LIRA Journal, 2024, Vol. 1, 39-52.
https://journal.lira.pk/LIRA/

Military-Public Relations: A study of contemporary Information Warfare in Clausewitz Trinity through CogSec Perspective

Laiba Imran Dr. Zeeshan Zaighum** Rana Faizan Ali****

**Researcher, School of Media & Mass Communication, Beaconhouse National University, Lahore.*
***Assistant Professor, School of Media & Mass Communication, Beaconhouse National University, Lahore.*
****Assistant Professor, School of Media & Mass Communication, Beaconhouse National University, Lahore.*

Abstract

Contemporary information warfare aims at weakening a state internally. Literature shows that such attacks are targeted at the relationships between and among the elements of Clausewitz's Trinity i.e. government, military, and public. The study offers military and academic literature to contextualize the dimensions, attacks, and vulnerabilities of COGSEC (Cognitive Security) in the Online Information Environment The present study explores the public discourse on twitter to comprehend military-public relationship in Pakistan in the context of COGSEC (Cognitive Security), the hashtag under study was #PakArmy. The study is a qualitative research and the researcher has carried out discourse analysis by using the Speech Act Theory of Searle (1979) and examined tweets into five categories: Assertive, Commissive, Declarative, Directive and Expressive. The researchers have also mapped vulnerabilities as proposed by Linan Huang and Quanyan Zhu (2023) i.e. Perception, Memory, Attention and Mental Operations. In addition to this, the researchers have categorized the public discourse into favorable, unfavorable, and neutral in the context of military-public relationship of the Clausewitz's Triangle. The data shows that perception is the most persistent vulnerability in the public discourses. Whereas, the data also poses that public discourse is also dominantly unfavorable towards the relationship-reflecting attacks on the relationship. Furthermore, expressive tweets were found to be in majority. The study has recommended a three phased strategic framework to strengthen Military – Public Relationship. The advised framework poses that aggressors are trying to create a wedge between Military and Public, therefore, at the short term level SOCMINT should be used to encounter such activities. For mid and long term level, perception management as well as narrative warfare must be engaged.

Keywords: Cognitive Security, Military – Public Relations, Information Warfare, Online Information Environment, Public Discourse.

INTRODUCTION

Digital Technologies have transformed the character of warfare. This transformation has emerged into information warfare that has been challenged through the Cognitive Security (COGSEC) perspective. Cognitive security is an approach in which ideologies, thinking processes, and

perceptions of individuals are protected so that they do not misinterpret the information available to them on online platforms, as this could backlash for the country and is likely to weaken the deterrence posture of the country, especially for a country like Pakistan where people do not have media literacy. Meaning there by, that giving in at adversaries and becoming a vulnerable state not being able to prevent itself from a cyberattack or international attack.[1] Therefore, a comprehensive analysis of the Clausewitz Trinity, especially the military component in the context of Pakistan should also consider the role digital media plays in information warfare as well as the influence of the three key elements of Trinity; government, military and public, where Trinity is a useful tool to conceptualize the chaos of war.[2] In simpler terms it means to examine how digital spaces are used by government, military and the public to conduct informational operations.[3] However, the main focus of this thesis would be on the between military and public would be studied for information warfare through a cognitive security perspective in Pakistan.

Problem Statement

Modern digital technologies have completely transformed the digital realm by rapidly increasing information networks in number. This transformation has led us into information warfare. This means that traditional war methods are replaced by this new modern (information) warfare which further includes sensitive aspects like those of attacks on cognitive security. Such attacks exploit vulnerabilities in human cognition and also affects the way humans now perceive things which ultimately has decision making consequences. Hence, there are significant implications on the military - public relations that falls within the framework of Clausewitz trinity. It also harms the trinity by causing doubts amongst the elements which can have serious damages on the national security. If the public continues to believe on the manipulated content against the military, it helps the adversaries in successfully carrying out their COGSEC attacks. However, the existing research focuses mainly on the traditional warfare or military strategies and thus fails to address the multifaceted challenges posed by the attacks on COGSEC. Therefore, this study aims to study contemporary information warfare through a cognitive security perspective and would also analyze how various strategies and tactics that are employed on these attacks have an effect on Clausewitz's Military - Public relations. By understanding the intricate interplay between cognitive security attacks, human perception ability and the dynamics of Clausewitz Trinity, this research seeks to provide most effective communication strategies and strong cognitive security measures for the safety of national security interests.

