 100%. The internet users in Thailand during 2012 were 20 million (Internet World Stats, 2014). Popularity and growth of the social media are similar with other countries. Most internet users have ever used social media before such as Facebook users in Thailand until 2012 were 17 million. Most activities in social media are pursued information, chatted with friends or shared pictures and so on (Electronic Transactions Development Agency (Public Organization, 2013; Internet World Stats, 2014)

Figure 1.2. Social Network Service Providers since the past

Source: Headlund, 2011

Besides using for daily life in society; the results of technological development of communication devices and the distinction of social media are misused which harms other sin society either seeking gains or harming other. Examples happened from misusing social media affecting the existence of people in society such asforeseeing the others' information and disseminating them without permit, disturbing others' privacy or cyber stalking. For example, the case of Joseph Ostrowski aged 29 years was sentenced by the Pennsylvania Court for 30 years term on charges of accessing the network of student social media in Michigan University and use private information of a student posted (FBI, 2013) while hectoring through cyber stalking. A case of a 12-year old girl in Florida committed suicide caused by pressures from social media satirized by her 14-year old friend (CNN, 2013) and so on (Khanaathip Thongraweewong, 2013). The evident problems and diffusing in society at present are the cyber violence especially cyber bullying through social media attributed in condemnation, threats, accusation, and sexual harassment. Such problems hurt those who are involved and relations within society at large (Shariff, 2008; Samoh, Boonmongkon, Samakkeekarom, Ojanen and Guadamuz, 2014). However, cyber violence in social media is not only used with intention for personal gains as mentioned but also for seeking political gains particularly the countries facing political conflicts such as Syria, Iran, Egypt, Libya and Thailand.

Political conflict in Thailand and online hate speech in social media

Communication technology using internet overturns the present world borderless. People can freely communicate with unlimited distance or places. In addition, communication devices are developed to meet the internet system and enabling to occupy with various activities like photographing, sound recording and storing data. As such, the communication devices respond to the needs of humans and by the distinction of interaction with other people, progressively social media, which is similar to virtual community (Wiyada Thitimatchima, 2010). The social media users will use cyber space as public sphere to share opinions and other activities. Any activities in the public sphere will be speedily disseminated and, with the distinction of social media, it allows the action taken by the groups, organizations or workplaces to

use this medium to access targets like economy, social and even politics (Dahlberg, 1998).

In Thailand, social media is so popular and so undeniably useful to politics because of speed in public relation allowing all political group, politician, parties and movements groups along with people to receive political news into social media. In reality with the past politics, the political conflict in Thailand still exists among the government supporters and the opposition supporters, both groups would use media for political activities. At present, social media is the major channel with any groups (Thaweesak Kertphokha and Ratiya Khathanya, 2012; Arthit Suriyawongkul, 2012). However, the impacts of virtual community in the cyber space; any expressions are not necessarily real. Without control from social laws or rules, freedom of speech and violent political conflict, the expressions in social media are always violent, aggressive, threatening, and hectoring others by hate speech and violating other private rights (Charnchai Chaisukkosol, 2011).

Expression by online hate speech is part of cyber violence, and present, it is the problem happening Thailand, particularly on politics, which social media is the major channel for communication and the Thai society has no norms of “social measures” to be clearly defined (Sissanee Archawananantakul, 2011). It includes the legal provisions related to the offense of hate speech with unspecific stipulation. Moreover, the agencies’ measures in social media cannot efficiently control, especially from the public sector agencies. In addition, it is unclear on the course of practices, which allow rudeness, aggression and words arousing violence. They can be found in every political page in the social media (Foundation of Media Studies, 2002) (Figure 1.3). Furthermore, the presentation of political information creates disinformation or misinformation. Since the political opinion is characterized to present information to support one’s own party and attacking the opposite party, it is arousing the sentiment and the receivers to have more common mood until expressing violence. Damages of hate speech unavoidably affect the speakers, the accused, people around and society on defamation, and self-images on being directly spoken of. The impacts on society lead to schism of people in society, violence uses, assaults against body and property and further diffused to be social problems (Charnchai Chaisukkosol, 2011).

Figure 1.3. Examples of online hate speech

The sentiment survey with people about politics; it was found that 57.5% felt it was normal to express hate speech and online social media was used as a channel to express such violent behaviour (Thairath Online., 2014). It is not surprised what incident leads to online hate speech which is the current problem. Such problem is diffusing to human behaviour in society expressing reality and leading to assaults just because of hate crime. Schism among people or the improper behaviour with

intention to assault for life and property illustrate the Thai social problem. These result from political conflict with hate speech arousing or encouraging such social phenomena.

Impacts of political conflicts on Thailand

The influences of social media lead the growth of using hate speech in political conflict to the level of inciting hatred on the group of political contradictory opinion. It culminates to eradicate the targeted groups or using violence and assaults (Study Center of Media Policy: School of Communication Arts, Chulalongkorn University, 2013). In the past, damages from political conflicts of the different groups led to violence until death. For example, the clash between the military with the National United Front of Democracy Against Dictatorship (UDD) during May 14-16, 2010 took 35 lives. The other examples were the clash between the people of different political opinion between the People's Alliance for Democracy (PAD) and the National United Front of Democracy Against Dictatorship (UDD) during September 2008 (Thairath Online, 2014) and the riot around Ramkhamhaeng University between the UDD and the students of Ramkhamhaeng University during November 2013 (Krungthepthurakit, 2014). Each incident brought death from the clashes. The consequences of political rally so much affect the image of Thailand.

Nowadays, Thailand enacts laws and regulations to impose wrongdoers of using online hate speech, i.e. the Criminal Code and the Computer Crimes Act B.E. 2550 (2007) including monitoring and supervising any content in social media by the public sector agencies; Ministry of Information and Communication Technology, the National Broadcasting and Telecomunications Commission (NBTC) and the Technology Crime Suppression Division (TCSD). However, the real phenomena in online political conflict hate speech are growing problematic to Thai society. It demonstrates the inefficiency of the preventative measures against online hate speech in Thailand. Hate speech reduces the level of social bond and diffused to behavioural expression in society and creating social problems, which hardly control and correct in associated with this issue is rarely studied recently.

In order to find approaches to prevent and solve such problems, there should be an investigation on the current preventative measures employed the public

sector agencies against online hate speech, particularly in the case of political conflict among Thais. What are the problems and limitations in practices of preventative measures against online hate speech? And what are the approaches to amendment and improvement of those preventative measures for the public sector agencies against online hate speech, particularly in the case of political conflict? The results would be as guide to further plan and to stipulate the preventative measures against online hate speech with better efficiency.

1.2. Research Questions

1.2.1. What are the current preventative measures employed the public sector agencies against online hate speech, particularly in the case of political conflict?

1.2.2. What are the approaches to amendment and improvement of preventative measures for public sector agencies against online hate speech, particularly in the case of political conflict?

1.3. Research Objectives

1.3.1. To investigate the preventative measures of the public sector agencies against online hate speech, particularly in the case of political conflict; and

1.3.2. To investigate the approaches to amendment and improvement of preventative measures of the public sector agencies against online hate speech, particularly in the case of political conflict.

1.4. Scope of the Study

1.4.1. Content: it is to explore the current public sector agencies' preventative measures against online hate speech in the case of political conflict.

1.4.2. Population: it is concentrate to the public sector agencies that hold duties of policymaking and applications. The population is then 24 informants from

the public sector agencies related to suppression and prevention online hate speech, i.e.

1) Eight (8) informants from the Ministry of Information and Communication Technology

2) Eight (8) informants from National Broadcasting and Telecommunications Commission (NBTC)

3) Eight (8) informants from Technology Crime Suppression Division (TCSD)

1.5. Expected Benefits

1.5.1. To know the limitations of the preventative measures of public sector agencies against online political conflict hate speech and to be the guide for improving the efficient measures.

1.5.2. People would be aware of impact from using online hate speech and attend the activities in preventing such behaviours.

1.5.3. Reducing the violence or crimes caused by political conflict in Thailand.

CHAPTER II
LITERATURE REVIEWS

This study was to investigate the current preventative measures and the approaches to amendment and improvement on preventative measures of the public sector agencies against online hate speech, particularly in the case of political conflict. Another objective was to adopt the findings to be as guides to amend and to develop the preventative measures and constructive enforced them. The researcher reviewed related literatures on theories and concepts to be as guide in formulating the conceptual framework as below.

2.1. Definition and Meaning of Hate Speech

Since the hate speech is similar to propaganda and provokes schism among people in society, which endangers their life and property and endangers internal and international security. These lead to suspicion and distrust among people on effectiveness of the government agencies' security operations, including problem on online hate speech spread (Gattuso et al., 1993). To define "hate speech" is inevitable to be the conceptual framework on preventative measure against such behavior of people in society. However, it is not defined at international level, which allows law in each country or international laws differently define it (Mendel, 2010; ECHR, 2013).

Example of the hate speech in the convention

International Covenant on Civil and Political Rights – ICCPR 1966 does not define its specific meaning but prohibits in the article. 20(2) that "Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law"

The Council of Europe defines Hate Speech in 1997 as covering all forms expressions which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance."

The American Convention on Human Rights prohibits the hate speech in the article 13(5) that "Any propaganda for war and any advocacy of national, racial, or religious hatred that constitute incitements to lawless violence or to any other similar action against any person or group of persons on any grounds including those of race, color, religion, language, or national origin shall be considered as offenses punishable by law."

International Convention on the Elimination of all forms of Racial Discrimination 1965 – CERD divides hate speech into four types, (Mendel, 2010), i.e.

1. Dissemination of ideas based on racial superiority
2. Dissemination of ideas based on racial hatred
3. Incitement to racial discrimination
4. Incitement to acts of racially motivated violence

National Telecommunications & Information Administration (NTIA), United states Department of Commerce defines hate speech that (Gattuso et al., 1993):

1. Speech that advocates or encourages violent acts or crimes of hate.

2. Speech that creates a climate of hate or prejudice, which may inturn foster the commission of hate crimes.

With the meaning of "Hate Speech" from the international convention and international laws, it could be concluded that speech creating hatred are the expressions by either wording or any other acts characterizing contempt, insult or devaluing humanness or discrimination by using the causes of race, religion, skin, language, social status, gender or by other reasons. Such expressions might lead to violence or endanger any targeted individuals or any targeted groups.

All expressions exploited by differences regardless being race, religion, ethnic or skin are unfound in the Thai society. However, recently causes made Thailand segregated or parity is significantly political thoughts or political ideology. Consequently, the meaning of “Hate Speech” in the Thai context should be focused on the differences of political thought or political ideology which leads to hatred or segregation in Thai society.

This research aimed to investigate hate speech in the case of political conflict only. Therefore, “hate speech” here is referred to expressions by any methods regardless being speaking, announcement, advertisement or spread by any other methods characterized in contempt, insult, sarcasm, discrimination or devaluing humanness caused by political opinion, political ideology and the consequences of these expression may lead to violence or endanger any targeted individuals or any targeted groups.

Finding that the impacts of hate speech are not only leading to violence , which may endanger to people in society but also impact the domestic and intentional security because the root of political conflict is sensitive and affects the feelings of those individuals and groups or the country with similar nature. Also, IT development makes any information could be speedily spread, and results to the difficult of monitoring. Consequently, to prevent violence or endangering acts against people in society and to ruin the unity of people in the country just by online hate speech demands to adopt theoretical principle of anti-crime for analysis in order to find solution in stipulating practical measures of the responsible personnel.

2.2. Concept of Social Control Theory

2.2.1. The history of anti-crime theory

During early 20th century, most criminologists turned to Ecological approach (Mazerolle, Wickes and McBroom, 2010; Wortley and Mazerolle, 2011; Tibbetts and Hemmens, 2014) to find the causes of crime. The Social Disorganization theory is one that uses the ecological approach. Its principle is crime and social deviation come from the change of societal conditions of a community for

urbanization happens all the time. It lowers social control mechanism and rises social disorganization, which l further leads to crime or deviation (Bursik, 1988). Disorganization comes from migration and differences of community population either by status or by culture (Kornhauser, 1978). Nevertheless, in 1960, this theory because less popular because of its content error (Lewis and Lewis, 2011).

Modern criminologists gave importance to social structure in studying the causes of crime such as social interaction, or abiding by laws in community (Bursik, 1988). It led to the study of victimization and criminals in a community. Crime prevention was directed to victims' behaviors and impulses of the criminals and environment arousing wrongdoing. This was call victimology because this theory has a principle of crime prevention through the victims' behavior (Lewis and Salem, 1981).

During 1980, as the consequences of social class differences and natures of the US hetero-ethnic population, the popular studies again turned to the relationship of crime with place, community, economic status and quality of life (Sampson, 2002). This study has just prioritized collective capacity because social disorganization comes from the community structure, which is not conscious about common values of people. In order to retain social orderliness, it associates through formal and informal collectiveness. The formal collectiveness may clarify there is coordination, cooperation and organizational and institutional involvement such as churches, schools and workplaces. The informal collectiveness may clarify the ties with others such as family members, friends and the known persons through exchanges of opinions and information within a society. These display the collective efficacy (Morenoff, Sampson and Raudenbush, 2001). If a society were strong, problems within it would be alleviated either people with better health or caretaking of siblings by parents or less family violence (Lewis and Lewis, 2011).

It is found that cause of crime and deviance applying human relation approach rather than investigating macro social structure as in other theories; new criminological theory like Social control theory has been applied. It is another criminological dimension focusing on interpersonal within society rather than focusing on the influence of the public sector mechanism to counter crimes. In later dates, crime

prevention has welcomed social participation as in the principle of social control theory more rather than the public sector personnel as in the past.

2.2.2. Social Control theory

It investigates the criminal causes through the interpersonal in society (Lewis and Salem, 1981). It differently explains deviation and criminal behavior from other criminological theories and sees that deviation and criminal behavior require arousal. For example, the Strain theory sees that deviation comes from social pressures because one cannot reach targets set by society (Merton. 1938). The Differential Association theory sees that humans can learn values and techniques of crime if interacting with criminals (Sutherland, 1939), for example. The Social control theory believes that since birth human own drives or impulses to express selfishness and these drives leads to criminal behavior. As such, it leads to set research questions of why people follow rules and laws or why do people not do wrong things rather than asking the cause of wrongdoing (Hirschi, 1969).

The social control –based research welcome many theories from criminologists which presented different perspective and approaches to explain the causes of offensive behavior. For example, the Stake-in-Conformity theory contending that human would not do wrong if the act had high risk or great loss to oneself (Toby, 1957; Briar and Piliavia, 1965). The Containment Theory advocated that if a wrongdoer had stronger social attraction to do wrong than resistance not to do wrong (Reckless, 1961; Kelly, 1996). The theory of Family Relationships and Delinquent Behavior claimed that criminal behavior and deviant behavior come from inefficient social control (Nye, 1958). The Social Bond theory believed that humans behave under laws if abide with social bond: attachment, commitment, involvement and belief (Hirschi, 1969).

It could be concluded that the Social Control theory aimed to investigate the influence of interpersonal within society and significantly enabling to interfere or resist criminal behavior or deviation rather than investigating the mechanism of public sector influence to interfere individuals to do wrong. The Social Control theory in the past did not explain the dimension of law enforcement in countering crimes but viewed interpersonal dimension that it was the key to control human behavior through

informal social norms (Hirschi, 1969). Mechanisms controlling human behaviors in society were various institutions such as family, school, religion and neighbor, for example. In a society or institution with strong interaction; there would be less found with deviation or crime, if parents fostered instruction and behavioral care for example, graffiti by youth. The outcomes of the Social Control theory have been developed into the indicator of the collective efficacy and the approach of counter crimes and deviation (Sampson, et.al., 1997).

However, this research aimed to investigate the preventative measures against online hate speech, which is a part of cybercrimes. It impacts domestic and international security. To control the behavior and to prevent such crime through various institutions in the past failed in their efficacy (Jaishankar, 2008; Ngo and Paternoster, 2011). Accordingly, countering such behaviors through the mechanism of the public sector or formal control plays the key role and worth to suppress online hate speech rather than employing social control or informal control. The criminological theory explaining counter crimes and deviation through the mechanism of the public sector is the Deterrence Theory.

2.3. Concept of Deterrence Theory

It is focused to explain the legal influence in governing people in society rather than explaining the causes of crime or deviation. Its foundation is any wrongdoings in society if done cannot retrieve time. Consequently, if such wrongdoing happens, it needs to find preventative measures not to allow it happen again. Retaliation is an approach to prevent it happens again. The foundation of the decision making process to commit crime is to consider the extent of retaliation or costs and benefits if being caught. If misery or pain is more than benefits of wrongdoing, individual will decline to do wrong. On the contrary, if the benefits are more worth with the risk of retaliation; an individual will decide to do (Kennedy, 1983).

Cesare Beccaria (1968) the father of the “Deterrence Theory” postulates that retaliation must contain three things, i.e. 1) swiftness of punishment, 2) certainty of punishment, and 3) severity of punishment. Details are as below.

1) Swiftness of Punishment – when there is a wrongdoing, the wrongdoer must be speedily sued for punishment that others will witness the example that upon wrongdoing what consequences are. On the contrary, if the wrongdoer has been late punished, all people will forget the incident, which leads to those who think to commit offense to offend. Deterrence fails here.

2) Certainty of Punishment - when there is a wrongdoing, the wrongdoer must be sued for punishment. It is the threat to the wrongdoer and others fear to offend.

3) Severity of Punishment – punishment must be appropriate and proportionate to the offense committed either too severe or too light. Crimes or wrongdoings will not be committed if laws are efficient and appropriate. Meaning, the punishment is enacted with severity while the judgment process must be swift and wrongdoer meets high opportunity to be caught. The punishment of the Deterrence theory is divided into two models, i.e. (Stafford and Warr, 1993).

1) General Deterrence – it is a punishment to exemplify others to witness that how wrongdoing deserve punishment. The aim is to allow other to see mishaps of wrongdoing and fear not to offend.

2) Specific Deterrence – it is a punishment aimed to prevent recidivism and after punishment, the wrongdoer fears to be punished again.

Examining the Deterrence theory, its estimated efficiency against crimes or wrongdoing contains five (5) approaches, i.e. 1) punishment-hike policy, 2) the relationship between severity punishment and crime rate, 3) social understanding on the deterrence principles, 4) efficiency of applying rehabilitation as punishment, and 5) the influence of imprisonment punishment (Nagin, 2011). Many studies have been conducted on the efficiency of each approach.

The research on the punishment-hike policy include the policy of intensifying anti-deviation. The data collection was conducted before the policy was enforces until the end of the policy period and compared the pre- and post outcomes. Most studies claimed that the punishment-rise policy reduced crimes (Nagin, 1998;

Apel and Nagin, 2011). On the other hand, there were some research claim that the punish-hike policy had no impacts on crime in long-term. Nagin, Cullen and Jonson (2009) commented on the influence of the punishment-hike policy that 1) the policy was only short-term. 2) the influence of the policy on wrongdoing would gradually be lessened. 3) the policy did not affect deterrence against crime, and 4) some policies contributed contradictory outcomes on what have been predicted.

