A MODEL OF CYBERTERRORISTS' RHETORICAL STRUCTURE TOWARDS PROTECTING CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

KHAIRUNNISA BT OSMAN

DOCTOR OF PHILOSOPHY

2024

Institute of Technology Management and Entrepreneurship

A MODEL OF CYBERTERRORISTS' RHETORICAL STRUCTURE TOWARDS PROTECTING CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

Khairunnisa bt Osman

Doctor of Philosophy

2024

A MODEL OF CYBERTERRORISTS' RHETORICAL STRUCTURE TOWARDS PROTECTING CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

KHAIRUNNISA BT OSMAN

A thesis submitted in fulfilment of the requirements for the Doctor of Philosophy

Institute of Technology Management and Entrepreneurship

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2024

DEDICATION

It is snow on the beach feeling. I dedicate this research to my beloved husband, Muhamad Hafidzul b Ahmad Shahrin who always been my willow in life, endlessly in understanding and supporting me especially during the cruel of summer. This is also to my beloved mother, Faziyah bt Haron and to my beloved father, Shaari b Hashim, who always been my motivation in achieving my wildest dream. Hopefully, this research also could make my beloved son, Hazeeq and my beloved daughter, Husna is enchanted and wonderstruck with her mother. Long lives lovers.

ABSTRACT

Presently, many efforts to eliminate the terrorists are focusing on the physical controls such as body scanner, CCTV, weapons, alarms, and other tangible procedures. Same as the way organizations secure their networks and information from the terrorists' exploitation by focusing more on the defence mechanism such as anti-virus software, malware protection, firewall, and others. However, we should not ignore that the fact that the dependency to the technology has been increasing rapidly due to inexpensive, borderless, fast, and safe by people including the terrorist itself which causes the increase of successful passing of any defence mechanism that being placed. Instead of concentrating of the protection attempts, another strategy as utilizing the situation that the web is overloaded with information put by the people including by the terrorists must be used as other efforts to understand the core causes of terrorists and eventually use it to prevent it from evolves. Therefore, this research is focusing and exploring the terrorists' corpus area by identifying the types of rhetoric in cyber terrorist's communication, analysing how the cyber terrorists utilize the rhetoric in appealing the audience, the preferred stylistics devices and argumentation in their communication. We believe the corpus research able to identify the terrorists' rhetorical strategic and past background. Understanding from the rhetoric side might help eliminating the terrorists as the current efforts are focusing more on defence mechanism which can be defeated eventually. The samples of actual terrorists' postings in the social media are used in the rhetorical analysis. Most of the samples' postings are given by CyberSecurity Malaysia as a credible cybersecurity expert in Malaysia whereby the samples given for the purpose of research and education only. A new research methodology has been designed in this research using the combination of the Norreklit's Methodology, Neo-Aristotelian Criticism, and Ideologist Criticism. The combination of these criticisms can pry out the types of rhetoric used by the terrorist to convey their messages to their target audience. Based on this design, the types of rhetoric are assessed in the attributes of pathos (emotion), ethos (trust), logos (logical), the common stylistic devices used, and the appearance preferred in the social media in term of web's colour and design. These attributes are combined to develop the model of cyberterrorists' rhetorical structure which the effort from this literature perspective able to understand the strategy used by the terrorists in the cyber realm during appealing their audience. The models developed has obtained the accuracy verification by the expert that has vast experience in terrorism and extremism. The model aligns with expert's view based on responses and expert's key writings and books. Recognizing the red flag during social media communication is helping in reducing and disrupting the terrorism activities from continually evolving. The model can be used for the reference of authority, policy maker, system developer, and public by enlarging the benefits in each own field for the protection and security of Critical National Information Infrastructure (CNII) in Malaysia.