Research Objectives

Q1: Studying the Public Discourse on Military – Public Relations.
Q2: Examining the existing COGSEC.
Q3: Vulnerabilities in cognitive security that make adversaries easily manipulate individuals Or groups.
Q4: To devise a framework for strengthening cognitive security.

Digital media is a critical component that is used to influence the minds, perceptions and ideas of individuals as well as groups to achieve strategic goals.[4] Influencing the human brain or cognition

[1] Chambers, *South Asia in 2020: Future Strategic Balances and Alliances*.
[2] Cserkits, "The Concept of War in Ancient Mesopotamia: Reshaping Carl von Clausewitz's Trinity."
[3] Arquilla and Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*.
[4] Arora and Predmore, "Social Media as a Strategic Tool: Going beyond the Obvious."

through digital media could be done through brainwashing individuals by providing them with misinformation, which is like feeding the human brain with information that is manipulated for personal means.[5]

Psychological warfare is planning to use propaganda in such a way that an individual's thoughts, decisions, perceptions and sometimes even attitudes can be influenced to fit into a particular narrative.[6] There are three types of propaganda; White, grey, and black. The white propaganda has true information and is cited; however, it is slightly biased. The grey propaganda has almost true information, but it is not cited. The black propaganda is completely fabricated news.[7] These propagandas are used to influence the cognitions of people, which ultimately affect the information environment.

Many components of the information environment in his article such as one of the main components identified by the author is the social context in which media operates. This includes the "Norms and Values" and belief systems that shape how messages or information from the media are received and interpreted by people. The authors claim that media is not neutral in representation of social reality, rather they are shaped by dominant ideologies and power structures of the society which ultimately influence the production and dissemination of information.[8] This component also includes the cultural context of the information environment. As social norms and values are part of cultures factors like language, symbols, and traditions also shape the way messages are constructed and received. The author argues that media messages are not simply transmitted but are actively constructed by keeping in mind the cultural aspect by the producers and consumers of the content.

Another important component of the IE identified by the author is the "Regulatory Framework" or the political context in which the media operates. It includes the institutional structures that govern media production and distribution. The author notes that media is subjected to various forms of regulations including legal, economic, and social constraints that influence the content of information.

In addition to these components, the author identifies "Information systems and technologies" as a crucial factor in shaping the information environment. This includes the use of new technologies such as social media which has altogether transformed the way messages are produced, distributed, and consumed. The author notes that the use of new technologies has also created new forms of control in the IE realm, as it has given significant power to the use due to which there are implications for the production and distribution of information.

---

[5] Bagozzi and Dholakia, "Antecedents and Purchase Consequences of Customer Participation in Small Group Brand Communities."
[6] Matadi et al., "Effects of Biphenyl Polymerization on Lithium Deposition in Commercial Graphite/NMC Lithium-Ion Pouch-Cells during Calendar Aging at High Temperature."
[7] Longley, "An Introduction to Psychological Warfare."
[8] Li, Pearce, and Low, "Media Representation of Digital-Free Tourism: A Critical Discourse Analysis."

Moreover, the author mentions "Data and Information" because the raw data and the information being processed is what make an information environment. The data is produced, disseminated, and consumed in the form of messages and information. Thus, data is what makes information which eventually forms a part of the information environment. Similarly, studying the constituents of the information environment also shows a link with media ecology, as the constituents and media ecology have an interchanging concept, but this is a discussion for later on.