The research on influences of imprisonment punishment to prevent crimes mostly found that imprisonment could not reduce crime. Conversely, imprisonment led to more recidivism while probation led to less recidivism (Nagin, 2011).

Research on relationship between violent punishment and crime rate at macro level, Pratt and Cullen (2005) studied 31 variables and 6 variables among them were used to measure deterrence: 1) imprisonment, 2) arrest rate, 3) police budget, 4) policy of rigid law enforcement, 5) ratio of police and population, and 5) number of policemen. Research results showed that among the six variables above, only imprisonment strongly affected crime deterrence while the rest five least affected crime-rate reduction.

At present, crimes arisen were not only the conventional crime such as street crime as in the past but also changed and developed by technology. Wrongdoings used communication technology as the tool or channel of cybercrime, for instance, cyber stalking and hacking. Such crimes are distinctive from the conventional crimes such as anonymity, or damages are not immediate. These affect to behavioral control and prevention of cybercrime through various institutions in societies of applying the social control theory and the deterrence theory. These theories are inadequate to prevent crimes above. In order to deter crimes efficiently and accepted in practices, it is necessary to consider the development of communication technology including the pattern of cybercrimes in order to be applied with the concept of deterrence theory, so called Cyber Deterrence Theory

2.4. Concept of Cyber Deterrence Theory

For the past 10 years, the communication theories have been continuously invented and developed. The internet system is one of the communication technology invented and widely used while strongly affecting daily life of people. In 2015, for example, 87% of the US people in total used internet (Miniwatts Marketing Group, 2015) and technology was not restricted only for the adults. It influenced children and youth life too. For example 93% of youth used internet in their daily lives while more than half US youth citizen owned hand phones (Lenhart, Purcell, Smith and Zickuhr, 2010). Further survey showed that social status did not affect any internet service uses. The US black and the US Hispanic with low social status had greater rate of using internet than the US white with higher income (Smith, 2010). Even parents influenced children and youth but youth life spending was too preoccupied with using internet and games online (Lenhart et al., 2010). Furthermore, communication technology eased communication even in distance; people could connect each other at any plane in any time. Such connectivity from distance, it reduced interaction with neighboring community and homes, too. It also reduced the influences of community norms and values (Putnam, 2000).

Surveying the US children and youth showed that 70% of online social media earned family incomes lower than 30,000 USD (Lenhart et al., 2010). It was further found that more than half chatted with strangers through online social network (Lenhart, Lewis and Rainie, 2001). It was seen that children and youth behavior dramatically changed and caused by the communication technology development. Online social media gradually played key roles to command the children and youth behavior more. Online social media consumption became the emerging behaviors among children and youth. By reason, their personal data found in the online social media which enabled their intimate persons or friend groups to access, comment and chat all the time (Boyd, 2007). These led to the studies on impacts of online social medias uses (Ellison, Steinfield and Lampe, 2007; Yardi, 2009) advocating the social learning theory of Bandura (1977) which explained the imitation behavior. For example, youth playing games online would behave the behaviors shown in the games. Similarly, behavioral imitation of online hate speech by inefficient suppression arouses other to imitate it and hikes problems as in today. Also, the communication

technology development demands suppressions to consider the influence of technology against people in society too (Lewis and Lewis, 2011). This leads to the application between the conventional deterrence theory and the communication technology, which brings the new model of criminological theory enabling to respond the problem of cybercrimes under the name of the Cyber Deterrence theory.

2.4.1. The Cyber Deterrence theory

Its objectives are to dissuade or suppress wrongdoing by making the loss becomes greater than the benefits in the wrongdoer. Theoretically, it is divided into two (2) parts. First, it is a strong defense for example, if any countries had strong prevention, any attacks were likely impossible. Intruders might select not to attack because it is risky to lose by the attack. Second, it is retaliation as such with the same case that if the intruder wants to encounter aggressive retaliation; result is none dare to intrude again because of loss happened from the counter attacks(Haley, 2013).

The flaw is found from the conventional deterrence theory is disabling to point out the source or the original of the wrongdoers. Such flaw makes it hard to retaliate the cybercrimes especially the unique of the cybercrime is anonymity. Accordingly, it is necessary to add “Attribution” to the third part in the cyber deterrence theory (Haley, 2013.

Hence, considering the elements of the deterrence theory with the cybercrime, there are three parts, 1) defense, 2) retaliation and 3) attribution as the following details (Haley, 2013).

2.4.1.1. Defense

Kramer (2009) views that cybercrime is like real wrongdoing at three (3) issue, i.e. 1) large amount of population, 2) few barriers to wrongdoing, and 3) opportunity eases hiding. Nevertheless, the different point is the distance between the wrongdoer and the victim. There is so long distance in the cyberspace, which is different from the wrongdoing in the real world where the wrongdoer is near his/her victim.

In reality, it is impossible to check and charge every wrongdoing (Morgan, 2010). Consequently, prevention is the key part according to the concept of deterrence theory. Such prevention has two objectives, i.e., to prevent

wrongdoer to enter the system and to deter others to enter the system because of less opportunity to access information.

Efficient prevention demands cooperation between the physical structure and the efficacy of the users (Haley, 2013). The physical structure either being the device or various information needs efficient prevention. The system complexity or the reserved data is the important method to prevent the possible wrongdoing. The other important part of prevention is the efficacy of the user because reserving data and attending the system require practical knowledge and skills and there is no perfect security system. It is necessary to have regular improvement and development (Morgan, 2010).

Similarly, Geers (2010) prioritizes prevention to deter cybercrime. He adds that to have efficient prevention requires three elements. First, capabilities are the skills or potentials of the preventative tools and devices. Second, communication is the internal and between collaboration to stipulate suppression against cybercrime. Finally, credibility is the display that preventers are able to suppress wrongdoing and strong determination to prevent cybercrime. In addition, Goodman (2010) further adds that the wrongdoer must be retaliated while the innocent will not be endangered (Kugler, 2009).

The responsibility to prevent cybercrimes should not be restricted within the public sector but in the private sectors too. Rationally, at present, the national administration is run through the private companies. Accordingly, to consider the internet system safety or the cyber world, it is necessary to invite private companies to cooperate. However, the government has no direct responsibility to supervise the safety of the private companies but just to regulate for practices only. Consequently, private companies should develop their potential and also participate in the cybercrime prevention, which is not different from the physical world safeguarding where private companies or various villages have to install their own safety system (Haley, 2013).

2.4.1.2. Retaliation

Defending wrongdoing demands retaliation; if not the wrongdoer will not fear but dare to offend (Morgan, 2010). In the case of the wrongdoers are non-state actors; their proper retaliation is difficult because there is no

international legal enforcement. Accordingly, the appropriate and rational retaliation through lawsuit and law enforcements become the sample case for the next wrongdoing. However, in the past, it is found that the wrongdoers do not fear punishment. As a result, for efficient prevention; the imprisonment and fine as punishment should be subject to observation and probation over the wrongdoers too (Haley, 2013). If the wrongdoers are the countries and large companies; retaliation or any actions created consequent impacts including the interrelation. To this case, it demands other way of deterrence, for example, legal strike back like economic sanction or diplomatic sanction (Jansen, 2012). In retaliation, it is not necessary to be proportionate with the damages from the wrongdoing but to retaliate in terms of politics or relation. Retaliation demands efficiency of deterrence for recidivism (Jansen, 2012; Morgan, 2010).

The objectives of the wrongdoing are not the punishment after wrongdoing only but it needs to witness the consequences of the act too. The proportion of retaliation must be more than the expected benefits gained from the wrongdoing and it will be the threat not allowing other individuals to offend (Cullifo et al., 2012). This retaliation becomes the norms of practices in future and it will be the avoidance of the state or the organization conflict (Kugler, 2009).

2.4.1.3. Attribution

The problem of cybercrime is attribution because the cyber world involves many users and cannot be attributed and thence attribution is so difficult (Goodman, 2010). However, it may not be impossible but it needs more budgets to invest in technology development and to develop potentials and skills of the personnel involved. To investigate cybercriminals will deter others who think to commit cybercrimes. As a result, attribution is very important in defense (Goodman, 2010; Geers, 2010; Guitton, 2012). Conversely, it does not mean that the efficiency development for attribution must help arrest every cybercriminal and increases higher potential in cybercrime defense which is the important part of the cyber deterrence theory (Haley, 2013).

In conclusion, the cybercrime defense based on the deterrence theory requires attribution because what makes the cybercriminals do not fear laws is inefficient to find them with poor skills of the personnel or obsolete technology.

Finally, the defense of cyber world and online hate speech need more efficiency, which requires developing measures of attribution in order to couple with defense and retaliation according to the conventional deterrence theory. Such missions must not be restricted within the public sector responsibility but also other sectors have to involve in this defense and seek further development. Moreover, the agencies involved have to improve and develop skills and technology restlessly to deter other not to commit crimes and deviation (Guitton, 2010).

2.5. Communication Evolution and the Thai Political Conflicts

Thailand has began its democracy sin 1932 until today but its political conflicts forever exists even so many amendments of its Constitution until today. The major cause of its political conflicts is unavoidably the cronyistic government administration (King Prajadhipok's Institute, 2012). The government administration policy would have some media agreed with and some disagreed. Each party has its own objectives to persuade media to involve or to agree with while discrediting the opposite party. The operation al tools cannot be otherwise variety of communication disciplines of either newspapers or radios or TV or online social network because these media are influential to the attitudes and thoughts of the receivers to be prone to the contents (Eid and Ward, 2009).

Though there were many restless amendments of the Constitution; the Thai political conflicts are tooled by various media and in the past they have been at violent level to use arms and weapons in both the government and the its opposition. Until today, there are four periods of political conflict. As mentioned above, media have been used by the apolitical groups to differently tool their missions.

Period I: The Political Unrest during 1973-1976

The contingency of October 14, 1973 became the critical change in the political history of Thailand. More than 500,000 university students, students and people claimed for their Constitution from the administration of Field Marshall Thanom Kitikajorn, Prime Minister. The government deployed military and police forces to control the mob with weapons. Death and injuries were prevailed but finally

Field Marshall Thanom Kitikajorn defected from the country (Kowit Wongsurawat, 12010). A similar contingency in October 6, 1976, the university students protested the return of Field Marshall Thanom Kitikajorn the ex-Prime Minister and there were clashes between police, military with the protestors and also death hiked (King Prajadhipok's Institute, 2012).

During 1973-1976, the communication technology development was still obsolete. Political activities of the government were through TV, radio and newspapers to launch public relation for its performances (Ungpakorn, 203). For example, in 1976 the press release of M.R. Seni Pramote Prime Minister on the contingency was by TV and radio broadcasting of the military to accuse the action of the university students (Seni Pramote, M.R. 2005). Also, the media disseminated what they have received such as the administration of Field Marshall Thanom Kitikajorn in 1973 through newspaper (Lerphop Sorat, Saman Ngarmsanit, Boonrieng Srihiran and Charnchai Jitlao-arporn, 2011). The university student groups, student groups and resisters, at the same time, used leaflets and newspapers to request for the mass cooperation to resist the government (Kullada Ketboonchoo Meid, 2009; Wiccharn Jampakhao, 2011).

Period II: Political Violence in 1992

It is call the Black May with id political rally in 1992. A contingency when the mass protested the government during the administration of Gen. Suchinda Kraprayoon Prime Minister. The cause was to object the Constitution with undemocratic contents and object the succession military junta named the “National Peace Keeping Council – NPKC”. It was led by Gen Soonthorn Kongsomphong the Supreme Commander and the NPKC Chief, Gen. Suchinda Kraprayoon the Army commander; Admiral Praphat Krissanajan the Navy Commander, Air Chief Marshal Kaset Rojjananil and Pol. Gen.Sawat Amornwiwat as the NPKC Deputy Chief having Gen. Issaraphong Noonphaksi as the NPKC Secretary (Chowwana Traimas, 2007). Violence diffused and needed State of Emergency Declaration in Bangkok. Clashes began between the military and police, which brought large amount of death and injuries (Phirongrorng Rammasutr, Phimolwan Chai-anant, Chanansara Orranop Na Ayudhya and Yubol Benjarongkij, 2010).

During the political rally, the communication technology intervened in the Thai daily life with hand phones and pagers, which were very popular. The protesters used these channels to communicate in order to avoid controls and block by the government. The protesters called themselves, “Hand-phone Mob”. On the other hand, the government used TV and radio for its public relation because it could control the presentation. Often time, the presentation unmatched with reality. After this rally, there was an establishment of free TV called “ITV” where the mass would have opportunities to receive real news and without the government control (Phirongrorng Rammasutr, 2010; Arthit Suriyawopngkul, 2012).

Period III: Political Violence in 2005-2010

The political rally began again in 2005 caused by conflicts between political groups from groups of people who viewed that the administration of Dr. Thaksin Shinnawatr created overlapped interest and corruption (McCargo, 2008) and staged rally in the name of “People's Alliance for Democracy- PAD” led by Mr. Sonthi Limthongkul, Mr. Somsak Kosaisuj, Mr. Somkiat Phongphaibul, Mr. Phipop Thongchai and Maj. Gen. Chamlong Srimuang as the mainstays. At the same time, the supporters of the government launched also their movements and created the violent segregation in the Thai societies (Pathan Suwan Mongkol, 2006). Finally, there was a military coup and the military played another time the political roles. Later in 2007, even though there was an election again, the Plalang Prachachon Party won the election. However, PAD still on the move again seeing that Dr. Thaksin Shinnawatrwas in the backdrop (Wassana Nanuam, 2008). Later in 2008, the court orders dissolve of the Plalang Prachachon Party the government at that time. It needed resolution to find new Prime Minister. The parliament resolution selected Mr. Abhisit Vejjajiva the leader of the Democrat Party as the Prime Minister. The result of the resolution turned the Pueithai Party with its majority members were from the dissolved Plalang Prachachon Party became the opposition party immediately. The resistant side staged movements called the “United Front of Democracy Against Dictatorship-UDD chaired by Mr. Weera Musikkaphong, with Mr. Jatuporn Promphan, Mr. Weng Tojirakarn, MD, Mr. Chinnawat Haboonpard, Mr. Arissaman Phongruengrong, Mr. Nattawut Saikuia, and Maj. Gen. Kattiya Sawaddiphol as the committee members. The

UDD movements was prolonged until 2010 and clashes began with the protesters and the military with death an injuries, Finally, Mr. Abhisit Vejjajiva declared the parliament dissolved and organized new election in 2011 (King Prajadhipok's Institute, 2012).

During the rally, it was observed that the large number of mass joined the movement either supporting or resisting because of the uses of satellite TV stations and community radio (local business radio) as the channel for communication and played the critical roles in politics. These channels presents of clear schism (Nanthawitch Laowictchaya and Sasiroj Taenrattanakul, 2012). The benefits of using these channels for dissemination to public are with limitless access and without public sector control. It allowed the political movement incited the mass at large number coupled with the satellite TV stations, the internet communication which is the new popular mainstream. Websites were designed for their own groups with the objectives to allow readers to access and stage their opinion such as the Manager Website, designed by the PAD, the Freedom Website designed by UDD and the Pantip Website which allowed people to stage issues for opinion and so on. In addition, the internet communication in the form of social media especially Facebook Network began to play the political role when politicians and political parties deployed the online social media for other to pursue their news. For example, there was the fans page of the Democrat Party, Chartpattnan Party, Mr. Abhisit Vejjajiva the Democrat Party leader and Dr. Thaksin Shinnawatr the Thai Rak Thai Party leader and so on (Pattamai Inthajan, 2008; Phirongrorng Rammasutr, 2010; Arthit Suriyawopngkul, 2012).

Period IV: the Political Violence in 2013-2014

The Thai crisis was born again after the resolution of The Amnesty Act Draft for political protesters and political demonstration of the parliament. This resolution was objected by many groups of people and tagged their objections. It was led by PDRC - People's Democratic Reform Committee, an Anti-government Protest Group, headed by Suthep Thuagsuban (Khaosod English, 2013). Even the senate rejected the resolution but the protester still active by changing the rally into resistance against the government reasoning that the government administration is not transparent and the corruption in many projects. The results of this rally pressured the

government dissolved and organized new election (Matichon Online, 2013). However, the protesters impeded the election and the government had to declare the State of emergency in Bangkok and its premises. Later there were clashes between the protester and the mob control authorities leading to many lives and injuries (Aljazeera, 2014).

This rally could be called the real cyberwar because it was the era of the popular online social media and it is part of human daily life (Nanthawitch Laowictchaya, 2013). This communication channel cannot be controlled or blocked perfectly by the public sector. The cyber space is special and beyond control of the public sector but it does not mean the public sector cannot do anything. To control and block are still active but not totally because users can open new services and perfectly hide themselves in the online social media (Thaweesak Kerdphokha and Ratiya Khathanya, 2013). The opinion can be explicit which allows various groups through online social media like Facebook and Twitter where opinion associates and organizes common activities for those with common political agreement. Moreover, the speed in dissemination of information, data and pictures attracts this communication type is used in running the political activity which provide clear results. Each political party uses online social media to stage their own public relation on information. In addition, it can discredit the opposite parties too (Wowpailin Chorwichian, 2011; Arthit Suriyawopngkul, 2012).

2.6. Related Laws against Hate Speech in Thailand and in Abroad

The efficient defense against hate speech requires true practical laws with severe retaliation and can deter individuals to act as such. The researcher thus selects related laws prevent hate speech from abroad like 1) USA, 2) the United Kingdom, and 3) Australia . Reasons are these countries accommodate hetero-ethnic groups and hetero-cultures. Thence, problem of hate crimes and hate speech would be prevailed. This is to study their laws, the definition and law enforcement to be as guides to amend and to develop the preventative measures against hate speech in Thailand.

Thailand

The constitution BE 2550 (2007) enacts individuals and mass media own rights and liberty of speech in Article 45 Paragraph 1 that

"Individual owns freedom of opinion, speech, writing, printing advertising and other method of communication."

Restriction to Paragraph 1 is prohibited except the power of provisions of law on the state security to protect rights, liberty, honor, fame, rights in family or personal life of others, to secure the peace and order or good morality of people or to prevent or cede mental deterioration or health of people…."

Though the Constitution BE 2550 (2007) allows liberty of individual opinion and mass media. Nevertheless, if the opinion or dissemination in any media with objectives against the national security and the expression is not in the constitutional frame; the actor is subject to offense according to the Criminal Code Article 116. Or if the statements or expression is characterized as libeling others; the law stipulates such act as an offense under the Criminal Code Articles 326-328 on the accusation of contempt.

Using hate speech in Thailand is never specifically enacted such offense is subject to the accrued punishment or other punishment measures. The wrongdoer will be examined as common wrongdoing as enacted in the Criminal code only. That is against the internal security of the Kingdom (Article 116) and the wrongdoing of contempt (Articles326-328).