MODEL STRUKTUR RETORIK PENGGANAS SIBER KE ARAH MELINDUNGI INFRASTRUKTUR MAKLUMAT KRITIKAL KEBANGSAAN

ABSTRAK

Pada masa ini, banyak usaha untuk menghapuskan pengganas sedang memberi tumpuan kepada kawalan fizikal seperti pengimbas badan, kamera litar tertutup, senjata, penggera, dan prosedur fizikal yang lain. Sama seperti cara organisasi melindungi rangkaian dan maklumat mereka daripada eksploitasi pengganas dengan memberi tumpuan lebih kepada mekanisme pertahanan seperti perisian anti-virus, perlindungan perisian berbahaya, tembok api, dan lain-lain. Walau bagaimanapun, kita tidak boleh mengabaikan bahawa hakikat bahawa ketergantungan kepada teknologi telah meningkat dengan pesat kerana murah, tanpa sempadan, cepat, dan selamat oleh orang-orang termasuk pengganas itu sendiri yang menyebabkan peningkatan kejayaan bolos dari mana-mana mekanisme pertahanan yang diletakkan. Selain berkonsentrasi kepada usaha perlindungan, strategi lain seperti memanfaatkan situasi yang web berlebihan dengan maklumat yang diletakkan oleh orang-orang termasuk oleh pengganas itu sendiri mesti digunakan sebagai usaha lain untuk memahami punca teras pengganas dan akhirnya menggunakannya untuk mengelakkannya dari terus berevolusi. Oleh itu, penyelidikan ini memberi tumpuan dan mengeksplorasi sudut bahasa pengganas dengan mengenal pasti jenis retorik dalam komunikasi pengganas siber, menganalisis bagaimana mereka menggunakan retorik dalam menarik perhatian penonton, stilistik yang disukai dan argumen dalam komunikasi mereka. Kami percaya penyelidikan kesenian bahasa mampu mengenal pasti latar belakang dan masa lalu pengganas. Pemahaman dari sisi retorik boleh membantu menghapuskan pengganas kerana usaha semasa lebih memberi tumpuan kepada mekanisme pertahanan yang boleh dikalahkan akhirnya. Sampel penyiaran sebenar di media sosial oleh pengganas digunakan dalam analisis retorik ini. Kebanyakan sampel penyiaran diberikan oleh CyberSecurity Malaysia sebagai pakar keselamatan siber yang boleh dipercayai di Malaysia dengan sampel yang diberikan untuk tujuan penyelidikan dan pendidikan sahaja. Kaedah penyelidikan baru telah direka dalam kajian ini menggunakan gabungan Metodologi Norreklit, Kritik Neo-Aristotelian, dan Kritik Ideologi. Gabungan kritikan ini boleh menjejaskan jenis retorik yang digunakan oleh pengganas dalam menyampaikan mesej kepada penonton sasaran mereka. Berdasarkan reka bentuk ini, jenis-jenis retorik dinilai dalam ciri-ciri pathos (emosi), ethos (kepercayaan), logo (logik), peranti stilistik yang biasa digunakan, dan penampilan yang disukai dalam media sosial dari sudut warna dan rekaan web. Ciri-ciri ini digabungkan untuk membangunkan model struktur retorik pengganas dimana usaha dari perspektif sastera ini mampu memahami strategi yang digunakan oleh pengganas di dunia siber. Model yang telah dibangunkan telah memperoleh pengesahan ketepatan oleh pakar yang mempunyai pengalaman luas dalam bidang keganasan dan ekstremisme. Model ini selaras dengan pandangan pakar berdasarkan respons serta tulisan dan buku utama pakar tersebut. Mengetahui tanda-tanda bahaya semasa komunikasi di media sosial membantu dalam mengurangkan dan mengganggu aktiviti keganasan daripada berkembang. Model ini boleh digunakan sebagai rujukan kepada pihak berkuasa, pembuat dasar, pereka sistem, dan orang awam dengan memperluaskan faedah dalam setiap bidang masing-masing untuk perlindungan dan keselamatan Infrastruktur Maklumat Nasional Kritikal (CNII) di Malaysia.

ACKNOWLEDGEMENT

Alhamdullilah, first and foremost, praise and thank to the Almighty God for guiding and sending wonderful and good people that can help me out in life including this achievement. I would like to take this opportunity to express my special acknowledgement to my supervisor, Associate Professor Dr. Zanariah Jano from the Institute of Technology Management and Entrepreneurship (IPTK), UTeM for her invaluable patience, supports and advise. I also would like to express my sincere thank you to my co-supervisor, Professor Ts. Dr. Rabiah Ahmad from Faculty of Information and Communications Technology (FTMK), UTeM for the trust, encouragement, and opportunity. Special thanks to UTeM grant funding for the financial support throughout my most of years in this research project. Additionally, this endeavour would not have been possible without the valuable cooperation from Ts. Dr. Zahri Hj Yunos, the Chief Operating Officer (COO) of CyberSecurity Malaysia who had shared the valuable profiles of cyberterrorists that has become the vital samples in this research. I am also grateful to my UTeM lecturers, university mates, classmates and officemates for the lessons and help that had been given along this journey. Special thank you again to my beloved husband, my mother, my father, my son, my daughter and to all my beautiful family for the prayers, belief and motivation. Lastly, thank you to my friends and everyone who have impacted and inspired me to stay strong mentally and physically in achieving and completing this journey.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF PUBLICATIONS

Osman, K., Alarood, A., Jano, Z., Ahmad, R., Abdul Manaf, A., and Mahmood Marwan Mahmood, M., 2019. A Conceptual Model of Cyberterrorists' Rhetorical Structure in Protecting National Critical Infrastructure. In: In: Benavente-Peces, C., Slama, S., Zafar, B. (eds) *Proceedings of the 1st International Conference on Smart Innovation, Ergonomics and Applied Human Factors (SEAHF)*, Smart Innovation, Systems and Technologies, Cham: Springer.