In addition to this, the components of IE do not only include the above-mentioned constituents it also includes Non-state and State Actors which are discussed as follows.
Paganini defines non-state actors as organizations that hold power and influence but cannot be considered a part of the official state structure – that is the control the government has over it.[9] The author's focus is on the exploitation of online platforms by terrorist groups like Islamic State (IS) for propaganda, recruitment, and financing. These online platforms have aided in the provision of powerful means for the non-state actors, i.e. dissemination of messages, and ideologies and in coordination and execution of their activities. These groups have been able to scale up their anonymity and reach of the internet to establish and maintain global networks of sympathizers, supporters, and members. Paganini's paper also talks about the crucial challenges that non-state actors bring to national and international security, particularly around cyber-attacks and their use of digital media for the conduction of terrorist activities. Non-state actors are increasingly using sophisticated cyber tools and techniques to perpetrate attacks on critical infrastructure, steal sensitive information, and disrupt government operations.

Moreover, state actors are referred to as individuals who hold authoritative positions within the state, they could be politicians, individuals in assemblies, bureaucrats and so on so forth.[10] These individuals play a very important role in shaping public policies thus public opinions. They have the power to implement laws and regulations, provide public goods and services and they also have to ensure national security. They can be elected or appointed by the people or the government itself to serve at different designations within the government, it could be from a local level to a national level. The authors state that the actions and decisions made by the state actors can have a high impact on the country's social, economic and political outcomes. This is the main reason why they are always under public and media scrutiny, thus, they become answerable if something goes wrong. Moreover, the paper just not only defines state actors and non-state actors it also examines the rule of "trust" in shaping the relationships between these actors and citizens in development countries, especially in the context of service delivery as public expects them to provide with deserving services for the citizens. The authors argue that trust play a very crucial role in determining the effectiveness of state actors in delivering public goods and services such as healthcare, education, and infrastructure. Moreover, the authors believe that trust in state actors is influenced by many factors for instance quality of governance, the level of political competition and the degree of social capital in the given country. They argue that the most effective way of improving public service delivery is by building trust in state actors by the public.

Hence, by reviewing the above it can be concluded that the above-mentioned constituents and factors are what make up the information environment in its entirety. However, there is an

[9] Paganini, "Non State Actors in Cyberspace: An 'Attempt to a Taxonomic Classification, Role, Impactand Relations with a State's Socio-Economic Structure. Commentary."
[10] Acemoglu et al., "Trust in State and Nonstate Actors: Evidence from Dispute Resolution in Pakistan."

emergence of new threat actors too. There are two types of emerging threat actors that can cause immense harm for the information in future.[11]The authors believe they are information capitalists and elected vigilantes. Before describing the threat actors, the authors explained that since the technological world is evolving so are the actors. They believe that state-sponsored or independent terror actors will continue to exist alongside new "bad" actors due to the expansion of network technology. The authors believe that the *information capitalists* would be those actors who would trade information for their profitable means. Meaning that they would capitalize on the traded information which would create a division between who could access information and who could not. The authors believe this will be done either by gaining revenue from the information which would exclude people from access if they were unable to afford it. Others would be those who might have the finance to purchase it but not necessarily the supporting infrastructure to access it. This is how actors would not only profit from the information rather also create a gap of accession. The other category of actors about which the authors talk is the *elected vigilantes*, in which they believe that the future government will use tactics that are like those used by criminal organizations to maintain public safety. They believe that the government would use tactics of surveillance, monitoring or even manipulation that could be considered as illegal or unethical activities. The authors fear that such tactics would mean that governments will open themselves up to the possibility of their systems being attacked, misused, or abused by malicious actors or criminals.

Cognitive security is an approach used in cybersecurity that uses multiple techniques like machine learning and tactics like artificial intelligence to detect, respond to, and prevent any cyber threats that come in the way of breaching security. It includes the use of various algorithms and models that are used to analyze huge amounts of data to identify patterns that show security threats. Cognitive security (COGSEC) believes in using tools that would maximize accuracy as well as the speed of threat detection by incorporating human-like reason or cognitive computing into cybersecurity systems.[12]