Article 116: "Anyone acts to appear to people by word, book or any other methods and not he act under the intent of the Constitution or not the opinion or critique with honesty

(1) To change in the law of the land or the government by coercion or by assault

(2) To create chaos or rebellion among people so much to create unrest in the Kingdom or

(3) To allow people to violate law of the land are subject to imprisonment of not more than seven years.

Article 326* “Anyone imputing other to the third person by the possible act to damage fame, contempt, or hatred; the person is subject to offense of contempt and subject to imprisonment not more than a year for fined not more than twenty thousand Baht of both”

*[Article 326 is amended in the Criminal Code (Copy 11) BE 2525 (1992) dated February 14, 1992]

Article 327 “Anyone imputing the dead to the third person and the impute cause the father , the mother , the spouse to the children of the dead defamed, contempt or hatred; the person is subject to the offense of contempt and subject to punishment enacted in Article 326”

Article 328* “ if the offense of contempt is committed by documental advertisement, drawing, painting, movie, picture or letters by any methods, gramophone disk or sound recorder, picture recorder or letter recorder though broadcasting or on-air or by announcement by other method, the actor is subject to two-year imprisonment and fine of not more than twenty hundred thousand Baht.”

*[Article 328 is amended by the Amendment of Criminal Code Act (Copy 11) BE 2525 (1992) dated February 14, 1992].

However, exceptions for opinion actor to disseminate or the statement is not subject to offense of contempt enacted in Article 329 in the Criminal Code that

“Anyone comments or any honest statement

1) For justification, self-protection or protecting the stake for oneself by fairness

2) Being the official on duty

3) Critique with fairness where individual or anything with disposition of people should do

4) Inform with fairness on disclosures of act in court or in meeting.

The person is free from the offense of contempt.

If using hate speech displaying fake information or from modification, editing and used in online social media or computer system and possibly create damage for others, the national security besides subject to offense in the Criminal

Code and might offend according to Computer Offense Act BE2550 (1997) in Articled 14 and 16 enacted

”Article 14- anyone offends as following specified is subject to imprisonment for not more than five years and fine not more than hundred thousand Baht or both.

1) Load into the computer with fake information wither all or parts or false computer information with possibility to create damage for other or people.

2) Load into the computer with fake information with possibility to create damage for the national security or panic among people.

3) Load into the computer with any information against the national security of the Kingdom or offense of terrorism under the Criminal Code.

4) Load into the computer with any information with pornography and common people can access the computer information.

5) Disseminate or relay computer information by knowledge of being the information according to (1), (2), (3) or (4)”

“Article 16 – anyone accesses computer system which any people can access the computer information appears to be other’s pictures. And the pictures are built, edited, touched or modified with electronic methods or any methods with possibility to make others defame , contempt, hatred or endangered is subject to imprisonment for not more than three years and fine not more than sixty thousand Baht or both….”

United State of America

“The United States Constitution prohibits the making of any law respecting an establishment of religion, impeding the free exercise of religion, abridging the freedom of speech, infringing on the freedom of the press, interfering with the right to peaceably assemble or prohibiting the petitioning for a governmental redress of grievances.” (First Amendment to the United State Constitution).

USA under First Amendment to the United State Constitution provides rights and liberty to people in expressions being either the speech or religion or assembly. Besides the U.S. law does not define the meaning of hate speech with

specific. However, Hudson (2002) notes that any expressions or speeches within the scope of both cases will not be protected under the First Amendment to the United State Constitution, i.e.,

1. Incitement to imminent lawless action

The Supreme Court declares about the expressions or speeches, which are not within the scope to be protected by the First Amendment to the United State Constitution. The State cannot interfere or prohibit the speech or the expression for supporting the use of violence or the violation of laws except the act is the provocation or the incitement of violence or the violation of law (Brandenburg v. Ohio, 1969).

2. True threat

The Supreme Court defines true threat as the speeches or the expressers communicate the intention to use violence against individuals or groups and the speakers are not necessarily following the threat. To prevent threats is to protect individuals or groups from fear arisen from violence or threats to impose violence (Virginia v. Black, 2003)

In addition, hate speech can sometimes be turned to hate crime if action taken against individuals or groups. The hate crime laws aimed to implicate the wrongdoer who offends against victim caused by nationality, race, religion skin or gender. Its punishment is more server than the common laws generally enforced because such crime affects the sentiment of people wider than general crimes (Anti-Defamation League, 2012).

The statistics of offense lead to hatred arisen in USA. It is found that in 2012 there were 5,796 cases of such crimes. Half of the offenses were caused by racial bias followed by gender differences, religion and nationality, respectively (FBI, 2013).

The preventative measures against online hate speech in USA; the FBI uses Sniffer or software to detect which has been used in traffic information, which detects and choose some data detection programmed. Normally, this program is installed in the network software to scan internet traffics where the information could be sent. When the suspicious information is found, it will decode and retrieve data from the packet sent (internet sends every size of information by separating the data

into packet). For example, data indicate IP number of the sending computer or the received computer and every information has been exchange between both computers. The Sniffer used by FBI is called “Carnivore” which works like tapping by scanning the packet. Information in every packet exchanged among various computers and records just the information involved with the suspicious issue. “Carnivore” records letterhead that has sent (with name of the sender) and sent to whom. The data of the server in every website and every file uploaded or downloaded every file with IP number who enters to call for uses and enabling to pursue each one. Every computer accessing webpage or call for all files even the “Carnivore” work like “defensive” or does not enter to correct the content and does not block any statements. Nevertheless, detecting data as such is adequate to ease the job of the FBI because the US internet traffic passes through few giant companies for service providers. The FBI thus installs the “Carnivore” program with every center of the service providers.

Though the FBI specify this software will access data permitted by the Court only but “Carnivore” allows the FBI to access the internet data of all users who use ISP service and not just have the court warrant. This could easily violate personal rights (Nattaya Suksanguan, 2014).

England

England differently separates crimes from hate speech from other crimes. This offense is enacted in the Crime and Disorder Act 1998 with more severe punishment than other common offense. Hate speech becomes crime on the following conditions (Home Office, 2013).

1. Disability
2. Race or ethnicity
3. Religion or belief
4. Sexual orientation
5. Transgender identity

Hate speech enacted in three laws in England, i.e.

1. The Public Order Act 1986 – it is the law for securing peace and order within society. Hate speech is in Part 3 on Expression of Racial Hatred Article 18 enacted:

"A person who used threatening, abusive or insulting words or behavior, or displays any written material which is threatening, abusive or insulting, is guilty of an offence if -

a) he intends thereby to stir up racial hatred,

b) having regard to all circumstances racial hatred is likely to be stirred up thereby.

2. The Racial and Religious Hatred Act 2006 – this law is additionally enacted to the content of the Public Order Act 1986 on the issue of religious belief found in article 29J on Protection of freedom of expression enacted:

"Nothing in this Part shall be read or given effect in a way which prohibits or restricts discussion, criticism or expressions of antipathy, dislike, ridicule, insult or abuse of particular religions or the beliefs or practices of their adherents, or of any other belief system or the beliefs or practices of its adherents, or proselytizing or urging adherents of a different religion or belief system to cease practicing their religion or belief system."

3. The Criminal Justice and Immigration Act 2008 similar with The Racial and Religious Hatred Act 2006 enacted to add the content of The Public Order Act 1986. This law adds the protection of individual on gender and sex taste, which rejects by social, i.e. homosexual and bisexual as the contents found in schedule 16, article 29 AB:

"In this Part "hatred on the grounds of sexual orientation" means hatred against a group of persons defined by reference to sexual orientation (whether towards persons of the same sex, the opposite sex or both)."

The police-recorded hate crime during 2012-2013 was surged to 42,236 cases. A Crime Survey for England and Wales disclosed that during 2011-2012 and during 2012-2013, hate crimes surged 278,000 cases a year or 40% higher when entered the police process (Home Office, 2013).

Besides stipulating measures and punishment for hate crimes, the UK still impose measures of lawsuit to hate speech specifically in the internet having the public prosecutor to investigate and the interrogation contains two (2) parts, i.e.

1) The requirement of evidential sufficiency

2) The public interest

At first, a prosecutor must be satisfied that there is sufficient evidence to provide a realistic prospect of conviction. This means that an objective, impartial and reasonable jury (or bench of magistrates or judge sitting alone), properly directed and acting in accordance with the law, is more likely than not to convict. It is an objective test based upon the prosecutors assessment of the evidence (including any information that he or she has about the defence). A case which does not pass the evidential stage must not proceed, no matter how serious or sensitive it may be.

Communications sent via social media are capable of amounting to criminal offences and prosecutors should make an initial assessment of the content of the communication and the conduct in question so as to distinguish between:

1). Credible threats

2). Targeting specific individuals

3). Breach of court orders

4). Communication which are grossly offensive, indecent, obscene or false

If the offense were within the scope of 1-3, the lawsuit would be proceeded as above: seeking evidence and witnesses and later consider the impacts to pubic. But if it is within the scope of No. 4; the process of hearing is higher by examining necessity, and proportion of the expression. Based on human rights on freedom of speech enacted in Article 10 of The European Convention of Human Rights, which provide that

“Everyone has the right to freedom of expression. This right shall include the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers …”

Australia

Being the multiple-race country and cultures, it is necessary for the state to define rules to control the acts possible to become conflicts. Australia has a law to protect victims affected by discrimination, accusation and assault caused by the differences of race, skin, religion and sex in Racial Discrimination Act 1975, which is like the master plan of Australia.

The Racial Discrimination Act 1975 enacted actions including speech or dissemination of statements to public, which are characterized as intimidation, humiliation or insult caused by the differences of race, nationality, and skin to be offenses (Australian Human Rights Commission, 2012). However, actions become offenses when they are within the scope of:

1) The act is don't "otherwise than in private"
2) The act is reasonably to offend, insult, humiliate or intimidate
3) The act is done because of race, color or national or ethnic origin of the group However, people own the rights of freedom of speech, which the Racial Discrimination Act 1975 cannot be forced if the expression is from reasonability and good faith as of the four conditions, i.e.

1) An artistic or performance
2) An academic publication, discussion or debate
3) A fair and accurate report on a matter of public interest
4) A fair comment if the comment is an expression of a person's genuine belief

The lawsuit against the violation of the Racial Discrimination Act 1975 is that the victim at fist may want to deal with the situation himself/herself by raising it directly with the person or people involved or with a supervisor, manager or discrimination/harassment contact officer. If this does not resolve the situation, or victims do not feel comfortable doing this, victims can make a complaint to the Australian Human Rights Commission. They can also have someone such as a solicitor, advocate or trade union representative make a complaint on victims' behalf. If complaint is not resolved, or it is discontinued for another reason, victims can take

complaint to the Federal Court of Australia or the Federal Circuit Court. (Australian Human Rights Commission, 2012).

2.7. Related research

Gordon (2014) studies “Policy of Cyber Threat Prevention of New Zealand” and found that applying the theory of Cyber Deterrence against the cyber threat prevention in the country and in abroad resulted to the effective of cyber threat prevention in the country. However, there were arguments to follow the government policy in the dimension of intrusion of private rights of people.

Wei (2015) studied the result of applying theory of “Cyber Deterrence” in many countries, and found that it was inefficiently inapplicable. The impact factors are the current obsolete technology, international law enforcement, the absence of attribution, and inefficiency in the process of punishment.

Banks (2010), Cohen-Almagor (2009) studied, “Possibility to Reduce Violence from Online Hate Speech with Controls by Applying legal Measures and Techniques.” They found that controlling online hate speech with legal measures and supervising technology such as detection, agreement of the internet service providers and closedown of the users can reduce possible violence. In addition, these do not affect the right of free speech and information sharing.

Bailey (2006) and Banks (2011) studied “Restriction of Law Enforcement to Prevent Online Hate Speech”. They found that the law enforcement by charters and conventions if inefficient because of the opposition to law in each country. Therefore, to efficiently prevent online hate speech is not only focusing on law enforcement but to integrate working on supervision and control of technology such as pursuance and check or the involvement of the internet service providers. It includes also all sectors like the government, business sector, private sector and public have to involve in solving the online hate speech.

Henry (2009) studied “Limitations between the State Agencies and NGOs on Online Hate Speech. Finding that most state agencies focused on important or interested affairs only while NGOs, which are small organizations, cannot fully prevent online hate speech. Though given potential to carry out technically, they were

struck by time and sources. Therefore, efficiently preventing online hate speech better, both organizations were the important parts to reduce violence from online by using the strength of each party to the fullest uses.

A research of “Good Corporate Governance against Dissemination of Hate Speech” (Thai Media Policy Center: Faculty of Communication Arts, Chulalongkorn University, 2013) found that hate speech lead to violence such as incitement for hatred, assaults or intimidation through online space. There are three models in Thailand, i.e. webboard, social media and clipping VDO of YouTube. There are four (4) levels of violence, i.e. 1) unclear objectives, 2) creating misunderstanding, 3) provocation for hatred and 4) eliminating the targeted groups. At present, the context facilitating hate speech is political conflict. Users at 36.7% use hate speech in Facebook. 53.0% use webboard and 75.8% use YouTube. Most violence is provocation for hatred against the targeted groups by accusation, violent allegation, condemnation, disclosure, gossip, insult, disparage, amusement, devaluation, discredit before others, severe sarcasm, serve-someone right, defame and inhuman comparison.

In addition, this research suggests that governance over online hate speech requires watching the nature of media with its different objectives toward the targeted groups and the levels of violence. Some contents might not need supervision. Moreover, it requires mixed model such as if the hate speech for encouraging hatred against individuals or groups; the supervision could be efficient through supervising the mediate. However, if the hate speech is to incite violence against the target; it should be subject to legal supervision (Thai Media Policy Center: Faculty of Communication Arts, Chulalongkorn University, 2013).

Asst. Prof. Phijittra Zukamoto (Sunai Phasuk, 2014) suggested approaches to control and supervise the dissemination of hate speech with balancing between hate speech with media freedom by not allowing the state authority to deliberate on supervision media but draw all non-government sectors to participate in supervising contents. It might require a committee from the professional organization to watch dissemination of hate speech, which might lead to hate crime.

Mr. Arthip Jittarerg (2012) recommended law enactment to control hate speech, which deserves legal restrictions since it may lead to physical violent acts. The relationship between hate speech, which the media creates physical violence has to be

proved that any media are hate speech themselves especially. And if the hate speech yield legal outcomes; it needs to prove first that it create hatred and leads to physical violence and the alleged must prove what one say is not hate speech on the principle that the alleged is innocent unless proved guilty. Burdens of proving must be focused on the alleger and not the alleged to prevent the law of hate speech insulting identity and is over used in political coloring. In addition, hate speech should be civil case that can be compromised and not to be the criminal caw. If it has to be criminal case, it should meet petty punishment only. Finally, victims of hate speech should be individuals or groups suffering the consequences of hate speech only and not the well-wishers.

Ms. Chanansara Orranop Na Ayudhya (Thai Media Policy Center: Faculty of Communication Arts, Chulalongkorn University, 2013) noteed that it needs mixed approaches. Media disseminating hate speech of the first level must not be supervised by the state but by media themselves. The contents creating severe hatred deserves supervision under law enforcement by the organization supervising radio and TV and by the social supervision on what measures against media creating hatred. In addition, receivers should be encouraged to know as media, individual potential development in the media profession, retaliation against contents crating hatred with non-violence and enhancement of social norms. A supervision of the organization supervising radio and TV has to appropriately supervise on the content creating hatred to persuade violence against the target. at present, the domestic laws and international laws have covered contents creating hatred. However, examining offense, it should not be only examining the content but it needs to examine its environmental contexts and also examining whether it immediately links hatred to danger of violence or not.

2.8. Research Conceptual Framework

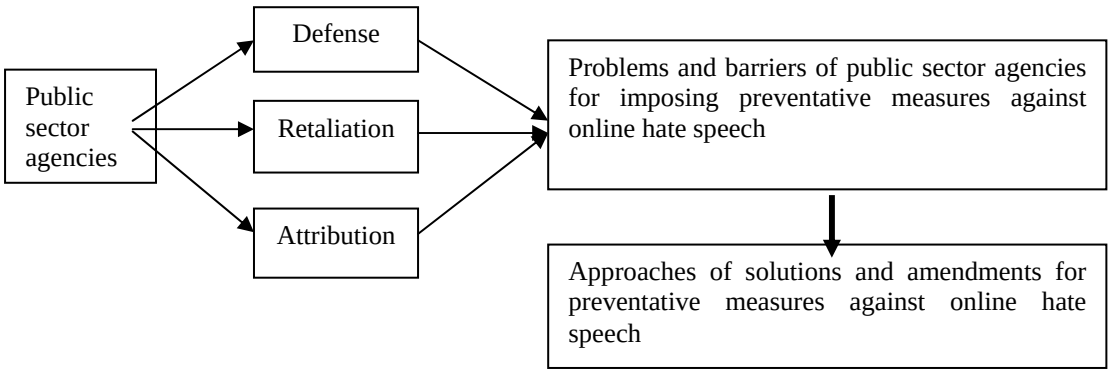

Figure 2.1: Research conceptual framework on preventative measures against online hate speech: a case of political conflict
Source: Haley, 2013

From literature reviews on concepts, theories and related research, the researcher could conclude the conceptual framework as in Figure 2.1. The preventative measures against online hate speech have to be based on the Cyber Deterrence theory, which involves three elements, i.e., defense, retaliation and attribution. The consequences of the public sector agencies responsible for planning and setting preventative measures against online hate speech would display problems and limitations of those measures currently applied. They are divided into three issues according to the elements of the Cyber Deterrence theory advocated by Haley (2013). This will lead to recommendations of remedies and improvements of the preventative measures against online hate speech.

Definition of the Terms

1) Hate Speech is referred to expression by any acts either speaking or announcement or advertisement or dissemination by other methods which display insult, contempt, sarcasm, discrimination and devaluation of humanness by deploying the causes of race, religion, ethnic, skin, language, social status, sex or by other

reasons. The consequences might lead to violence or endanger any individuals or any targeted groups.

2) Public sector agencies are referred to official workplaces related to controls and suppression against online hate speech. They involve two aspects, i.e. 1) the agencies of policymaking and planning involving Ministry of Information Technology and Communication, the National Broadcasting and Telecommunications Commission, Technology Crime Suppression Division (TCSD); 2) the agencies suppressing crimes, i.e., Technology Crime Suppression Division (TCSD).

3) Defense is refereed to prevention not to allow individuals to use online hate speech. It involves three parts, 1) capabilities - skills or potentials of the tools and equipments used in prevention, 2) communication – cooperation within the agency and between agencies in stipulating preventative criteria against online hate speech, and 3) credibility – displaying ability to suppress wrongdoings.

4) Retaliation is referred to measures or procedures after arrest or by identifying the users of online hate speech,

5) Attribution is referred the investigation to identify who are the wrongdoers in using online hate speech.