Osman, K., Jano, Z., and Ahmad, Rabiah., 2024. A Model of Cyber Extremists' Rhetorical Structure Towards Protecting Critical Infrastructure, *Journal of Computer Science*, 20(6), pp. 610-627.

CHAPTER 1

INTRODUCTION

1.1 Background

The use of network infrastructure for cyber communication is increasing especially in the current of 21st century. It has been skyrocketing since early 2020 due to the pandemic (Kemp, 2020). According to Roztocki et al. (2019), the secure and quick medium is one of the factors contributing to the growing use of information and network technology in daily communication. Recent statistics from Statista (Petrosyan, 2024) has shown the numbers of internet users from 2005 to 2024 are increasing to 5.4 million where 5 million are the users of social media. Therefore, it is no surprise that the cyber communication is a liability because it has become a preferred medium of communication as well as a preferred medium of attacks from those who possess malicious intent including the terrorist (Counterterrorism Yearbook, 2021).

Usually, the security focuses on the terrorist technical attack to protect the life and critical infrastructure such as the forbidden of dangerous items to certain areas, bomb scanner, CCTV, alarm, security check at borders and entrance, etc (Webber, 2024). These are being implemented as part of the standard response for protection controls and security measures when the destruction is visible and has the potential to instil an overwhelming sense of dread, panic, and terror among people. The efforts of enhancing the security controls where mostly on the physical environment and the most preferred aspect of security measures (NATO, 2024).

Like the physical world, the cyber realm has been concentrating also on the component of access-control in the network and application level. According to Zheng et al. (2022), the cybersecurity focuses more on the defence and response mechanism such as firewall, anti-virus, password, intrusion prevention system, and others in order to prevent the non-authorized party such as terrorists from being accessing the protected critical site. The demand has caused many studies conducted more on developing a new method of protecting and securing the cyber world from being penetrated by the non-authorized party based on journal written by Li and Liu (2021).

While the controls emphasize on the tangible and visible area which primarily on the physical security and access-control in the cyber realm, it has resulted the ignorance on several crucial perspectives. Our cyber realms are laden with the information overloaded; where with a proper strategy and methodologies, a comprehensive picture of terrorist activities such as recruitment of new member, plan of attacks, relationship background, businesses, daily routine, etc. enable to be obtained (Prezelj and Zalokar, 2023). Focusing on the terrorist rhetorical is enable the core causes and valuable information are identified in which a way more effective and efficient in saving lives and protecting the critical infrastructure.

Given the growing reliance on the cyber technology, it makes sense to participate in the study of terrorist information on the internet as part of important area of cyber security (Savas, S., and Karatas, S., 2022). Developing methods to understand the rhetorical strategies such as terminological assumptions, violent metaphors and ethical conflicts are deemed essential to understand the terrorist background and upbringing. They can be used to determine the types of rhetoric strategies so that the terrorists' appeal approach to the audience can be examined. It is also possible to look at further patterns in the picture, colour, and physical characteristics used by the terrorist in the terrorism communication. The

strategy used by the terrorist to influence and propagate the agenda to the audience is vital to be identified by a public sector, private sectors and citizen as well, so that the prevention of the terrorists' activities can be conducted during early signs (Shire, M.I., 2021). This rhetorical analysis can be used as part of component in crucial security measures; considering the objectives of this effort enable to the understanding of the terrorist activities is obtained from the root causes (Martin, J., 2020). It is important for protecting the human life and the critical infrastructure.

1.2 Problem Statements

Literature on Information Technology indicates dependency on technology. According to the Masiga and Marchant (2023) from the World Economic Forum, technology is a vital tool for creating a cleaner, safer and more inclusive world. Businesses are looking for digital transform to become more efficient and productive. It is no doubt that computing platform is continuing to evolve, the rise of quantum computing that begin to solve problems in physical worlds such as materials, chemistry, encryptions, and others (McKinsey and Company, 2024).

Therefore, according to Admass et al. (2024), the cyber world now has become a target due to rise in dependency and dependant aspects because it is inexpensive and borderless when compared to other ways of access including land, air, sea, or even space. These days, malicious individual and groups regularly attack websites, making this reliance on technology a liability that harms essential infrastructure and services that depend on it (CISA, 2022). According to Broeders et al. (2021), the terrorist attack on 9-11 has brought attention to the possibility of the cyber terrorism. According to them, the advancements in technology, such as artificial intelligence and blockchain, can both mitigate and exacerbate the threat of cyber terrorism.