Robert O Andrade and Sang Guun Yoo aim to explore the concept of cognitive security with its application in cybersecurity. The authors define COGSEC as a multidisciplinary field that is the combination of science, psychology, neuroscience, and computer science all of this in the context of cybersecurity to enhance human abilities in a way they can easily identify threats as well as have capabilities to respond to them.[13] The paper emphasizes the improvement of traditional security measures with the advancement of new technology, where initially security methods focused more on securing the technology or infrastructure related to the technology and the new focus in cognitive security is on comprehension of human behavior and their cognitive processes so that there could development of more effective security solutions. The paper discusses the terms, cognitive bias and mental models. The former refers to the tendency of humans to make errors, systematic errors, in judgment and reasoning of perceived information. Whereas the latter is the internal representation (mental) of the external world of how the information is perceived and what should be the response to it. The authors also highlight the role of artificial intelligence

[11] Ross and Rutland, "A Military of Influencers."
[12] Huang and Zhu, "An Introduction of System-Scientific Approaches to Cognitive Security."
[13] Andrade and Yoo, "Cognitive Security: A Comprehensive Study of Cognitive Science in Cybersecurity."

and machine learning in cognitive security. It is so that these technologies can help in identifying anomalies and the patterns in human behavior which are key indicators of security threats. The paper discusses the importance of designing security systems that are user-friendly as well as intuitive (like humans) so that human limitations and cognitive biases can be considered. For instance, the paper discusses biometric authentication, gamification, visualization, and personalization.

Cognitive Security Vulnerabilities

The authors Linan Huang and Quanyan Zhu discuss the vulnerabilities that are operationalized in Cognitive Security (COGSEC) by the attackers to exploit their target audience.[14] The four main vulnerabilities that the authors talk about in detail are attention, perception, mental operations and memory. They are as follows.

Perception vulnerability

According to the authors, the way humans perceive information is complex and thus it has an involvement of various sensory systems. The attackers analyze and comprehend the human sensory system to take advantage in a way that the victim is unaware of. For instance, the authors explain that such attackers create environments to exploit the perception limit like timing or sensory effect such as when in 2013 there was an incident of hijacking the Association's Press Twitter account where the enemies posted false news about explosions in the white house which has resulted in Barack Obama's injury which ultimately caused a drop and recovery of $136B. This example proves the point the authors Linan Huang and Quanyan Zhu are trying to prove that playing with time, or visuals in such a way can affect the targeted person subconsciously and they get attacked with the message the adversary is trying to convince with, however, the person themselves do not realize it.[15] The authors note that the attackers can manipulate perception of information, message, image, or even a word by using psychological techniques such as priming: which influences how stimuli are interpreted by the receiver or processed. Positive priming can emphasize ideas or create associations with words or images easier and faster, while negative priming slows down the processing speed of the same association. The authors believe that both priming techniques are used by attackers to deceive people, however, these techniques are comparatively to be detected by the systems or COGSEC management unit. Hence, the authors claim that adversaries are more likely to use subliminal priming which is a technique that is below the threshold of conscious perception, due to which it is far more difficult for the systems to detect and can very easily deceive people and influence their decision-making subtly.

Attention Vulnerability

The authors have discussed two main vulnerabilities that are exploited by adversaries in the "attention" part of the human brain. This cognitive vulnerability has two parts the reactive attention attack and the proactive attention attack. The authors note that in the former attack, attackers use social engineering techniques and phishing techniques in such a way that the already distracted person fell prey to it. This could happen if they are distracted or because of lack of attention, when the adversaries are aware that their victim is inattentive, they would exploit this time for their gain to conduct a malicious activity. Similarly, the authors note that attackers use reactive attention attacks strategically to influence human attention patterns. The authors explain this with an example of a bombardment of emails, all of them would have the same message except that one

[14] Huang and Zhu, "An Introduction of System-Scientific Approaches to Cognitive Security."
[15] Huang and Zhu.

of them would have a hidden disruption message for the victim's system also known as the information denial of service attack (IDoS). Thus, both techniques are very carefully used by the attackers to cause harm to their victims.