CHAPTER III
RESEARCH METHODOLOGY

The objectives of this study were to investigate the current preventative measures and the approaches to amendment and improvement of those preventative measures of the public sector agencies against online hate speech, particularly in the case of political conflict. Another objective was to adopt the findings to be as guides to amend and to develop the preventative measures. The research methodology was a qualitative research methodology involving in-depth interviews for data collection enabling a response which perfectly matches the research objectives.

3.1. Methodology

The process began with a review of the related literature covering theories, previous research, and documents involved with the preventative measures against online hate speech in the case of political conflict, in order to formulate a conceptual framework.

In-depth interviews conducted with this qualitative research aimed to collect detailed in-depth data related to the preventative measures against online hate speech in the case of political conflict. The researcher purposively selected informant interviewees from the responsible agencies in charge of the monitoring, control and supervision of online social media users.

3.2.Sampling Method

The data collection was made through in-depth interviews with interviewees selected via purposive sampling, and the key informants comprising key personnel of policymaking and policy implementation in the field of planning and stipulation of preventative measures against online hate speech.

Consequently, the population comprised the public sector personnel directly involved because they could provide accurate, precise information to meet the research objectives while representing the entire population. The 24 key informants were purposively selected from:

1) Eight (8) informants from the Ministry of Information Technology and Communication

2) Eight (8) informants from National Broadcasting and Telecommunications Commission (NBTC)

3) Eight (8) informants from Technology Crime Suppression Division (TCSD)

3.3.The Research Instrument

The interview questions were based on a semi-structured interview formulated from processing the concepts, which gained from the literature review involving the influences of IT on human behaviours, anti-crime theories and deterrence theories in the cyber world. All the questions must fit within the conceptual framework of this research. The interview questions covered:

3.3.1. Authorities of the responsible agencies against online hate speech

3.3.2. Related laws against online hate speech in the case of political conflict

3.3.3. The existing approaches and measures to monitor, control and supervise online hate speech

3.3.4. Barriers and limitations against online hate speech

3.3.5. Recommendations, amendments and the improvement of the preventative measures of the public sector agencies against online hate speech in the case of political conflict

3.4.Data Collection

3.4.1. The researcher reviewed the related literature to form the basis of the theoretical background and concept in order to properly specify the course of the investigation.

3.4.2. The interview format for the data collection was founded on the theories and concepts reviewed in the literature and congruent with the research objectives.

3.4.3. The researcher applied a face-to-face in-depth interview technique to disclose the motivation and attitude of the informants by specifying questions to cover the research objectives. Before interviews were conducted, the researcher informed participants of the objectives of the interviews and obtained approval for taking notes and recording. The researcher freely interacted with the interviewees to enable the flow of exchanged opinions.

3.4.4. During the interview session, the researcher took notes on the important and interesting issues while also recording the interviews.

3.4.5. The information collected from the interviews was decoded for its completeness and the information from interviews was re-checked by the interviewee for accuracy.

3.5.Data Analysis

3.5.1. Analysis method

A typological analysis by the conceptual framework was applied with the qualitative data collected from the in-depth interviews. This was to find their links and relationships to meet with the research objectives. The analysis process was to decode each interview to explore whether the interviewees had adequately responded to the research question.

3.5.2. Checking the validity and reliability of the data

The research applied a triangulation technique to check data validity and reliability, which involved time, place and persons. This was because in this investigation, the researcher conducted in-depth interviews with three groups of personnel involving different times and places. Furthermore, in each key informant group, there were many members questioned for data collection.

CHAPTER IV
RESEARCH RESULTS

This research focused on the current preventative measures of public sector agencies against online hate speech in the case of political conflict. It would lead to remedial approaches and development for better efficiency. In-depth interview was conducted with key informants from public sector agencies who played the roles and duties of their stipulation and application. Data were applied with typological analysis and synthesis. Presentations of the analysis were divided into five (5) parts, i.e.

Part I: The authority and responsibility of the agencies against online hate speech

Part II: Related laws against online hate speech

Part III: The existing preventative measures against online hate speech

Part IV: Barriers and limitations of the current preventative measures against online hate speech

Part V: Recommendations of the remedial approaches against online hate speech: in the case of political conflict

This research offered comparative results on similarities and differences of data gained from in-depth interview in each part conducted with the public sector agencies related to the stipulation and the applications of the preventative measures against online hate speech. The public sector agencies are:

1. Technology Crime Suppression -TCSD
2. Ministry of Information and Communication Technology -MICT
3. The National Broadcasting and Telecommunications Commission – NBTC

Details of the results are as below.

4.1. Part I: The authority and responsibility of the agencies against online hate speech

From the data collection of the three agencies, results show that the authority and responsibility are enacted in laws or regulations in each copy and lead to the differences of authority and responsibility in each agency. Each authority and responsibility in each agency is presented below.

4.1.1. Technology Crime Suppression Division –TCSD

The research results show that its authority and responsibility are regulated in the Office of the National Police Bureau on Duties of the Office of the National Police Bureau BE 2552 (2009) with major duty of technology suppression crimes, investigating to find the wrongdoers under the Criminal Code and the Criminal Penalty Act found in the computer system. TCSD operations are subject to the Computer Related Crime Act BE 2550 (2007). Informants from TCSD noted:

> *TCSD authority and responsibility are subject to the regulations of the National Police Bureau on Duties of the Office of the National Police Bureau BE 2552 (2009) recently amended. In short, it is the authority of investigation and interrogation, and suppression of cyber crimes which by principle, it is the offense according to the Computer Related Crime Act BE 2550 (2007) including other related offenses around the Kingdom. (Personal interview, November 25, 2014)*

Crimes or offenses under the TCSD responsibility are enacted in the Royal Decree of the Divisions of the Office of the National Police Bureau BE 2522 (1979). Examining various offenses, cyber crimes could be divided into three types by “roles” of the computer, which involve in wrongdoing (personal interview, 25 November 2014). The three types of cyber crimes are:

1. Computer as target – for example hacker, hacking, attacks or computer modification

2. Computer as an instrument of crime – such as cheating and fraud online, patent violation online and gambling online and so on.

3. Bad content (prohibited information by Computer Related Crime Act BE 2550 (2007)) such as uploading the false information damaging others, panic information, the state insecurity information and pornographic contents

Considering details of each type, there is a difference between "the computer as a target" and "computer as an instrument of crime". "Computer as an instrument of crime" the targets might be something else, not just computer system, by using the computer system.

On the contrary, the offense of bad content is different from the two types above because this offense would be assessed as a crime when it is uploaded in the computer system and subject to the Computer Related Crime Act BE 2550 (2007). Online hate speech is categorized as bad content.

4.1.2. Ministry of Information and Communication Technology – MICT

Data collections from MICT reveal that the ministry is subject to the Act on Organization of Ministries, Sub-Ministries and Departments B.E. 2545 (2002) authorized on planning , promoting, developing and operating ICT and other public affairs enacted (personal interview, 8 December 2014). The suppression of online hate speech is under the responsibility of Technology Crime Suppression and Protection Office.

This office operating against online hate speech is policymaking that people can creatively and freely express opinions without violating others' rights and liberty (personal interview, 8 December 2014). In addition, another duty of this office is support other agencies on the convergent policies. One informant in the ministry noted:

> *Technology Crime Suppression and Protection Office operates under the Computer Related Crime Act. B.E. 2550 (2007) and the Criminal Code complement to suppression of bad content websites …the authority of the ministerial personnel*

> *is in accordance with the legal authorization in supporting information regarding evidences. When the personnel collect evidence, they will be submitted to the interrogation officer for proceeding lawsuits. (personal interview, 16 December 2014)*

4.1.3. The National Broadcasting and Telecommunications Commission – NBTC

Data collections from NBTC show that the responsibility of NBTC is monitoring the affairs of broadcasting, TV and telecommunications. The authority is enacted in the Act on Allocation of Frequency and Supervision of Broadcasting Radio, Television and Telecommunication BE 2553 (2010) (personal interview, 24 December 2014). Regarding online hate speech, it is subject to Telecommunication Enterprise Act BE 2544 (2001) and the Communication Radio Act BE 2498 (1955). However, the authority of NBTC does not directly monitor in online hate speech behaviour, but indirectly involved. Meaning, it does not supervise the content within the computer but just supervise the licenses to provide internet services to cooperate with the public sector for control the uploading content on the internet. An informant noted:

> *NBTC is an office supervising the internet channel only. It is like a road and the contents are like cars, which NBTC will look after the road only but not any cars. However, internet service providers (ISPs) have to follow the regulations, which include the content too (personal interview, 22 December 2014).*

In summary, the differences between the three agencies on their authority and responsibility against online hate speech, TCSD is the key to investigate, arrest wrongdoers and suppression. MICT is the support information unit to the agencies, and analyzes policymaking for the people to use the information technology rightfully. On the other hand, NBTC has no authority to control the content but supervision and control internet service providers (ISPs) to cooperate with public sector agencies and to follow the condition as permit, including the prevention on uploading bad content in the internet.

4.2. Part II: Related laws against online hate speech: a case of political conflict

Besides studying the authority and responsibility of the three agencies as in Part I, the researcher has studied laws and regulations of each agency enforced in their operations how are they similar or different. Their details are as below.

4.2.1. Technology Crime Suppression Division –TCSD

Data collection of laws related to TCSD enforced against online hate speech, TCSD mostly enforces the Computer Related Crime Act BE 2550 (2007) coupled with Criminal Code or other related laws. Statements in computers by laws are called "Computer Information". However, information in internet is right or wrong, it depends on offense enacted in the Computer Related Crime Act BE 2550 (2007) or not. If the statement creating hatred in social media and matched with the offense against the Computer Related Crime Act BE 2550 (2007), then it become a offense as enacted in Article 14 with 4 sub-Articles. However, hate speech converges to any offense or not, needs to examinations on other statements such as gestures, emotion and environment at that time (personal interview, 24 November 2014).

There is no specific law enforced against hate speech and political conflict, but just the Computer Related Crime Act BE 2550 (2007) which authorized the officers appointed with more special authority than others. Moreover, it is in accordance with Article 18 as of calling for internet data log or information from ISPS, validation, seizure and confiscation. These special authorities are the common authority, not specified only against any hate speech. An informant noted that:

> *...At this moment, there is no law identifying that hate speech is an offense but it needs other article of law on part of the statement or the entire statement is an offense. TCSD officer has no authority over the administrative personnel or the police as in the Criminal Procedural Code. But TCSD officer will appoint some of them as enacted in the Computer Related Crime Act BE 2550 (2007). They will own special authority more than being enacted in the Criminal Procedural Code, for example*

they can call for internet data log or information from ISPS. (personal interview, 24 December 2014)

Investigating to locate the wrongdoers is based on the Criminal Procedural Code to be enforced with regards to interrogation, validation, and collections of evidence coupled with the Computer Related Crime Act BE 2550 (2007). This code specially authorizes the officers as aforementioned (personal interview, 24 November 2014).

4.2.2. Ministry of Information and Communication Technology – MICT

MICT enforces two laws against online hate speech, in the case of political conflict, i.e. 1) Criminal Code and 2) the Computer Related Crime Act BE 2550 (2007). Online hate speech could be categorized in two types, i.e.

1. Common offenses under the Criminal Code, which is victimized by the computer system, for example defamatory libel in social media
2. Offenses enacted in the Computer Related Crime Act BE 2550 (2007), for example uploading false information into the computer system under Article 14(1) or (2)

Investigating offenders, MICT prominently enforces Article 18 of the Computer Related Crime Act BE 2550 (2007) in collecting evidences, for example, inquiring internet data log or information from ISPS and so on. Furthermore, the Computer Related Crime Act BE 2550 (2007) requires ISPS to store internet data log and users, if not, one is subject to specified retaliation (personal interview, 16 December 2014).

4.2.3. National Broadcasting and Telecommunications Commission – NBTC

Online hate speech, particularly in the case of political conflict, NBTC is responsible for supervising ISPS to follow the license conditions as in the announcement on the Standards Condition of Permit on Telecommunication Enterprise only. If ISPS fail to follow the license condition, for example cooperation

with the public sector upon request or stipulation of measures against offenses (personal interview, 22 December 2014), NBTC could begin the process for action taken beginning from warning until license withdrawal. An informant validates the action taken by NBTC that:

> *…Upon failure to abide with license conditions of the licensees, They fail to follow MICT Announcement of Standards Condition of Telecommunication Enterprise. The administrative punishment is then imposed because the telecommunication service is the matter of public services and does not affect the peace and order, which is subject to criminal punishment. The administrative retaliation begins with ordering, warning, license withdrawal and so on (personal interview, 24 December 2014).*

Although an authority and responsibility of any public sectors agencies against online hate speech are different in each other, but the laws and regulations enforced in each agency being either TCSD or MICT are the same, the Criminal Code and the Computer Related Crime Act BE 2550 (2007). Except NBTC, the prominent authority of this sector is the authority of supervising ISPS to follow the license conditions as in the NBTC Announcement of Standards Condition of Telecommunication Enterprise.

4.3. Part III: The existing preventative measures against online hate speech: a case of political conflict

4.3.1. The preventative measures or Defense

One of the measures enforced by the public sector agencies against online hate speech, in the case of political conflict, is the preventative measure. All agencies currently enforce public relations, education, knowledge building and understanding on internet use. Furthermore the three agencies: TCSD, MICT and NBTC, the watch

centers have been established to inspect websites along with the complaint centers. Details of the study result are as below.

4.3.1.1. Technology Crime Suppression Division –TCSD

TCSD's preventative measure against online hate speech, in the case of political conflict, imposes public relations, education and knowledge building and understanding of laws which includes how to use internet properly. This is through projecting, and activities, e.g. project of clean online, this project emphasizes on education and public relations to youth students in schools about how to safely and appropriately use internet (personal interview, 24 November 2014). Negligence to receive information on their accuracy affects political attitude among people, leading to the political movements. A TCSD informant suggested some preventative measures that:

> *…There are two TCSD preventative measures: 1) public relations through website: www.tcsd.in.th of the TCSD. 2) Aggressive measures through participating the community activities or various institutions to educate on useful use of social media and this is to build the community network to prevent also other wrongdoings. (personal interview, 27 November 2014)*

Additionally, TCSD has established cyber crime watch centers for monitoring the internet information whether these are offenses/affect security or not. These watch centers will reports all related information to the agencies involved for immediate action taken.

4.3.1.2. Ministry of Information and Communication Technology – MICT

Public relations, educating on laws and proper uses of internet as in the interview results are the preventative measures against online political conflict hate speech. In addition, the ministry focuses on children and youth by organizing projects for them to post their opinions without infringing any rights of others (personal interview, 8 December 2014).

The aggressive measure is to establish the watch centers to check various websites and the compliant centers. If something is possible to commit an offense or to affect security, warnings to the users or ISPS will immediately be taken as one of the MICT personnel noted that.

> *…MICT monitors improper websites around the clock with complaint centers and propagates the Computer Related Crime Act BE 2550 (2007) for people and various public sector agencies to recognize the law. (personal interview, 16 December 2014)*

4.3.1.3. The National Broadcasting and Telecommunications Commission – NBTC

NBTC is not directly responsible to control the internet content or information. However, it supervises ISPS to follow the criteria and condition as in the license. There are measures against online hate speech through organizing seminars for ISPS, giving order to always monitor the internet system and cooperate with the public sector upon request or coordination.

Moreover, NBTC provides public relations, education and organization of activities to educate related law and the ways to properly use of internet. The complaint center also is the other channels for reporting any information so that the personnel will further take action. As one of NBTC informant noted that:

> *...The online hate speech is beyond NBTC authority but we supervise ISPS to follow the license conditions. Action taken by NBTC is to directly cooperate with agencies involved – TCSD and MICT (personal interview, 23 December 2014).*

Examining all the preventative measures from all the three agencies, there is no difference because all of them emphasize on public relations, knowledge building on laws and the proper uses of internet through various projects

with the cooperation of people. Moreover, another way is an aggressive measures, the establishment of watch centers and complaint centers.

4.3.2. The measures of legal retaliation or punishment

Suing wrongdoers or criminals is another measure against online hate speech particularly in the case of political conflict. TCSD focuses prominently on investigation and arrest whereas MICT and NBTC support the TCSD to impose lawsuit with offenders. In addition, the responsibility of NBTC is to supervise ISPS to follow the license conditions. Consequently, if anyone fails to comply with the conditions, NBTC has the authority to impose retaliation on them. However, the criminal punishment is not under any responsibility of these three agencies. Results of lawsuit by each agency are as follows:

4.3.2.1. Technology Crime Suppression Division –TCSD

The existing TCSD measures are the investigation and arrest the offenders. Moreover, the cooperation with other agencies and private sectors to charge offenders are the strategies of TCSD as well. However, the punishment is exactly related to the responsibility of TCSD, but relies on the adjudication of the court. In addition, the process on any suspects, TCSD has made the watch-list to monitor and prevent potential offenders or recidivists. One of the TCSD informant stated that:

> *….The TCSD watch-list projects process like the projects of Immigration Bureau – the internet watch-list which includes the political conflict. TCSD prominently works in pair with MICT. Meanwhile, the coordination with private sectors, TCSD mostly works with ISPS to gather offensive information, leading to arrest the offenders for lawsuit (personal interview, 24 November 2014).*

4.3.2.2. Ministry of Information and Communication Technology – MICT

The mainly retaliation measures of MICT for action against the wrongdoers are the cooperation with the interrogation officers by supporting and providing information and evidence (personal interview, 3 December 2014). Additionally, in the case of finding any probable statements or speech against laws or security; the internet users would be warned by MICT. If the users disregard, MICT and the interrogation officers will further enforce the lawsuit on them (personal interview, 8 December 2014).

In part of retaliation or punishment enacted for the offenders unlikely authorizes by MICT because the adjudication is empowered by the court only. However, a MICT informant commented about the appropriate retaliation or punishment in compliance with the Computer Related Crime Act BE 2550 (2007) that:

> *… The Computer Related Crime Act BE 2550 (2007) is the criminal law enacted both imprisonment and fine with severe punishment than common law. In my opinion, the existing enacted punishment is worth to a certain extent because the impact of offense is more damageable. So they deserve higher punishment (personal interview, 16 December 2014).*

4.3.2.3. The National Broadcasting and Telecommunications Commission – NBTC

Controlling the computer content is not the responsibility of NBTC. In the same way, punishment on the accused offenders of online hate speech seems unlikely as well (personal interview, 22 December 2014). The duty of NBTC is report the information to TCSD or MICT, which own duties of suppression.