However, according to North Atlantic Treaty Organisation (NATO, 2024) in recent article, NATO's works on counterterrorism is focusing on awareness of the threat, developing capabilities to prepare and respond and enhancing engagement with partner countries and international. For researcher, the efforts more on detection and response rather than prevention and identification of core-causes of terrorism. Same as UN Global Counter-Terrorism Strategy (UN, 2023), the efforts focus more on the military detection, response and regulations in general. Same efforts in the cyber realm where much research at present focus on the ways in which organizations secure their networks and information in the supply chain, ignoring the ways in which organizations construct and understand the core of the cybersecurity risks (Burak, 2023). The cybersecurity focuses more on defence mechanism such as anti-virus software, malware protection, firewall, and more on securing network and application (Fruhlinger, 2022). However, it would not stop the terrorist activity from being occurring. The terrorists will always return with the improved attack techniques since the last time (Colin, 2022).

According to Braddock (2020) through his book of Weaponized Words: The Strategic Use of Persuasion in Violent Radicalisation and Counter-Radicalisation, the significant gap in traditional terrorism studies, which often overlook the rhetorical dimensions of extremist communication. The early discussion and analysis in the development of the subject of computer science are only marginally applicable to today's problems and do not address emerging issues like the corpus of cyberterrorists. For example, studies like Myriam Dunn Cavelty's investigation as cited in Bjorgo and Silke (2018), the rise of cyber-terrorism discourse as a reflection of physical acts of terrorism (like the 1995 Oklahoma City bombing) shows that the language level studies that do exist for cybersecurity have focused almost exclusively on state and nation-level cyber-rhetoric and have not systematically examined the everyday business decisions that hackers (of all hat colours) are making.

Web is one of the technologies where the terrorists always prefer to channel their

communication through web application to promote their ideology, to facilitate internal communications, to attack their enemies, and to conduct criminal activities (Jematia, C., 2021). According to Mansour (2018), the ISIS group has used social media as weapon platform to attract new members, transmit ideology, operation, tactics and battles on a scale of that is exponential. ISIS is a well-known terrorist group which stands for "Islamic State of Iraq and Syria" (History, 2017). Therefore, the web applications are hampered by the information overload including terrorists' information and the greater study to examine the terrorist corpus is needed as the web is flooded with numerous conversations and data posted by the terrorists based on Scrivens et al. (2024). As a result of people's increasing reliance on technology, including the terrorists themselves, the information encumbered in the cyber realm should not be ignored and it should be indicated that the corpus study is important as part of solutions to comprehend terrorist action (Altamimi, 2021).

Moreover, the roles of sociologist and rhetor researchers in cybersecurity realms are deemed essential given that the web is laden with terrorist information such as terminological assumptions, violent metaphors, propaganda rhetoric, ethical conflicts, appearance preferable, and others (Matusitz, 2018). The fundamental strategy for cybersecurity efforts to comprehend the pattern and the language used by criminals and terrorists daily should include the understanding of the approach taken by the terrorists. According to Toro and Adrew (2018), understanding the core causes of the terrorism activity is able to detect the early sign such as the education background, past-trauma, culture and others.

1.3 Research Questions

The objectives of this research have been through the following three (3) main questions:

1.3.1 What types of rhetoric and preferred stylistic devices used by terrorists in the cyber communication?

1.3.2 How the cyber terrorists utilize the rhetoric in appealing the audience and

during argumentation in communication?

1.3.3 What is the model of rhetorical structure for cyber terrorists?

1.3.4 Is the model developed is obtaining verification from expert?

1.4 Research Objectives

The objectives of this project were as follows:

1.4.1 To identify the type of rhetoric in cyber terrorist's communication.

1.4.2 To analyse how the cyber terrorists utilize the rhetoric in appealing the audience, the preferred stylistics devices and argumentation in their communication.

1.4.3 To develop a model of cyber terrorists' rhetorical structure.

1.4.4 To obtain the verification of the model from an expert.

1.5 Research Scope

To achieve the research objectives, the samples of terrorists' postings are obtained as per Table 1.1.

Table 1.1: Samples of cyberterrorists' profiles

No.	Profile Name	Platform of social media	Language Used	Number of Postings	Timeline	Terrorists Group Related
1.	Pattani Darussalam - Khattab Media Publication	blogspot	Melayu-Malaysia	11	July – August 2008	Tandzim Al-Qaeda Southeast Asia