Memory Vulnerability

The authors also discuss the vulnerabilities related to memory and the security risks the human memory play which makes it easier for attackers to exploit cognition for security purposes. The authors talk about the limitation of the human mind regarding memory errors forgetfulness or retrieval and the limitation of digital "minds" regarding restricted capacity and limited speed of information storage. Hence, these limitations are exploited by the adversaries which pose security threats. The authors note that due to the forgetfulness nature of humans, they tend to use the same passwords for different platforms or tend to write it down somewhere to keep them from forgetting. These problems are identified by the attackers and hence they use this human limitation for their use by exploiting or hacking the systems which ultimately creates attacking vectors. The authors explain attack vectors by the techniques of phishing emails or misleading hints so that memory loss can be triggered, or false memories can be injected. However, the authors also propose solutions to stay away from such traps by using single sign-on or graphical passwords.

Mental Operations Vulnerability

The authors also discuss some human cognition biases that make way for attackers. The author talks about four main biases that make people vulnerable to attack: anchoring, framing, optimism bias, and in-group bias. The authors describe anchoring again as a social engineering technique in which people are already given information through malicious activity, and then they build on that information which makes it more repetitive and persuasive thus they fall prey to the scam or attack again. Similarly, the authors note that attackers manipulate or present the information in such a way that they "frame" it to gain personal meaning. In addition to this, the authors talk about the optimism bias where humans are highly optimistic by nature that they tend to neglect the negative or downfalls of an activity, they overestimate the positive outcome and undermine the negatives. Lastly, an in-group bias is also present in people that is noted by the authors, they explain how people believe an insider over outsider whereas that insider could be a part of the adversary. The purpose of noting these biases by authors' point of view is to understand human nature and how such biases can create sensitive issues regarding security.

The authors also talk about the personal traits that people have that can cause biasness. For instance, reciprocity element, social proof (an adversary person being friends with your social circle), (imitation) authoritative person, or a person who likes you (pretence), scarcity (to cause urgency), and lastly (false) commitment. Such biases of victim's were exploited by the Pegasus attacks by using existing biases against their own selves.[16]

Theoretical Framework

The theoretical framework of this study is based on two core theories; The Clausewitz Trinity and the Technological determinism theory. The theories independently as well as when correlated play

[16] Khurana, "Pegasus and Its Effects in International Realm."

a crucial part in helping comprehend the dynamics of Clausewitz Trinity like those the relationship between the Military and Public. Similarly, these theories help in understanding how technology plays a vital role in society in the context of information warfare, such as when the information is disseminated and it is time to perceive that information to make decisions based on it like that under cognitive security.