Nevertheless, NBTC directly supervises ISPS to cooperate with other public sector agencies and follow the license conditions. Furthermore, ISPS must not to involve with any activities possibly against security. If not, NBTC could enforce the administrative power to impose retaliations beginning from warning to license withdrawal. A NBTC informant commented on retaliation that:

> *… NBTC supervises only the internet providers to follow license conditions. However, the offenders are common people not ISPS. If ISPS do not follow the license conditions, they are subject to legal punishment, which is the administrative retaliation not criminal punishment. This is because the internet service providing is the public service, which does not against the peace or order. By administrative measure. The administrative punishment begins with ordering, warning, and until license withdrawal (personal interview, 24 December 2014).*

When considering the lawsuit against offenders in each agency, there are obvious differences about the retaliation measures in each other. The retaliation processes of TCSD are mainly the investigation and arrest the offenders for lawsuits, whereas MICT generally supports the information and evidence leading to lawsuit. Clearly, NBTC has no responsibility of arrest offenders, but just supervises ISPS to follow the license conditions.

In term of punishment, all of them have no responsibility of judgement. The court is the only one agency in the criminal justice, which has the responsibility of judgement.

4.3.3. The measures of attribution

The critical measure against online hate speech is attribution. TCSD and MICT prominently enforce the Criminal Procedural Code and the Computer Related Crime Act BE 2550 (2007) for seeking evidence to attribute or identify wrongdoers. Nevertheless, gathering the evidence for attribution the offenders is met barriers. For examples, the website servers are located abroad, or the social media has no regulation of attribution the users and so on. Not just supporting ISPS to cooperate with the public sector for seek the evidence, NBTC, additionally, owns duties to collect data of mobile-phone users. However, the registration of the mobile-phone users is met with hindrances at present.

4.3.3.1. Technology Crime Suppression Division –TCSD

The attribution measures of TCSD are guided by the Criminal Procedural Code and the Computer Related Crime Act BE 2550 (2007). Because the online hate speech occurs in cyber space, actually there is no eyewitness to attribute the offenders. So the officers' duties are gather all electronics evidence and circumstantial evidence, which probably identify who the offenders are. To fulfill the process, there are two steps of investigation 1) physical investigation and 2) computer investigation. One of TCSD informant commented on attribution that:

> *…Attribution needs to specify the time of offense. We investigate to assert identity. Normally, wrongdoers use the computer for committing crime; the hardware connects with the system. And the system leads to outputs. Therefore, investigation has to be retrospective until we can locate the device. Then we have to identify who the offender is (personal interview, 27 November 2014).*

Essentially, gathering evidence for specifying the wrongdoers during such period of offense. ISPS can provide such internet data log (computer investigation). They have to keep records for 90 days enacted by law, and must hand over the data to the officers upon request. When time and place are confirmed, the officers must gather evidence to prove guilty on the person who uses the devices as tools for committing offend at that specific period of time (physical investigation) (personal interview, 25 November 2014).

4.3.3.2. Ministry of Information and Communication Technology – MICT

In term of attribution, MICT is authorized to enforce the Computer Related Crime Act BE 2550 (2007) to call for internet data log from ISPS, if it is not exceeding 90 days. MICT collaborates with the interrogation officers by support the information and evidence for imposing both technical and physical investigation (personal interview, 16 December 2014).

Even so, problem of calling for internet data log is the oversea location of ISPS. As a result, the law enforcement of The Computer Related Crime Act BE 2550 (2007) is limited. Therefore, seeking data or evidence is impossible. The MICT informant commented on this point that:

> *…the attribution measure is bound with law. ISPS have to store data for 90 days. Nevertheless, there are still problems arisen on disabling to collect data such as using computer technology avoidance or the servers are located abroad. Besides the usage of computer information for attribution, there are other circumstantial evidence could be use as well such as phone number or email. (personal interview, 8 December 2014)*

4.3.3.3. The National Broadcasting and Telecommunications Commission – NBTC

In term of attribution, NBTC, which have the authority to supervise ISPS, reiterate them to provide internet data log to the public sector agencies and cooperate upon request. In addition, NBTC owns the duty to control the internet usage through mobile phones by specifying any enterprises to systematize registration for users. However, the registration is met with barriers, with either the users or the enterprises themselves. The NBTC informant commented that:

> *…In attribution, if the communication is connected through the internet, it we could check from IP address. Even so, it is necessary to prove the wrongdoers. If the communication if connected through mobile phones, by the announcement of the number allocation, the license holders have to systematize registration for the helpful of pursuance the number owners. Nonetheless, there is no assignment of registration methodology. Consequently, it creates loopholes for avoidance (personal interview, 24 December 2014).*

The process of attribution measure, TCSD and MICT are similar – enforcement of the Computer Related Crime Act BE 2550 (2007) and the Criminal Procedural Code in order to identify offenders. The necessary attribution is to call for the internet data log from ISPS. These data would helpfully trail the wrongdoers. Nonetheless, there are the obstacles on the process. For example, the length of data storage is exceeding 90 days or ISPS are located abroad.

On the other hand, the only authority of NBTC is the supervision on ISPS to follow the license conditions. Even so, in term of attribution, NBTC gives the importance to cooperate with the public sector agencies by supporting data or evidence. Additionally, NBTC has the main authority to control the mobile internet using. At the present, there are criteria for the registration of mobile phone users. This rule is very helpful to the attribution when the hate speech is uploaded in the mobile phones.

4.4. Part IV: Barriers and limitations of the existing preventative measures against online hate speech

The research results reveal that barriers and limitations for officers on preventative measures against online hate speech weaken the efficiency of the action taken and consequently affect people's behaviour as mentioned above. TCSD's problems and limitations are the gathering evidences, which affects lawsuit in the justice administration, e.g. attribution in the social media and the ISPS are located abroad. Furthermore, another factor, which weakens the efficiency of the preventative measure, is the soft retaliation.

Meanwhile, MICT personnel commented that the problems of attribution, which including the problem in the users' registration, also weakens the efficiency of the preventative measure. Soft retaliation is another problem as well. These result to harden to arrive at the goal of punishment. Moreover, the different political attitudes of the Thais and misunderstanding in information received become the roots of the rift inonline hate speech. Finally, NBTC's problems and limitations are the disharmony of internal administration. Classifying by agencies on the research results of problems and limitations against online hate speech is as below.

4.4.1. Technology Crime Suppression Division –TCSD

The research results disclose that the problems weakening the efficiency of the TCSD officers against online hate speech are the limitations of attribution, gathering evidence, in case ISPS are located abroad and soft retaliation.

4.4.1.1. Limitations of attribution

The foremost problem of Thailand is the discouraged infrastructure in the attribution (personal interview, 27 November 2014).

Eight interviewees provided the important problems weakening the preventative measures against the speech online in the case of political conflict are the masquerade in social media caused by internet system in Thailand., for instance Facebook, Twitter and Instragram and so on (personal interview, 25 November 2014). Even though, the Computer Related Crime Act BE 2550 (2007) authorized to call for the internet data log from ISPS, which probably guides to the attribution, but the prevention on online hate speech is failure. The cause is gathering evidence for indentifying the wrongdoers is hard, because of regarding timeframe of ISPS's data storage; abroad located ISPS and verification of the offenders. Consequently, the offenders could commit without fear of arrest. A TCSD informant noted that:

> *….Internet system in Thailand discourages the enforcers to gather evidence or to seek the facts. For example, such as gateways or communication channels between Thailand and abroad have no intercept systems, checkpoints and users' registration (personal interview, 25 November 2014).*

4.4.1.2. Limitations of evidence collection, if servers are in abroad

Seven interviewees from TCSD claimed that the expression of political opinion in Thailand is extensively posted online, which could divided into 2 types. First, web hosting is located in Thailand such as Manager Online (www.manager.co.th) or Pantip Onlone (www. panthip.com). Second, web server

hosting is located outside Thailand such as Facebook, Twitter and Instragram and so on. But the officers can lawfully gather the evidence just for the offenses committed in Thailand. In the same way, the offenses have to be committed through the internet website which their server hosting is located in Thailand. For the located web server hosting outside Thailand, the officers are disable able to enforce the law on them. An informant commented that:

> *… In case server hosting is located abroad, there is hardship to coordinate for information from abroad. The processes have to take a long time or never receive any information because the existing laws cannot enforce in abroad (personal interview, 25 November 2014).*

The interviews showed that, there are barriers to gather evidence in case websites or social media server hosting is located outside Thailand. At the present, social media is used as the widespread channel to express the political opinions in Thailand, e.g. Facebook, Twitter and Instragram and so on. Many people utilize the gap in law to express the political opinion with the objectives to incite the mass, creating schism and opposing political point of views by using hate speech. But they do not concern about the truth of content (personal interview, 24 November 2014).

4.4.1.3. Undeterred retaliation

From eight interviewees, the soft retaliation against offenders impacts the determent on online hate speech. The results showed two different opinions about the current retaliation measure, i.e.

1) Not severe enough violent punishment if being compared with the damage, so it is undeterred

2) Appropriate retaliation but on process of adjudication, punishment does not severe enough if being compared with the damage.

When classifying by the law, online hate speech could categorized into two types, 1) common offense against Criminal Code and 2) offense

against the Computer Related Crime Act BE 2550 (2007). Each law enacts different punishment. For example, if the offenses are assessed as the defamatory libel by Article 326 of the Criminal Code, the sentence is for not more than one-year imprisonment or fine not more than twenty thousand Baht (20,000) or both. If the defamatory libel by advertisement or any other ways enacted in Article 328 of the Criminal code, the sentence is not more than two years imprisonment or fine not more than two hundred thousand Baht (200,000) or both. If the online hate speech met offense enacted in the Computer Related Crime Act BE 2550 (2007), Articles 14, 15, 16 or 17; the punishment enacted is higher than the enacted in the Criminal Code. For example, in Article 14, the sentence is not more than five years imprisonment or fine not more than one hundred thousand Baht (100,000) or both.

The data from the interview shows that, in case of the disproportionate of punishment, the retaliation measure cannot deter the offender from fear of recidivism or fear of arrest. The wrongdoers no longer feel any guilty of misbehaviour. It is corresponded with an informant that:

> *…the punishment deserves amendment for more severity because the data in the internet still exist for a long time. Therefore, any person by any acts should feel responsibility more than common people (personal interview, 24 November 2014).*

4.4.2. Ministry of Information and Communication Technology – MICT

The data collection from MICT shows that problems and limitation against online hate speech, especially in the case of political conflict, could be divided into four issues, i.e. attribution, gathering evidence if server hosting located abroad, undeterred retaliation, the difference in political attitudes and misunderstanding in received information.

4.4.2.1. Barriers of attribution

Seven interviewees commented that the disguise sustains a problem in social media. Member registration in some social media, such as Facebook,

Twitter and Line, is unnecessary to use real name. As a result, any expression in social media is impossible to identify the posters. So they probably feel without fear of arrest (personal interview, 9 November 2014).

In addition, five informants added that an important problem is disability on sim card registration in Thailand. The offenders could use unregistered sim card in various forms of offenses, including posting online hate speech. Consequently, the attribution measure is ineffective (personal interview, 16 December 2014). Recently, any measures of related agencies have been enforced to register sim card, but there is unlikely cooperated from the service providers and users. An informant commented about this issue that:

> *…Using pre-paid telephone for posting online hate speech is disregarded by service providers in collecting data (personal interview, 8 December 2014).*

4.4.2.2. Barriers of gathering evidence if server hosting is located abroad

Six interviewees informed that, in case, server hosting is located outside Thailand such as Facebook or Twitter, become vast barriers of gathering information and evidence for attribution. Thus, this loophole in the process allows the posters to express online hate speech without fear of arrest, including incitement, and creating schism from political conflict. The important reason is the failure of law enforcement if web hosting is located outside Thailand. An informant commented on this problem that:

> *…Facebook is the most important problem. Enforcing the attribution measure is hard because its server hosting is located abroad. So Thai laws cannot enforce (personal interview, 16 December 2014).*

4.4.2.3. Undeterred retaliation

The result of interviewing five personnel from MICT informed that non-severe retaliation becomes one of the barriers to prevent online hate speech, particularly in the case of political conflict. In the past, there were many captives but their punishment was inappropriate with the damages. The arrested did not fear of recidivism, and those who thought of offending did not fear of arrest.

> *… The damages are widespread but punishment is inappropriate. If there is amendment on the sentence; the determent would be more preventative (personal interview, 8 December 2014).*

4.4.2.4. Different political attitudes and misunderstanding in information received

In term of the limitation of preventative measures against online political conflict hate speech, four interviewees stated that the different attitudes and misunderstanding in information received are the main problems in preventative measures.

The root of political conflict is individual political attitude. The individuals are necessary to receive any information, especially from social media, and this prominently impact to their attitudes. By now, people are unlikely to consider the credibility of information, and being easily entrapped which finally are misled in the political attitudes. In addition, there are disseminating and passing on information in social media. So it is speedily widespread, but unknowingly whether the information is valid or not. With such reason, there is violent political expression as well as using hate speech.

> *…social network is wide and speedily forwarding. People are easily entrapped, creating group association with conflict among groups. Therefore, It is necessary to analyze the information and provide public relations for each group (Personal interview, 8 December 2014)*

4.4.3. The National Broadcasting and Telecommunications Commission – NBTC

Data collection from the NBTC personnel showed that the barrier of preventative measures against online hate speech, in the case of political conflict, is the operational disunity in the public sector. The NBTC's authority is just supervision on ISPs to follow their license conditions, not inspecting the contents in the system. Therefore, NBTC has no authority to directly prevent this behaviour, needs other agencies to handle. This proves the disunity of practices and time consuming. Additionally, the undeterred punishment and the disguise in social media are the other barriers, which weaken feasible efficiency against online hate speech.

4.4.3.1. Problems of disunity in the public sector

To efficiently prevent online hate speech, the public sector must progress measures and action taken with unity and short-cut to swiftly arrest and punish wrongdoers. Yet, the interview result from three interviewees stated that one of the limitations is the internal operation within the public sector itself.

The process of preventing against online hate speech demands unity of work and requires coordination to other agencies. As a result, the period of process is time consuming, including gathering evidence. So damages of the offense are immense (personal interview, 22 December 2015). Besides, the problem of the existing authority is met with conflicts within itself. For example, obviously, NBTC has no authority to monitor the content in the internet, even though NBTC is the authorized sector to issue license for ISPs. NBTC is thence unable to take action against websites, social media or the wrongdoers.

> *…The NBTC is authorized just "Warning" measure against telecommunication enterprise, internet, suspending and withdrawing license and excluded the content inside the system. It is not similar with the Broadcasting Affairs, which is empowered with controlling the contents (Personal interview, 24 December 2015).*

4.4.3.2. Undeterred retaliation

Though NBTC is not empowered to directly take action against the wrongdoer, just has the responsibility to punish ISPs declining to follow the condition. Three interviewees commented that the existing retaliation and sentence are undeterred; including law enforcement is yet serious. For example, there still have hate speech in social media, so the posters do not fear any legal actions (personal interview, 22 December 2014).

4.4.3.3. Problem of attribution

Eight interviewees stated that disguise in social media is the main problem about the preventative measure against online hate speech. Social media does not require member registration to disclose real identity, which allows wrongdoing thinkers feel without fear of identifying. Accordingly, they decide to commit offenses (personal interview, 22 December 2014).

With the currently development of technology, mobile phones are possible to access internet. Nevertheless, if sim card have been registered, it is possible to prevent online hate speech. However, this process in Thailand is just on the stage of public relations. Besides, registration demands for cooperation from the enterprise and users as well.

> *….The mobile phone sim card registration is active, but it is tough. It demands cooperation from the enterprises and users too (personal interview, 23 December 2014).*

In conclusion, the most important barriers and limitations which affect the preventative measures against online hate speech, in the case of political conflict, not to efficiently prevent the viral online hate speech in Thailand are the problem of attribution. This weakens the efficiency in investigation. Other barriers proposed by each agency such as inappropriate retaliation and web server hosting are located abroad, both TCSD and MICT agree to such problems. The MICT's key problems are barriers of the political attitudes and misunderstanding in information received and the disunity of internal administration in operation, like NBTC.

4.5. Part V: Recommendations of the remedial approaches against online hate speech: a case of political conflict

The recommendations of remedies against online hate speech in the case of political conflict could be divided by agencies of data collection. Firstly, the informants from TCSD proposed that the related public sector should provide appropriate knowledge in using social media and rightful understanding about politics. Technically, the regulation of attribution should be operated. In term of retaliation, the punishment or sentence should be more severe than the existing ones.

Secondly, data collection from MICT indicates that the agencies should launch campaign on the disadvantage from online hate speech. At the same time, it is necessary to launch public relations on accessing the information received. The improvement of retaliation deserving damages caused by online hate speech, the regulation of users' registration, and the development of personnel skill and budget support, all of these recommendations should be essentially operated.

Finally, the research result of NBTC's informants commented that all of the related agencies should build consciousness, political goodwill and people participation. Still, the improvement of retaliation should be progressed as a result of determent on offenders. Lastly, budget support to the agencies on skill development is necessary as well.

4.5.1. Technology Crime Suppression Division –TCSD

The remedies proposed by TCSD for more efficiency in preventative measures against online hate speech are (1) campaign, public relations, knowledge building about proper use of social media and rightful understanding of politics, (2) regulation the attribution criteria and (3) imposing more severe retaliation/punishment. Details are as below.

4.5.1.1. Campaign, public relations, knowledge building about proper use of social media and rightful understanding of politics

Data collection from TCSD shows all agencies should launch public relations on the damages of online hate speech. The research result also shows that the knowledge building about the Computer Related Crime Act BE 2550 (2007) with other related laws is essential. This results to the realization about the action

against the law and the punishment. However, such behaviour roots from each attitude toward politic, though legal action is not yet reach. Consequently, thoughtful building and resetting political attitudes of people in society, with the objectives of social unity and free from incitement, would be another remedies and coupled with public relations of statute. An informant commented on this point that:

> *…The public sector should launch campaign or point out the statements leading to hatred and directing decision making are the matters of wrong thoughts and attitudes (personal interview, 25 November 2014*).

4.5.1.2. Regulation the attribution criteria

Almost all of the informants (7/8) recommended that related agencies, which have the responsibility of the development of investigation and attribution, should focus on the technological development of attribution such as the technique of trapping the data on gateway system as CCTV system. However, the development of attribution needs to concern about justification, not tort others and subjected to the provisions of the law (personal interview, 27 November 2014). At the same time, web server hosting, located abroad, should be negotiated by the related agencies on the regulation of registration or coordinating on information in order to block the opportunities of offense. An informant commented on this point that:

> *…Thailand is yet to have legal intercept system or checkpoint. Similarly to the deterrence theory concept, If it can be developed it can deter wrongdoers, like CCTV. …including the member registration or measures to bargain the giant companies like Facebook or YouTube and so on (personal interview, 25 November 2014).*

4.5.1.3. Increase retaliation for wrongdoers

All informants suggested that all agencies must impose punishment for fear of punishment. If punishment is enforced, the sentence severity should deserve the offense damages. This affects to others feel fear of punishment and fear of recidivism, due to the fact that people have no fear of punishment at this moment.