Conceptual Framework

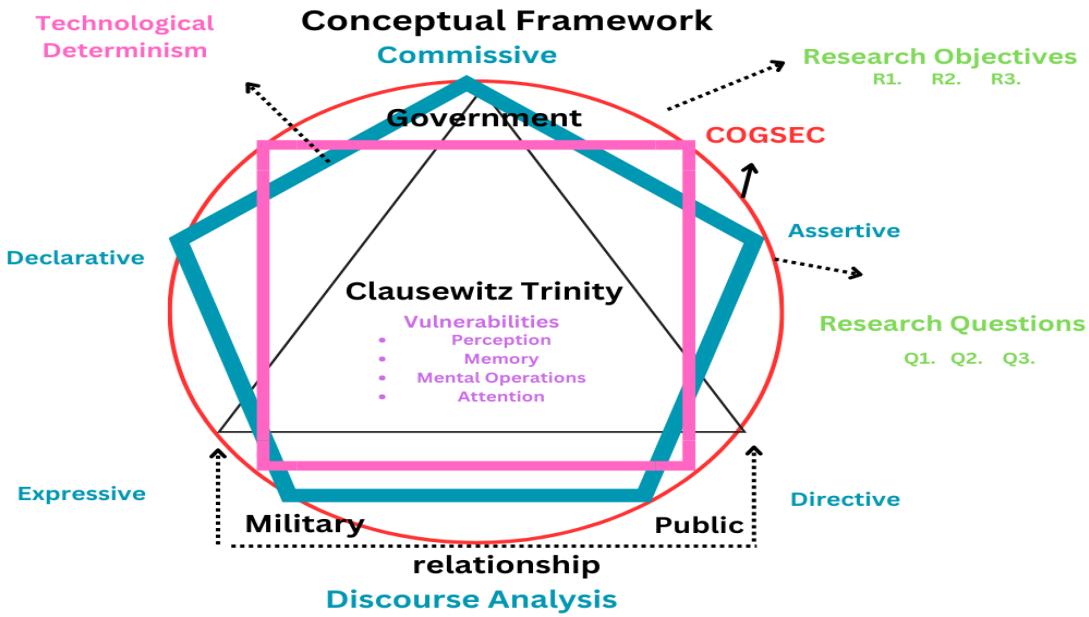

Figure 1: Conceptual Framework designed by The Researcher

The figure represents the conceptual framework of the study. The study aims to explore three theories, the Clausewitz Theory and Technological Determinism. The third theory is the speech act theory that is the base of discourse analysis. Searle's Speech Act theory, that will categorize the public discourse in five categories; Assertive, Directive, Declarative, Commissive and Expressive. Later, these theories will be incorporated in the research questions and objectives.

Research Methodology

The methodology used for this study is discourse analysis a qualitative research. The quality research is based on asking questions that answer "how" and "why" part of the study in discussion, which is not quantifiable in nature. Thus, unlike quantitative research which is linear in nature qualitative research is more flexible and adaptable, however, it does not mean it has no linear aspect. The biggest strength of qualitative research is its ability to study those human behaviors, attitudes and processes which would have been difficult to quantify.[17] This study is based on studying the human cognition such as attitudes, perceptions and the ability to make decisions in regards with military – public relationship, which is why qualitative research is used to analyze these aspects. As these aspects cannot be directly quantified, they need an analysis strategy for

[17] Tenny, Brannan, and Brannan, "Qualitative Study."

operationalization. Four main vulnerabilities: perception vulnerability, memory vulnerability, attention vulnerability and mental operations will be discussed to interpret the data in discussion.

Discussion

In the era of social media, the invention of a medium such as "Twitter" has emerged into powerful tool that can be used for information dissemination as well as public discourse. With the rise of social media platforms like Twitter, public opinions and perceptions are being shaped at an unpredictably alarming rate. These attitudes and opinions are then not only shaped rather are available out in the open which can further shape the perceptions of other people and influence their judgement and decisions. The study of "Military-Public" relationship through such opinionate tweets from Twitter helped this study in finding some valuable insights for the COGSEC perspective and information warfare. It also helped in understanding the intricate interplay of military and public relationships. Hence, understanding the dynamics of information warfare is becoming crucial because only then it will be easier to comprehend the implications it has on cognitive security and the impact it has on the "Military – Public" relationship from these interactions. In simpler words, the study of public discourse will help in understanding the dynamics of information warfare and the influence mediums like Twitter or social media has on people.

The paper used Searle's speech act theory for public discourse on the relationship of the Military and the Public. As mentioned earlier, 13132 tweets were extracted which were the amalgamation of tweets and retweets. A total of 5020 tweets were left and 10% was analyzed for the discourse. The hashtag used was #PakArmy as the study aims to explore "military" and "public" relationships. No negative or positive hashtags were chosen to study, rather a neutral PakArmy hashtag was opted so that all types of opinion (negative or positive) can be extracted for the discourse and the real relationship the two elements of Clausewitz Trinity have can be determined and thus concluded. Contemporary information warfare has transformed the public discourse area, especially in the context of military–public relations. Information warfare is any action that can deny, corrupt or exploit the information or information systems of adversaries through manipulation, degradation or denial of information.[18]

However, in the context of Military – Public relationship it is important to understand the Clausewitz Trinity, since it is with involvement of actors like military that disrupt the system of adversaries by trying to protect themselves from such attacks. Clausewitz Trinity suggests that three elements, the government, the military and the public have an intricate relationship with one another that leads to complex multifaceted situations like war.[19] The relationship of these elements is independent as well as interlinked with one another. The relationship begins to clash when there is an involvement of cognitive security. Cognitive security is an approach that uses techniques or methodologies to mitigate the potential threat to cyber security or system security. It can utilize diverse models and algorithms to study extensive datasets and recognize any threats or patterns of threats that could be posed or could indicate security vulnerabilities.