> *…Wrongdoing found in internet will exist. Damages still exist as well. Consequently, anyone who uploads any information will sense more responsibility than other common people will. Reasonably, sentence must be more severe than exist (personal interview, 24 November 2014).*

In addition, informants recommended about disagreement on legislation of specific law enactment of online hate speech in the case of political conflict that because Thailand already has emergency laws such as the Security Act and the Emergency Act. Nevertheless, if it is necessary to legislate, it must be legally clear for enforcement with purpose of not being a political tool (personal interview, 25 November 2014).

4.5.2. Ministry of Information and Communication Technology – MICT

The informants from MICT recommended for remedy the measures against online hate speech in the case of political conflict are similar to the TCSD's suggestions (public relations, attribution and retaliation). Nevertheless, there is an additional proposal of the personnel skills development. Yet, most place importance on public relations or campaign. Details are as below:

4.5.2.1. Campaign of knowledge building on proper use of social media and rightful understanding of politics

Seven informants commented that approaches or measures against online hate speech are to launch campaigns on rightful understanding and good attitude of politic. Due to the facts that any information, which is true or not, could be conveniently received from any social media, so people should have deliberately

consider on the information received. However, objectives of distribution the information might entrap to create political schism and incitement for social schism (personal interview, 8 December 2014).

Besides, the informants further recommended that the related agencies should plan projects to create understanding among users about proper use of social media. Any posters on social media have to be prudent about the lawful information. Otherwise, they shall be subject to lawsuit. Not just being lawsuit, but damages affect to other individuals or peace and order in the society. One of the informants stated that:

> *…. Public relations should be launched for people and public sector about currently enforcement of the Computer Related Crime Act and suppression on offenders in this case. It is necessary to use the process of attitude adjustment (personal interview, 16 December 2014)*

4.5.2.2. Online attribution

Five from eight informants recommended that there must be criteria of regulation of attribution in using social media. Nowadays, users are needless to attribution, and this result to the improper statements, improper opinions, and forwarding untrue information with political gains. Conversely, gathering evidence meets hardship for identifying the wrongdoers in social media. Thus, the regulation of attribution about user registration would be very helpful for monitoring, including usefulness on determent the wrongdoers (personal interview, 16 December 2014).

4.5.2.3. Appropriate retaliation

Half of all informants suggested an amendment of increasing the severity of retaliation more than existing. It is obvious that the existing retaliation is undeterred by witnessed of widespread online hate speech. Additionally, severity of the retaliation is inappropriately when compares with the harmful damages. Consequently, an amendment of increasing the severity of punishment for online hate speech should be necessarily proceeded (personal interview, 8 December 2014).

Additionally, two MICT's informants recommended on retaliation that due to online hate speech in the case of political conflict is caused by the difference of political attitude so the retaliation should insert the way of attitude adjustment.

> *…Retaliation enacted is already high, but additional measures like adjustment attitudes should be added (personal interview, 8 December 2014).*

4.5.2.4. Personnel skills development and budget support

Six informants proposed in prevention against online hate speech and other technology crimes that personnel skills development in the agencies should be proceeded. Due to the communication technology is continuously developed, as the communication devices, so the agencies have to focus on the person skills. Similarly, offenses would keep abreast with communication technology development. Accordingly, if the personnel lack the knowledge of technology, the prevention and suppression against online hate speech would be inefficient (interviewed 8 December2014).

Coupled with personnel skills development to acquire knowledge of communication technology, budget support is crucial as well. By reason of the process of skill development is essentially supported by budgets, if not, the prevention and suppression measures against online hate speech would be ineffective.

…Since the criminals of technology crime endlessly develop to find ways of committing crimes, it is necessary for officials to regularly develop knowledge skills. This has to support by budgets to proceed any projects of operations (personal interview, 16 December 2014).

4.5.3. The National Broadcasting and Telecommunications Commission – NBTC

The recommendations and remedies of NBTC against online hate speech in the case of political conflict are relative to MICT's recommendations. The related agencies' projects should proceed on rightful political attitude building, the regulation

of attribution criteria, enacting appropriate retaliation and personnel skills and knowledge development. Details of data collection are as below.

4.5.3.1. Rightful political attitude building

All NBTC's informants proposed that the related agencies should focus on building the rightful political understanding and attitude for people in society. At present, social media is used as the tool to disseminate political messages and various opinions; however, any information in social media is doubtful of truth. All of these are for the political objectives. Accordingly, remedies against online hate speech in the case of political conflict should solve at the root of problem, which is erroneous political attitude, by proceeding the public relations or other methods for political attitude adjustment (personal interview, 24 December 2014).

4.5.3.2. Regulation of attribution criteria

Most of all NBTC's informants stated that Thailand has no criteria to enforce users to truly identify themselves. This weakens the prevention of online hate speech because users believe without fear of lawsuit (personal interview, 22 December 2014). Consequently, to deter people to express such behaviour and for the benefits of the officers to collect evidences; the agencies should set criteria of attribution so as to deter people of committing crime, and for the useful of officers' gathering evidence.

Besides setting attribution criteria and regulations, four NBTC's informants added that systematizing the telephone numbers registration is another measure, which is needed implementation. At present, posting comments, including hate speech, on the social media could be done by using mobile phones, and most use unregistered number to commit various offenses. Accordingly, the related agencies and service providers have to set the criteria to systematize registration with the objectives of determent and investigation. The criteria have to be justified and significantly considering in the individual rights.

> *… Using a screening measure is one of the measures to attribute wrongdoers. It has to be developed, but there must legislate the specific law and authorized the agencies to take responsibility. For example, political conflict is part of creating chaos; otherwise, such measure will be distorted in application (personal interview, 24 December 2014).*

4.5.3.3. Enacting appropriate retaliation

Three informants commented on approaches or measures against online hate speech, particularly in the case of political conflict, that the current retaliation is inefficient to deter the wrongdoers, which include the inappropriate severity of sentence and the convenience of bail process. Accordingly, punishment should be amended by increasing retaliation without clemency. In case of recidivism, the punishment should meet the way of heavier punishment, similar to the narcotics offense, because the damages are more violent than common offenses (personal interview, 23 December 2014).

In addition, one informant recommended on retaliation that not only criminal punishment but to prevent such behaviour, the social sanction as a measure of retaliation should be enacted. This measure results as general and specific deterrence concepts in deterrence theory. The informant presents that:

> *…The criminal punishment must be decisive, with measures of non-imitation as in social sanction. Additionally, in the case of recidivism, its punishment must be heavier without adjudication because its impacts are seriously disastrous (personal interview, 24 December 2014).*

4.5.3.4. Personnel skills and knowledge development

The communication technology is endlessly developed as offenses roll after it. As a result, personnel skills and knowledge in cyber crime are extraordinary indispensable. The NBTC's informants suggested that the agencies give less precedence to personnel knowledge development. Often, countering offenders of

online hate speech and other technology crimes are inefficiency because the personnel skills and knowledge are not good enough to deal with (personal interview, 23 December 2014). Therefore, it is necessary to budget for training to acquire knowledge of communication technology. Moreover, the personnel should understand their duty and responsibility of each related agency to solve the problem at the right point.

> *Nowadays, the executive personnel do not understand the details of the problem, and little technique knowledge of cyber crime. For example, if offense being found, they will not know to whom they must deal with, firstly, and to whom the power and duty are involved with. All of these need skills and knowledge development for the personnel in order to raise efficiency of the operation (personal interview, 22 December 2014).*

There are many remedies of each agency being proposed to efficiently prevent against online hate speech, and disabled to spread such behaviour to societies, specifically knowledge building in using social media and sensibility and positive political attitude. Conversely, punishment or retaliation should be appropriately amended to deserve the damages of offenses. All of these remedies are all agreed by three agencies. Additionally, the attribution measures are proposed by TCSD and MICT. Accordingly, budgeting support for personnel skill and devices development is suggested by NBTC and MICT.

4.6. Conclusions

This Chapter shows the results of data collection from the public sector informants, who responsibility of planning the preventative measure against online hate speech in the case of political conflict (three agencies, TCSD, MICT and NBTC). There are five problems and limitations of preventative measures. Firstly, the problem of attribution is not yet set the criteria on identification the real members and users in social media. Secondly, barrier in gathering evidence when web server hosting is

located abroad, so the agencies are disable to enforce the law. Thirdly, the severity of retaliation or punishment is inappropriate and undeterred the offenders. Fourthly, Different political attitude among people still exists which it is unlikely to thoroughly solve problems. Finally, the disunity or non-systematic process in the agencies to follow various measures is another barrier.

In addition, data collection also shows the recommendations from informants as remedies, improvements, and developments of efficient preventative measures against online hate speech. There are many proposals consisting of public relations campaign on appropriate use of social media and political attitude adjustment, the regulation of attribution, amending severity of retaliation and personnel skills, knowledge and devices development.

CHAPTER V
DISCUSSIONS, CONCLUSIONS AND RECOMMENDATIONS

This research focused on existing preventative measures against online hate speech in case of political conflict**.** Its objectives were 1) to investigate the current preventative measures employed by public sector agencies against online hate speech, particularly in case of political conflict; and 2) to investigate approaches to the amendment and improvement of preventative measures for public sector agencies against online hate speech, particularly in case of political conflict. In this chapter, the researcher draws conclusions from the data collected and raises discussions convergent to the related concepts and theories (in Chapter II). In addition, recommendations for the benefit of future studies will be proposed. However, this study met with several limitations, which might have adversely affected efforts, as below.

1. Since the period of data collection was during an announcement of Martial Law and amendments to related laws for officials, the subject should be investigated further after the situation in the country returns to normalcy and relevant laws have been amended.

2. Data collection for this dissertation was conducted only in the public sector involved in setting preventative measures and behavioural controls. Nevertheless, there are other agencies involved in behavioural controls as well.

3. Data was collected from government personnel only, which might have limitations for examination of damage from such behaviour. In fact, damage might create ill effects on the private sector, while the public sector is neglected.

5.1. Discussions

The discussion will involve collected data convergent to the related concepts and theories, which are based on the research questions.

QUESTION I: What are the current preventative measures employed by public sector agencies against online hate speech, particularly in the case of political conflict?

RESULTS

The cause of viral behaviour for online hate speech in case of political conflict is a problem that Thailand is currently facing. This behaviour damages individuals and groups, causes disorder among people in society and affects national security. Consequently, the public sector agencies involved are required to set measures or plans to prevent such misbehaviour. Efficient measures or plans must be based on related theories. This study employs the Cyber Deterrence Theory, as in Chapter II. It aims to deter cyber crime and pressure offenders to feel duress under the threat of lawsuit rather than gains from their misbehaviour. The Theoretical elements are 1) defense, 2) retaliation and 3) attribution. Accordingly, theoretical measures of the public sector for implementation contain three (3) parts.

Data collection is from three public agencies, inclusive of (1) the Technology Suppression Crime Division (TCSD), (2) the Ministry of Information and Community Technology (MITC) and (3) the National Broadcasting and Telecommunication Commission (NBTC). The results of data collection are based on the Cyber Deterrence Theory, which illustrates each agency's similarity or difference measures taken and what barriers affect the inefficiency of preventative measures against online hate speech in case of political conflict.

PART I: The current preventative measures of TCSD against online hate speech emphasize aggressiveness, public relations, education, knowledge building about laws and information, including proper and appropriate use of the internet. In addition, MITC needs to organize projects and activities through public relations, education of laws, and appropriate use of the internet, specifically on children and youth. For NBTC, its responsibility is different from the other two agencies because it

not only controls the ISPs, but also organizes seminars for them and demands the checking and monitoring of cyber crime. The processes include public relations, education and organizing activities, which educate about related laws and guides proper and appropriate use of the internet.

Examination of the three agencies found that all conducted public relations and campaigns on political attitude, as well as understanding how to use social media. This is because all parties see that the root of misbehaviour comes from users. Prevention and correction must begin there. Besides, it is necessary to reform the political attitudes of people in societies to rightfully understand it and solve political conflict directly. Still, when examining all the approaches of the three agencies, it was found that they were repetitive and each concentrated on its own work, without unity, which might divert disseminated information and allow for misunderstandings or failure in this part. Accordingly, all related agencies should collaborate so that the work proceeds in the same direction, without confusion of information disseminated to people, to raise the efficacy of preventative measures against online hate speech in cases of political conflict. For example, it is suggested an operation center be established, which includes all related agencies and each agency pursuing its missions as assigned by the Director of the Center. As such, work will be done in the same direction and avoid repetition.

PART II: Current retaliation is directly subject to the court, which is empowered to adjudicate punishment. Yet, public sector agencies involved are also important to suppress such misbehaviour because they assist in enforcing laws. If law enforcement is rigid, it turns good to prevent such misbehaviour. The TCSD investigates and arrests offenders. It is also directly responsibility for gathering evidence leading to arrest, which should be collaborated with the private sector. In addition, TCSD prepares watch-lists for individuals at risk for misbehaviour, while MITC provides support with information and evidence for the related agencies in order to investigate and arrest the offenders. This includes warning the users who are at risk of offending. NBTC will support TCSD and MITC with different information. Additionally, the existing power of NBTC includes supervising ISPs to follow their license conditions. If there is any violation, it exercises its administrative power of enforcement.

It is witnessed that the key agency responsible for law enforcement is the police, while MITC and NBTC support TCSD with data and evidence. Still, the current state of law enforcement by the police has been met with inefficiency in the period of gathering evidence because it has to coordinate with many agencies, including MITC and NBTC. This consumes time and delays enforcement. Offenders could think without fear of lawsuits. Therefore, all agencies have to collaborate in order to understand their own roles and duties. For example, MITC must speedily support TCSD upon request. Alternatively, NBTC must make the private sector understand its responsibility to collaborate with the police.

Nevertheless, successfully deterring online hate speech, besides rigid law enforcement, requires retaliation that is critical to deter such misbehaviour. If it is not severe or inappropriate to the damages, offenders and people in society will not learn their lesson or fear punishment. However, punishment and adjudication are not under the responsibility of the three agencies from which this research has collected data. The results merely show that the current methods of enforcement and retaliation, either in severity or retaliation approach, cannot efficiently deter online hate speech. Consequently, the related agencies should amend punishment to better promote deterrence.

PART III: Attribution is the most important preventative measure against online hate speech because the cyber world is virtual and nothing is real. As such, it is necessary to set criteria to attribute users or offenders of cyber crimes. Data from TCSD reveals that it follows the Criminal Procedural Code and the Computer Related Crime Act BE 2550 (2007) to collect the physical and electronic evidence that leads to offender attribution. MITC attributes offenders through the Computer Related Crime Act BE 2550 (2007) in order to seek data and evidence, which it then hands on to interrogation officers or agencies involved in further investigation and arrest. NBTC reiterates ISPs to support with data and cooperation from the public sector. In addition, NBTC is responsible for systematizing the registration of mobile phone users. Telecommunications enterprises have to store the personal data of users for the benefit of law enforcement, if officers need data or evidence.

Considering attribution from the three agencies, it is found that current practices are only enacted from the Criminal Procedural Code and the Computer

Related Crime Act BE 2550 (2007), such as the enactment that ISPs must store computer traffic data for 180 days and the authority to request data for investigation of IP Addresses to locate servers. However, many ways remain available to circumvent official inspection, which prolongs pursuance, including without prudent criteria to attribute users. It allows viral online hate speech to continue at present. The three agencies need to develop technology to check and intercept those that flee in order to keep pace with ever-changing offenses. For example, it is necessary to install a gateway, which is technology that can check computer data within the system and use it in storing computer data and so on. Still, the timeframe for storing computer traffic data in the servers under the Computer Related Crime Act BE 2550 (2007) should be expanded. Gathering evidence consumes time and it might be beyond the timeframe, which is imperfect for a lawsuit. Such a period is not under the responsibility of the three agencies where the researcher collected data, but it must be the responsibility of the legislative governmental body to amend the law.

Thailand imposes preventative measures against online hate speech in the case of political conflict. To a certain extent, it can control misbehaviour. However, it remains to be found endlessly to this day. This point shows that the measures imposed by each agency have still been met with problems and flaws. It is necessary to propose points of improvement and development to raise the efficiency of deterrence.

QUESTION II: What are the approaches to amendment and improvement of preventative measures for public sector agencies against online hate speech, particularly in the case of political conflict?

RESULTS

The preventative measures against online hate speech enforced today by the public sector are found with limitations and affect working inefficiency as targeted. The results show that problems include gathering evidence against offenders, barriers of attribution, and inappropriate retaliation, as well as different political attitudes, the absence of knowledge and the ability of personnel and devices. This research conceptual framework has three parts of the cyber deterrence theory, which

lead to solving and improving the preventative measures against online hate speech in case of political conflict, which is the objective of this research.

The data collection shows that each agency proposes their own approaches to raise the efficiency of their preventative measures against online hate speech in case of political conflict while constructively reducing the viral spread of misbehaviour. This could be concluded in four ways, i.e. (1) campaign, public relations, educating for the proper use of social media and understanding of politics, (2) fixing attribution criteria, (3) imposing appropriate retaliation/punishment, and (4) developing personnel skills and improving device quality. The data shows their proposals as follows:

1). Campaign, public relations, educating for proper use of social media and understanding of politics

There are two methods proposed for this matter.

1.1. The political adjustment method – Political conflict is the root of online hate speech and wrong political attitudes without using discretion to listen completely to information, which results in misunderstanding. It affects segregation, seeing opposition as an enemy and ends in social schism. It leads to assault and property damage, even though all have the same objective: the growth of the nation. To constructively reform political attitude, it is necessary to build understanding among people in society to use discretion in listening to the news and other forms of public information. Rationally, communication technology today easily disseminates information to people more swiftly. Some receive it without knowing the source or knowing whether it is true or false, reliable or not. It is necessary then to organize public relations campaigns for people in societies to use their discretion when consuming news and information, so that they understand the national administration. The recommendations correspond with the study of Ms. Chanansara Orranop Na Ayudhya (Thai Media Policy Center: Faculty of Communication Arts, Chulalongkorn University, 2013), who commented that the related agencies should encourage media receivers to know the media and develop the personnel in the media profession, as well as react to hate speech with non-violence according to social norms.

1.2. Public relations and education of laws related to the topic is another method to be taken because disseminating news and information

without considering the content might make those who forward such information subject to lawsuit. Not just that, the impact is also against social security because it creates political prejudice and provokes people in society to hold uninformed political views. These lead to deviation and crime. Therefore, it is necessary to conduct public relations and educate people about the laws related to cyber crime and the corresponding punishment or retaliation, especially the Computer Related Crime Act BE 2550 (2007). Additionally, they should realize that which action is subject to legal violations and the punishment if done. This corresponds with the study of Ms. Chanansara Orranop Na Ayudhya (Thai Media Policy Center: Faculty of Communication Arts, Chulalongkorn University, 2013), where there should be knowledge creation and understanding in using social media for people in society in order to be conscious of the punishment arising from such deeds.