[18] Tenny, Brannan, and Brannan.
[19] Echevarria II, *Clausewitz and Contemporary War*.

The cognitive security itself does not harm the relationship of Military - Public rather when the cognitive security is breached, that is when this relationship starts to damage. Malicious activities like echo chambers, rumors, misinformation and disinformation are the tools that breach COGSEC. For instance, if any misinformation regarding the military is spread through social media platforms, the youth will immediately pick up that information and believe it, only few might counter check the given "misinformation" with facts which also refers to technological determinism as the way people perceive information in modern day is the result of this. Hence, such tools and technologies play a role in creating a gap between the two elements and the relationship begins to deter.

In addition to this, Pakistan already faces a range of security threats including terrorism, extremism, regional conflicts. Information warfare is now an addition to these existing threats which then contributes to the fragility of the issue.[20] It means that basically the "fragile" area of the information environment is from where the issue begins. Floridi describes the information environment as processes, resources or information that use this knowledge to apply it to the society. Meaning thereby, that when the information being disseminated is the *problem*, then the problem that causes breaches in cognitive security come later but the information environment itself becomes the problem to begin with.[21]

However, the vulnerabilities of cognitive security contribute to the problem of the information environment. Four vulnerabilities are described in the work of Linan Huang and Quanyan Zhu. The authors describe perception vulnerability, memory vulnerability, attention vulnerability and mental operations vulnerability.[22] The perception vulnerability is stated as an attack from adversaries through the technique of playing with time, or visuals in ways that can affect the targeted person subconsciously. They get attacked with the message the adversary is trying to convince with, however, the person themselves do not realize it and falls prey to the message. The message or visual is targeted at individuals or group so that their perception can be influenced, and they are convinced otherwise.

The one technique that is mostly used in perception vulnerability is the technique of priming, negative or positive priming. The word or image used in negative priming is to slow down the cognitive processes and thus the thinking brains. Whereas, in positive priming the word or image used to attack with is associated with something to create a sense of belongingness to deceive the person, and hence, influence the perception. The other vulnerabilities are rather simple. Attention vulnerability is stated as diverting the attention or reducing attention span on the important information to influence decisions. The memory vulnerability is associated with creating fake memories to convince the individual of something which would then influence their judgements. Lastly, mental operations work on the senses of the individuals or group to influence perception, decision making or judgement.

Vulnerabilities alongside the speech act theory of Searle helped in understanding the public discourse of military and public. Searle divided the theory into five categories; assertive,

[20] Khan, "Understanding Information Warfare and Its Relevance to Pakistan."
[21] Floridi, "Semantic Conceptions of Information."
[22] Huang and Zhu, "An Introduction of System-Scientific Approaches to Cognitive Security."

commissure, directive, declarative and expressive for the discourse analysis.[23] With the help of this, the discourse on #PakArmy was conducted which showed that 212/502 tweets were expressive tweets. And 279/502 tweets were not in favor of civil-military, which proves that there are clashes between the Military and the Public. Lastly, 361/502 tweets were categorized in perception vulnerability which emphasizes on how perception vulnerability is the most important vulnerability and if that is attacked then there is a breach in cognitive security, which further damages the relationship of the elements of Clausewitz Trinity.

CONCLUSION

The focus of the study was on the five categories of the speech act theory: Assertive, Declarative, Directive, Expressive, and Commissive. This categorization helped in understanding the dynamics of communication the Military and Public have with one another. Each category will be individually discussed, for instance starting by analyzing the tweets that fall under the assertive category of the speech act theory. Assertive tweets are statements that could be true or false, they are an expression of factual "claims", beliefs, or opinions.[24] By exploring the assertive category of tweets, cognitive dimensions of public discourse could be studied. This could help in understanding how these dimensions shape perceptions of people and influence the cognitive security environment. Starting by analyzing assertive tweets from a COGSEC perspective will help us in exploring various patterns, themes, and perhaps the potential cognitive tensions that could be visible within the military–public relationship.

Recommendation

Following is the recommended framework for the protection of cognitive security in Pakistan:

[23] Smith, "Speech Act Theory, Discourse Structure and Indirect Speech."
[24] Smith.