Examining the methods proposed in the form of campaigns and public relations on the political attitude and the rightful use of social media; the researcher suggests that these measures should couple on the operation because using online hate speech on political conflict can be divided into two elements, improper use of social media and misunderstandin political attitudes. Both elements can be solved by the above methods. Otherwise, preventing such misbehaviour is unsustainable because it cannot solve the root of misbehaviour. At present, the public sector implements both methods in either organizing activities or conducting public relations. Nonetheless, what has been found is that most people still fail to understand the political attitude, with an absence of discretion in consuming news and information, and being without conscious of the consequences for misuse of social media in politics. Therefore, all agencies involved should revise their practices and consider their past consequences as to whether there are any limitations to improve their efficiency.

2) Fixing attribution criteria

Remedies for improving preventative measures against online hate speech in the case of political conflict include three methods of attribution.

2.1. Technology development of capability to enable attribution or locate users and check their usage history. At present, Thailand has not

yet organized storage in the internet, as a result, the checking of data is delayed. It is proposed that the development of computer storage, such as installing a gateway with the objective of checking and intercepting damaging data in the computer with an immediate alert, or storing data in case of necessity for speedy checks, should be done. Banks (2010) and Cohen-Almagor (2009) support this method, commenting that violence from online hate speech can be alleviated if the agencies enforce laws coupled with measures of technological supervision, such as checking the data used in the system and locating the access points of users.

2.2. Setting attribution criteria is required because there is none in Thailand. This let people to offend or commit crime because investigation for arrest is impossible or tough. As such, the related agencies should set attribution criteria, which might be in the form of laws, regulations or rules that online users must abide by every time. At present, some social media platforms demand such attribution, such as siambrandname, which is an e-trading platform. The distributor demands the authenticity of any person logging on, such as ID card number or bank account number, to prevent cheating and fraud in e-trading.

2.3. Mobile phone pre-paid registration should be done, because the registration on pre-paid system and users' data storages are unclear. Consequently, there are many offenses committed by pre-paid mobile phones, which are disabled to check the users on those numbers. Pursuing offenders is difficult. Therefore, the agencies must set constructive criteria for storing the data of pre-paid users for clear attribution. This is a deterrent measure against offenders because they can be checked and identified.

From the proposal of remedies against online hate speech in the case of political conflict by attribution, the researcher comments that the agencies involved should preferably set attribution criteria and implement mobile phone registration for the pre-paid system. Such methods are not complicated and do not infringe on users' rights. This stage can be completed immediately. Thailand has imposed pre-paid phone registration since July 2015. If phones are not registered, the telephone number will be impeded. On the other hand, data-storage technology and locating users is ideal to prevent online hate speech and other cyber crimes. However, these methods demand a large amount of funding and efficacious personnel. In this regard, Thailand has met

some limitations. Additionally, these methods could be evidently enacted or regulated. These might violate freedom of speech for people in society and offenders might use them in the wrong way. The criteria have to be clearly set on authority and responsibility. At present, the related agencies are considering adoption of such approaches because many issues have to be reexamined, such as investment budget, laws, rules, regulations and freedom of speech for individuals.

3) Imposing appropriate retaliation/punishment

Imposing appropriate retaliation/punishment is another measure proposed for improvement and amendment against online hate speech in case of political conflict. Each agency has proposed various approaches, which can be concluded into two ways as follows.

3.1. Increasing the severity of retaliation because the current situation shows that online hate speech is viral with no signs of inclination. It shows the inefficiency of retaliation, which cannot deter people to stop such misbehaviour, even if it results in devastating damage to individuals and society. Hence, making retaliation effectively reduce such misbehaviour means the retaliation should be more severe and commensurate with the damage done. Alternatively, the heavier punishment for recidivism may be used (as with narcotics cases). People in society may fear the punishment if being arrested, and to deter them from committing such offenses.

3.2. To add punishment deserving of the nature and intention of offenses, online hate speech in the case of political conflict is aimed at discrediting or diminishing accountability of the victim. Consequently, retaliation might be reset to compel real damages. Besides imprisonment and fine, it could include such punishment as social sanctions by public services or imposition of volunteer work in society, such as in the case of drunk drivers. Additionally, retaliation by retuning the attitude of the offenders is another approach proposed because most offenses cause by misunderstandings of the political attitude. Therefore, retaliation should be focused on the cause of the offense: political attitude. This could be added into a part of retaliation section.

For appropriate retaliation, the researcher comments that the most efficient measure to prevent and deter misbehaviour is to enforce with severe punishment. In the past, there were many cases which the offenders were recidivism. This demonstrates that they did not learn their lesson from the past. Therefore, it is necessary to enforce progressively severe retaliation. This point needs cooperation from the courts where have the responsibility of adjudication for more severe punishment. Still, the heavier punishment may be another approach that might solve this problem. In the past, this measure could not efficiently deter such misbehaviour. For instance, the charge for a drunk-driving case sentenced to conduct social services still resulted in recidivism. In the case of law enactment or punishment stipulations for online hate speech in case of political conflict for specific purposes, the results of a study showed that it was not supported because such law would be distorted if enacted for use and Thailand already has a Provisional Law empowering personnel.

4) Developing personnel skills and improving device quality

The action taken by the public sector at present is hindered by budgeting to develop personnel potential and improve devices to meet the update of communication technology. The research results propose remedies that the agencies involved should budget for developing personnel potential and frontlines to acquire continuous knowledge of present technology as well as improve working devices because technology development is never stopped. If the agencies involved disregard this part, operations of prevention against online hate speech and attribution will be weakened, meaning it cannot prevent viral misbehaviour.

5.2. Conclusions

This study investigated existing preventative measures against online hate speech in the case of political conflict. It also looked at whether such approaches, directions and actions have been effective because at present, viral misbehaviour is rampant despite the various agencies imposing preventative actions. Such acts affect social disunity and damage national security. Therefore, it is necessary to study and spotlight the problems, limitations and barriers for personnel to take appropriate

action. This will lead to the solutions and improvement of various measures so that the preventative measures will reach greater efficiency. In this study, the researcher paid importance to the public sector, which is involved directly in designing strategies, plans, measures and implementation.

No research other than this one has been found to focus on the study on the public sector in Thailand on prevention of online hate speech in the case of political conflict. However, there are other researches that investigated the supervision of bad content that might create hatred online. Such researches never specifically studied the public sector for measures in the case of political conflict. Several such studies include the work of Asst. Prof. Pijittra Zukamoto (Sunai Phasuk, 2014), the study of Mr. Arthip Jittakrit (2012) and the research of Ms. Chanansara Orranop Na Ayudhya (Thai Media Policy Center: Faculty of Communication Arts, Chulalongkorn University, 2013). Some studies are related to online hate speech, but focused on the behaviour of speakers such as “Supervision of Content Disseminating Hatred” (Thai Media Policy Center: Faculty of Communication Arts, Chulalongkorn University, 2013). Another example is “Youth Perception on Cyber Bullying” (Natharatch Samoh, 2013). Therefore, this study can be applied in conjunction with those researches or other related researches to be guides for developing more potential measures against online hate speech and the benefit of suppressing other offenses in social media as well.

The study reveals that existing preventative measures against online hate speech in the case of political conflict have been met with some problems and limitations disabling the ability to prevent such misbehaviour. There are problems with gathering evidence, attribution, retaliation and disintegration of any agencies. All these problems directly weaken the efficiency of the preventative measures against viral misbehaviour. Accordingly, there should be amendments to prevent viral misbehaviour. Recommendations from the study for the agencies involved to prevent and control viral misbehaviour in case of political conflict include setting attribution criteria, political attitude adjustment, and campaigning for appropriate use of social media, as well as amendment of more appropriate retaliation approaches, personnel skills and devices development.

5.3. Findings

After analysis of the research results, it is found that the recommendations could be applied with the conceptual framework, which would enable application for related researches in preventing against online hate speech in case of political conflict. The conceptual framework is shown below.

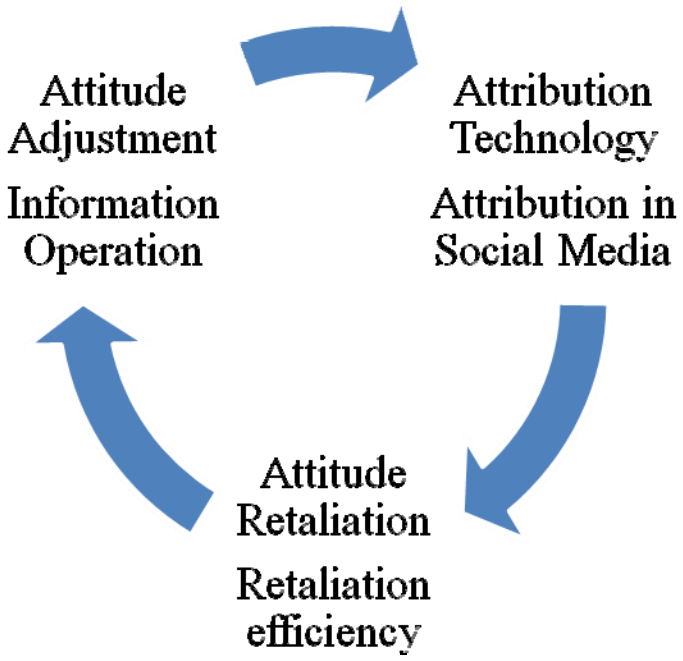

Figure 5.1 Conceptual framework gained from the study on preventative measures against online hate speech: a case study of political conflict

In this conceptual framework, it could be explained that prevention against online hate speech in case of political conflict for the public sector should begin with political attitude adjustment for common people and targeted individuals (politicians, hard-cores, sentenced persons). The information operation might be public relations in the form of knowledge building and understanding creation on consuming information and media.

At the same time, there must be technology development for attribution of online users to enable detection of offenders or persons with behaviour at risk of offending to further impose lawsuits. Using social media should have primary criteria

for online users, making it necessary to attribute their authenticity before use. This will deter persons to offend and the officers could be used to check for the wrongdoer's identity to be arrested for lawsuit.

Upon finding an offense and arresting the offender(s), they should be subject to efficient retaliation. This does not mean severe retaliation, but retaliation that is deserving of the damage so that offenders will learn their lesson and avoid recidivism. It may also deter others from committing such offenses. Furthermore, retaliation for offenders caused by political conflict will not only be subject to common punishment, but must also involve attending to attitude adjustment or retuning. This is because the root of their misbehaviour often cause by political misunderstanding.

The outcomes of retaliation would prevent such misbehaviour in the future because it is a deterrent to anyone. This also creates political understanding for people which is objective of this measure to prevent online hate speech in case of political conflict.

5.4. Recommendations

The objectives of this research were to investigate the current preventative measures of public sector agencies against online hate speech in the case of political conflict with respect to the barriers or limitations that lead to such misbehaviour and allow it to happen in Thailand. This research will lead to approaches for amendment and improvement of greater efficiency in the preventative measures. The results are presented in Chapter IV, where the existing measures are applied, including the problems and limitations restricting the operation of the public sector agencies involved in preventing and suppressing online hate speech.

From the investigation to improve and amend the preventative measures of public sector agencies against online hate speech in case of political conflict, the researcher provides recommendations for such measures in Thailand in various aspects, as follows:

1) Launching campaigns, education of knowledge on online social media and correct understanding of politics

2) Setting attribution criteria for online users

3) Improving appropriate retaliation

4) Developing personnel potential and budget support

5.4.1. Launching campaigns, education of knowledge on social media and correct understanding of politics

With the recent political conflict, social media has been found to be used as a tool to disseminate political messages and post opinions concerning any information uploaded onto the internet. Some are true, while others are false or have been modified or remade when they involve political objectives.

Using social media is liable to affect the individual rights of others if untrue information is uploaded on the internet. The damages do not only affect individuals, but also creates a schism among people in society because of incorrect or misinformed political attitudes. Such acts are counter to the Computer Related Crime Act BE 2550 (2007) or the Criminal Code depending on the offense. Therefore, adjusting or retuning the political attitude of people in society and the proper use of social media addresses the root of such misbehaviour. Recommendations for launching campaigns, education of knowledge on social media and correct understanding of politics are as follows:

1) From the study of public sector agencies involved in preventing online hate speech in case of political conflict, it has been found that they should promote public relations to allow people to see the damages caused against society by using online hate speech. At the same time, properly using social media and educating the public about the Computer Related Crime Act BE 2550 (2007) and other related laws allow people to understand that any acts violating laws would be subject to punishment or retaliation.

2) Misbehaving as such causes by the political attitude of individuals and misunderstanding that anyone who has differently views is on the opposite side. This leads to the rejection of others' opinions and the spread of schism or segregation in society. Therefore, it is necessary to establish correct political understanding for people in society. It needs to avail from the national level down to family institutions, as well as in educational institutions. In addition, it requires public relations for people

in society to use discretion in consuming information because the absence of discretion regarding information leads to misinformed political attitude.

5.4.2. Setting attribution criteria for online users

Using online hate speech in case of political conflict is a problem that Thailand is facing because users of social media have virtually unlimited access to information and can virally broadcast it at will. Conflicts among people in societies are the consequences. In the past, the public sector consistently prevented and suppressed it, but such misbehaviour still exists because there is no evidence to investigate and identify offenders.

Online attribution is a critical measure to prevent cyber crime, but in the past Thailand had no technical or legal measures to investigate and attribute offenders quickly, often being time-consuming and resulting in an inability to attribute them. It allows offenders using this opportunity to offend without fear of punishment. Accordingly, recommendations to set attribution criteria are as follows:

1) The study results reveal that the agencies involved with the investigation system or online attribution in the cyber world should develop technical and legal attribution for online offenses. Legally, it demands the regulation and obligation of identifying users' identity for ISPs or social media providers. Technically, it may be based on the CCTV principle, which can retrieve information by intercepting it at the gateway. However, it is necessary to consider the legality and must not violate others' rights while remaining subject to the statute. Conversely, ISPs or providers outside Thailand, where Thai law cannot be enforced, should involve bargaining by the agencies with them on registration systems or the coordination of information.

2) Systematizing the registration for telephone numbers is another measure to be done because mobile phones can easily access the internet and forward online hate speech with non-registered mobile phones. Therefore, the agencies and service providers involved should set criteria to systematize telephone number registration. The objectives are to deter and for the benefit of investigating to arrest offenders.

5.4.3. Improving appropriate retaliation

Punishment on offenders is another measure to deter people from offense, which bases on the Deterrence Theory concept. The severity of retaliation must be proportionate with the damages. Otherwise, it cannot deter offenders, but rather encourages people to offend. Actions in the cyber world remain forever and victims suffer likewise. Therefore, users must be responsible for their actions.

The study results in this matter show that the current retaliation regime cannot deter online hate speech. Retaliation should be increased based on the severity of offenses, including adding social sanctions and the heavier punishment measure to prevent imitation. In addition, the addition of attitude adjustment or retuning of political understanding in the punishment would be another measure to solve online hate speech in case of political conflict.

5.4.4. Developing personnel potential and budget support

Preventing online hate speech requires efficacious personnel and modern devices because social media links to the internet, which is always developing. If personnel own knowledge and abilities and device techonology are incompatible with the communication technology, operations cannot reach ultimate efficiency as expected, which also affects deterrence. Therefore, the recommendation is as follows:

The recommendation from this study concerns about the personal skills and devices development. The public and private sectors involved have to consistently develop their personnel to be equipped with the skills, knowledge and abilities necessary to pursue communication technology and respond immediately to the needs of society. Such actions should be coupled with the devices and equipment to support their operations.

Recommendations for further studies

1) Studies should be conducted with the group affected by online hate speech in the case of political conflict to identify further preventative remedies.

2) Studies should be conducted with the entire justice system, including prosecutors, the courts and department of corrections, to collect complete data for the justice system.

3) The recommendations of this study should be investigated in more detail concerning the results of whether and to what extent online hate speech affects people in society.

BIBLIOGRAPHY

Aghaei, S., Nematbakhsh, M. and Farsani. H. (2012). Evolution of the World Wide Web: From Web 1.0 to Web 4.0. *International Journal of Web & Semantic Technology, 3*(1), 1-10.

Ajchawanantakul, Sarunee. (2011). *Compilation of "The Truth from Virtual World, Part 1-6.*

Al Jazeera. (2014, 21 January). *Thailand declares Bangkok state of emergency.* Al Jazeera. Retrieved March 17, 2014, from http://www.aljazeera.com/news/asia-pacific/2014/01/thailand-declares-state-emergency-201412113424152787O.html

Anti-Defamation League. (2012). *Hate Crime Laws – The ADL Approach*. New York: Anti-Defamation League.

Australian Human Rights Commission. (2012). *Know your rights: Racial discrimination*. Australian Human Rights Commission.

Bailey, J. (2006). The inter-related roles of citizens, industry and government in combating Internet hate. *Canadian Issues, Spring,* 56-59.

Bandura, A. (1977). *Social Learning Theory*. Englewood Cliffs: Prentice Hall.

Bangkokbiznew. (2013, 2December). *Behind Riots "Ram.U"* Retrieved on September 7, 2014 from http://www.bangkokbiznews.com/home/detail/politics/politics/20131202/547109/.html

Banks, J. (2010). Regulating hate speech online. *International Review of Law, Computers & Techonology*, *24*(3), 233-239.

Banks, J. (2011). European Regulation of Cross-Border in Cyberspace: The Limits of Legislation. *European Journal of Crime, Criminal Law & Criminal Justice, 19*(1), 1-13.

Beccaria, C. (1968). Crime and punishment: An economic approach. *Journal of Political Economy, 76*(2), 169-217.

Boyd, D. (2007). Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life. In Buckingham, D. (Ed.), *MacArthur Foundation Series on Digital Learning – Youth, Identity and Digital Media Volume* (pp. 119-142). Cambridge: MIT Press.

Brian, McNair. (2003). *An Introduction to Political Communication.* London: Routledge.

Briar, S. and Piliavin, I. (1965). Delinquency: situational inducement and commitment to conformity. *Social Problems, 13,* 35-45.

Bursik, R. (1988). Social Disorganization and Theories of Crime and Delinquency: Problems and Prospects. *Criminology, 26*(4), 519-552.

Chaisukkosol, Charnchai. (2008). *Mystery of Information: political violence and non-violence in 21st century of Thailand.* Retrieved on March 17,.2014 from

Chaisukkosol, Charnchai. (2011).*Hate Speech and Dangerous Data: Political Retaliation Alternatives.* Retrieved on March 17,.2014 from http://chaisuk.files.wordpress.com/2 0 1 1 / 0 6 / hate-speech-alternative-respond-full-report-may0311.pdf

Chorwichian, Wowpailin. (2011). 7 Phenomena of Social Network in Asian. *Asean Hightlight 2011, 58-61*.

CNN. (2013). *Sheriff: Taunting post leads to arrests in Rebecca Sedwick bullying death.* CNN. Retrieved April 3, 2014, from http://edition.cnn.com/2013/10/15/justice/rebecca-sedwick-bullying-death-arrests/

Cohen-Almagor, R. (2009) Symposium: Comparative Law of Hate Speech: Regulating Hate and Racial Speech in Israel, *Cardozo Journal of International & Comparative Law, 17*(3), 405-415.

Cullifo, F., Cardash, S. and Salmoiraghi, G. (2012). A Blueprint for Cyber Deterrence: Building Stability Through Strenght. *Military and Strategic Affairs, 4*(3).

Dahlberg, L. (1998). Cyberspace and the Public Sphere: Exploring the Democratic of the Net. *Convergence*, 4, 70-84.

ECHR. (2013). Hate speech. *European Court of Human Rights*, Press Unit July 2013.

Eid, M. and Ward, S. (2009). Editorial: Ethics, new media, and social networks. *Global Media Journal – Canadian Edition, 2*(1), 1-4.

Ellison, N., Steinfield, C. and Lampe, C. (2007). The Benefits of Facebook, Friends, Social Capital and College Students' Use of Online Social Network Sites. *Journal of Computer-Mediated Communication*, *12*(4), 1143-1168.

FBI. (2013). *FBI Releases 2012 Hate Crime Statistics*. U.S. Department of Justice.

FBI. (2013, 17 May). Pennsylvania Man Sentenced for Cyberstalking and Child Pornography Offenses. *FBI*. Retrieved April 3, 2014, from http://www.fbi.gov/detroit/press-releases/2013/pennsylvania-man-sentenced-for-cyberstalking-and-child-pornography-offenses.

Foundation of Media Education. (2012). *Study Result of Hate Speech in Websites and Political Satellite TV (12-18 June 2012).* from http://www.thairath.co.th/content/edu/397816

Gattuso, J., Harris, B., Mattey, C., Nila, C. and Sloan, T. (1993). *Role of Telecommunications in Hate Crimes, Report to Congress*. U.S. Department of Commerce.

Geers, K. (2010). *The Challenge of Cyber Attack Deterrence*. Computer Law & Security Review 26. Elsevier.

Goodman, W. (2010) Cyber Deterrence: Tougher in Theory than in Practice. *Strategic Studies Quarterly*, *4*(3), 103.

Goodman, W. (2010). *Cyber Deterrence Tougher in Theory than in Practice?* Strategic studies Quarterly.

Gordon, R. (2014). Privacy, Security and the Cyber Dilemma: An Examination of New Zealand's Response to the Rising Threat of Cyber-attack.

Guitton, C. (2012). Criminals and cyber attacks: the missing link between attribution and deterrence. *International Journal of Cyber Criminology*. London: Kings College.

Haley, C. (2013). A Theory of Cyber Deterrence. *Georgetown Journal of International Affairs*.

Henry, J. (2009). Beyond free speech: novel approach to hate on the Internet in the United States. *Information & Communications Technology Law*, *18*(2), 235-251.

Hirschi, T. (1969). *Causes of Delinquency*. CA: University of California Press.

Home Office. (2013). *An Overview of Hate Crime in England and Wales*. London: Home Office. http://chaisuk.files.wordpress.com/2008/10/mystery-of-new-media-tech-vnv.pdf

Hudson, D. (2002). *Hate speech online*. First Amendment Center. Retrieved http://www.firstamendmentcenter.org/hate-speech-online

Inglehart, R. and Catterberg, G. (2002). Trends in political action: The developmental trend and the post-honeymoon decline. *International Journal of Comparative Justice*, 43(3-5), 300-316.

Intajak, Pattamai. (2008). *Political Communication in PAD Rally 2008.* Chiangmai: Payap University

Jaishankar K., (2008). Space Transition Theory of Cyber Crimes. In Schmallager, F., & Pittaro, M. (Eds.), *Crimes of the Internet* (pp.283-301). Upper Saddle River, NJ: Prentice Hall.

Jampokkhao, Wicharn. (2011). *PAD Political Communication: a case study of political rally after election of December 23, 2007.* Dissertation: Krek University , Bangkok.

Jansen, E. (2012). Cyber Deterrence. *Emory International Law Review, 26*, 773-824.

Jittaruek, Aarthip. (2012, 19 November). *Hate Speech: basic understanding, and point of consideration for suppression*. Retrieved on September 7, 2014 from http://www.prachatai.com/journal/2012/11/43747

Kaewthep, Kanjana. (1998). *Communication Arts Studies: Critical Theory.* Bangkok: Chulalongkorn University Printing.

Kelley, T. (1996). A critique of social bonding and control theory of delinquency using the principles of Psychology of Mind. *Adolescence, 31*(122), 321–337.

Kennedy, K. (1983). A Critical Appraisal Criminal Deterrence Theory. *Dickinson Law Review, 88*, 1-13.

Ketboonchu Meid, Kullada. (2009). *Political Conflict in Thailand: Cross over the Internal Dynamism.* Bangkok: Foundation of Sip Si Tula.

Khaosod English. (2013, 24 December). *Khaosod English's Note On Name Translation of Anti-Govt Leadership.* Khaosod. Retrieved March 17, 2014,

from http://www.khaosod.co.th/en/view_newsonline.php?newsid=TVRNNE56ZzNNalUzTlE9PQ==&catid=03

King Prajadhipok's Institute. (2012). *Reports of national Reconciliation*. Nonthaburi: King Prajadhipok's Institute.

Kornhauser, R. (1978). *Social Sources of Delinquency: An appraisal of analytic models*. Chicago: University of Chicago Press.

Kramer, F. (2009). Policy Recommendations for a Strategic Framework. In Kramer, F. et al. (Ed.), *Cyberpower and National Security* (pp. 15). Dulles: National Defense University and Potomac Books.

Kugler, R. (2009). Deterrence of Cyber Attacks. In Kramer, F. et al. (Ed.), *Cyberpower and National Security* (pp. 309). Dulles: National Defense University and Potomac Books.

Kulnarong, Nattakarn. (2007). *Political Communication on Internet during Anti-Thaksin*. Master of Political Science: Chiangmai University, Chiangmai.

Lenhart, A., Lewis, O. and Rainie, L. (2001). *Teenage Life Online.* Washington D.C.: Pew Internet and American Life Project.

Lenhart, A., Purcell, K., Smith, A. and Zickuhr, K. (2010). *Social Media and Young Adults*. Washington D.C.: Pew Research Center's Internet and American Life Project.

Lewis, D. and Salem, G. (1981). Community Crime Prevention: An Analysis of a Developing Strategy. *Crime and Delinquency, 27*(3), 405-421.

Lewis, S. and Lewis, D. (2011). Digitalizing Crime Prevention Theories: How Technology Affects Victims and Offender Behaviour. *International Journal of Criminology and Sociology Theory, 4*(2), 756-769.

Lhaowicha, Nanthawitch and Taenrattanakul, Siroj. (2012). Politics on Satellite TV and the Thai Social Conflict. *Executive Journal, 32(4), 67-73.*

Lhaowicha, Nanthawitch. (2012). Social Media Online and Thai Political Communication. *Executive Journal, 32(1), 105-109.*

Matichon ONLINE. (2013. 9 December). *Foreign Media Bell Yingluk Government Dissolves Parliament and Return Power to People.* Matichon. Retrieved

on March 17, 2014 from http://www.matichon.co.th/news_detail.php?newsid=1386559954

Mazerolle, L., Wickes, R. and McBroom, J. (2010). Community Variations in Violence: The Role of Social Ties and Collective Efficacy in Comparative Context. *Journal of Research in Crime and Delinquency*, *47*(1), 3-30.

McCargo, D. (2008). Thailand: State of Anxiety. *Southeast Asian Affairs 2008*. 332-356.

McNair, B. (2003). *An Introduction to Political Communication.* London: Routledge.

Mendel, T. (2010). *Hate Speech Rules Under International Law*. Centre for Law and Democracy.

Merton, R. (1938). Social structure and anomie. *American Sociological Review, 3,* 672–682.

Miller R, Lammas N. (2010). Social media and its implications for viral marketing. *Asia Pacific Public Relations, 11*(1), 1–9.

Miniwatts Marketing Group (n.d.). *Internet Usage and 2015 Population in North America*. Retrieved December 16, 2015, from http://www.internetworldstats.com/stats14.htm.

Morenoff, J., Sampson, R. and Raudenbush, S. (2001). Neighborhood Inequality, Collective Efficacy and the Spatial Dynamics of Urban Violence. *Criminology, 39*(3), 517-558.

Morgan, P, (2010). Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm.

Nagin, D. (1998). Criminal Deterrence Research at the Outset of the Twenty-First Century. *Crime and Justice, 23,* 1-42.

Nagin, D. (2011). Deterrence – Scaring Offenders Straight. In Cullen, F. and Jonson, C. (Eds.) *Correctional theory: Context and Consequences*. Thousand Oaks: Sage Publication.

Nagin, D., Cullen, F. and Jonson, C. (2009). Imprisonment and Re-Offending. In Tonry, M. (Ed.) *Crime and Justice: A Review of Research, 38,* Chicago: University of Chicago Press.

Nanuam, Wassana. (2008). *Secrecy, Illusion, Camouflage: Sand Castle Coup*. (3rd edition). Bangkok: Matichon.

Newman, N. (2009). *The rise of social and its impact on mainstream journalism* (working paper). Oxford: Reuters Institute for the Study of Journalism.

Newman, N., Dutton, W. and Blank, G. (2012). Social Media in the Changing Ecology of News: The Fourth and Fifth Estates in Britain. *International Journal of Internet Science, 7*(1), 6-22.

Ngo, F. and Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology, 5*(1), 773-793.

Nye, I. (1958). *Family Relationships and Delinquent Behaviour*. New York: John Wiley.

Office of Electronics Business Development. (2013). Report of a Survey on the Behavior of Internet Users in Thailand 2013. Bangkok: ETDA

Office of the Secretary of the House of Parliament. (2011). *Political Participation of People.* Bangkok: Office of the Secretary of the House of Parliament.

Phasuk, Sunai. (2014, 3 May). *'Sunai Phasuk' Points Out Anxious Hate Speech of Thailand Seeing People as Dregs.* Retrieved on September 7, 2014. from http://www.prachatai.com/journal/2014/05/52991

Phokha, Thaweesak and Khathanya, Ratiya. (2012). *Social Media: Problem of Opportunity of the Thai Society: problem do defining and misunderstanding free speech and hate speech.* Bangkok: Thammasart University.

Pramote, Seni.(2005). *Bio-scriptions*. Bangkok: Democrat Party

Pratt, T. and Cullen, F. (2005). Assessing macro-level predictors and theories of crime: A meta-analysis. In Tonry, M. (Ed.), *Crime and Justice: A Review of Research, 32,* Chicago: University of Chicago Press.

Putnam, R. (2000). *Bowling alone: The collapse and revival of American community*. New York: Simon and Schuster.

Ramsutr, Pirongrorng, Chainant, Pimolwan, Orranop Na Ayudya, Chanansara and Benjarongkij, Yubol. (2010). *Organizational roles/Association of Media Profession and Perspective/ Ideas on Media Reforms.* Bangkok: Chulalongkorn University.

Reckless, W. (1967). *The Crime Problem*. New York: Appleton-Century-Crofts.

Robert, A. and Nagin, D. (2011). General Deterrence: A Review of Recent Evidence. In Wilson, J. and Petersilia, J. (Eds.), *Crime and Public Policy* (pp. 411 – 436). New York: Oxford University Press.

Samoh, N., Boonmongkon, P., Samakkeekarom, R., Ojanen, T. and Guadamuz, T. (2014). Youth Perceptions on Cyberbullying. *Journal of Behavioral Science for Development*, 6(1), 351-364.

Samoh, Nattaratch. (2013). *Youth Perception on Cyber Space Bully*. Master of Arts: Mahidol University, Bangkok.

Sampson, R. (2002). Transcending Tradition: New Directions in Community Research, Chicago Style. *Criminology, 40*(2), 213-230.

Sampson, R., Raudenbush, S. and Earls, F. (1997). Neighborhoods and Violent Crime: A Multilevel Study of Collective Efficacy. *Science, 277*(5328), 918-924.

Sheriff, S. (2008). *Cyber-Bullying: Issues and solutions for the school, the classroom and the home.* Oxon, United Kingdom: Routledge.

Smith, A. (2010). *Americans and their gadgets*. Washington D.C.: Pew Research Center's Internet and American Life Project.

Sorat, Lerphop, Ngarmsanit, Samarn, Sriheran, Boonrueng and Jitlao-arporn, Charnchai. (2011). Roles of Mass Media and the Thai Political Participation. *Graduate Studies Journal*, 5, 117-129.

Stafford, M. and Warr, M. (1993). A Reconceptualization of General and Specific Deterrence. *Journal of Research in Crime and Delinquency, 30*,123–35.

Suksa-nguan, Nattaya. (2014). *Media Reforms for Dissemination Control of Hate Speech.* Office of Academics: Office of the Parliament Secretary.

Suriyawongkul, Arthit. (2012). *Politic on Facebook: culture-politics of Thai social media 2010-2012.* Master of Social Science and Humanity: Thammasart University. Bangkok.

Sutherland, E. (1939). *Principles of criminology*. Chicago: University of ChicagoPress.

Suwannamongkol, Pathan.(2006). Thai Government in King Prajadhipok's Institute, *Politics and Administration of Thailand for 60the Anniversary of His Majesty Coronation* (189-216). Nonthaburi: King Prajadhipok's Institute,

Thai Media Policy Center, Faculty of Communication Arts: Chulalongkorn University. (2013, 26 July). Disclose Research Work on Hate Speech Online –Multileveled Definition, Monitor Must See Objectives. Retrieved on September 7, 2014 from https://thainetizen.org/2013/07/online-hate-speech-in-thailand-research-chula

Thairath ONLINE. (2014). *Department of Mental Health Worrying Thais Familiarize with Violent Speech*. Thairath. Retrieved on March 17, 2014

Thairath ONLINE. (2014, 28 February.). Counting Bomb Blast of M.79 Atmosphere of Mob "PAD-RedShirt-PDRC. Retrieved on September 7, 2014 from http://www.thairath.co.th/content/406596

Thitimatchima, Wiyada.(2010). Online Network: Trends, Phenomena and Ethics. *Executive Journal, 320(4), 150-156.*

Thongrawiwing, Kanathip. (2012). Legal Measures to Protect Personal Privacy Rights: a case study on private rights by social media websites. *Association of Private Higher Education of Thailand Journals* 18)2), 39-51

Tibbetts, S. and Hemmens, C. (2014). *Criminological Theory: A Text/Reader* 2nd edn. California: SAGE Publications.

Toby, J. (1957). Social disorganization and stake in conformity: Complementary factors in the predatory behavior of hoodlums. *Journal of Criminal Law, Criminology and Police Science, 48*, 12-17.

Traimas, Chaowana. (2007). *Basic Data of 75-Year Democracy 1942-2007*. (4th ediction). Bangkok: P. Press

Ungpakorn, J.G. (2003). *From the city, via the jungle, to defeat: the 6th Oct 1976 bloodbath and the C.P.T.* Institute of Asian Studies, Chulalongkorn University, Bangkok.

Wei, M.L.H. (2015). The Challenges of Cyber Deterrence. *Journal of The Singapore Armed Force, 41*, 1.

Wongsurawat, Kowit. (2010). *Politics and Administration of the Kingdom: Multi-dimensions* . (3rd.editon). Bangkok: Kasetsart University.

Wortley, R. and Mazerolle, L. (2011). Environmental Crominology and Crime Analysis: situating the theory, analytic approach and application. In

Wortley, R. and Mazerolle, L. (Eds.), *Environmental Crominology and Crime Analysis* 2nd edn. (pp. 1-18). New York: Routledge.

Yardi, S. (2009). Social learning and technical capital on the social web. *Crossroads, 16*(2), 9-11.

APPENDIX

INTERVIEW FORM FOR DATA COLLECTION TITLE
"PREVENTATIVE MEASURES AGAINST ONLINE HATE SPEECH: A CASE OF POLITICAL CONFLICT"

PART I: GENERAL INFORMATION OF INFORMANT

Name of informant……..….
Position: ……..….
Date of Interview……..…
Place of interview:……..…..

PART II: EVALUATION OF CURRENT SITUATION ON ONLINE HATE SPEECH: A CASE OF POLITICAL CONFLICT AND RECOMMENDATIONS FOR REMEDY AND IMPROVEMENTS

2.1. The authority and responsibility of the agencies in preventing online hate speech

2.1.1. What are your agency's authority and responsibility against online hate speech?

2.1.2. What is your position responsible for preventing online hate speech?

2.1.3. Are there any follow-up, checking and evaluation of the performance in preventing online hate speech? How?

2.2. Related laws in preventing online hate speech in the case of political conflict

2.2.1. Which laws are enforced in preventing online hate speech?

2.2.2. Are there any specific laws enforced in preventing online hate speech? How?

2.2.3. Are there retaliation for non-compliance /law violation? How?

2.2.4. Does your agency have the measures on investigation to attribute offenders or not? If any, which law authorizes for action taken? How?

2.2.5. Are there any specific laws for applying with the political conflict in your agency or not? How?

2.3. The current measures in monitoring and supervising social media in the case of political conflict

2.3.1. What are the measures your agency applied against online hate speech?

2.3.2. Does your agency have specific measures against online hate speech in the case of political conflict or not? How?

2.3.3. Does your agency have measures to handle offenders or not? How?

2.3.4. Does your agency have the attribution measure or not? How?

2.3.5. Does your agency or your position coordinate joint-operation with other public sector or not? How?

2.3.6. Does your agency/your position coordinate joint-operation with private sector not? How?

2.3.7. By estimating current political situation, do you think that measures, that your agency applying, are appropriately efficient? How?

2.4. Barriers and limitations of preventing online hate speech, recommendations and solutions of preventing online hate speech in the case of political conflict

2.4.1. What are the barriers and limitations of preventative measures against online hate speech in the case of political conflict? And what is your recommendation to solve these problems?

2.4.2. In term of retaliation, what are the barriers and limitations of preventative measures against online hate speech in the case of political conflict? And what is your recommendation to solve these problems?

2.4.3. In term of attribution, what are your recommendations to solve the problems or limitations in the attribution development against online hate speech in the case of political conflict?

2.4.4. Estimating the current situation, about solving the problems of online hate speech in the case of political conflict, do you think your agency’s measures meet problem and limitations or not? How? And which part should be amended and improved?

BIOGRAPHY

NAME	Pol.Maj. Wanpadej Hongthong
DATE OF BIRTH	31 May 1985
PLACE OF BIRTH	Bangkok, Thailand
INSTITUTIONS ATTEND	Royal Police Cadet Academy, 2003-2006 Bachelor of Public Administistration (Public Administration) Sukhothai Thammathirat Open University, 2003-2007 Bachelor of Laws University of Kent, 2008-2009 Master of Laws (Criminal Justice)
HOME ADDRESS	2 Soi 2 Pattanakarn 28, Suanluang, Suanluang, Bangkok 10250 Tel.081-3751111 E-mail: pong_4460@hotmail.com
EMPLOYMENT ADDRESS	Huamark Police Station Ramkhamhaeng Road, Huamark, Bangkapi, Bangkok, 10240