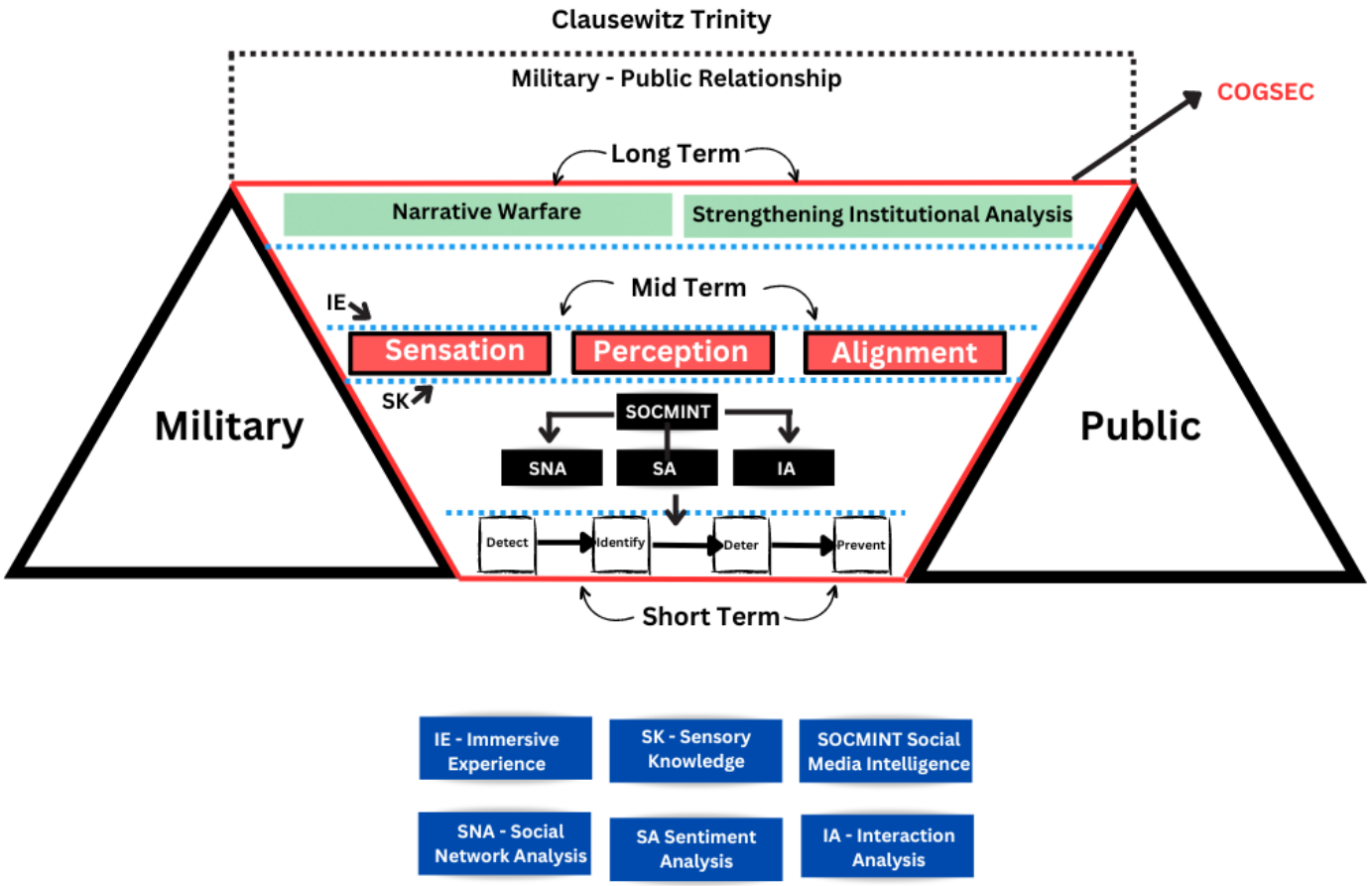

Figure – Designed by Researchers

The framework has been devised on three levels which are as follows:

- Short-Term: For short term detection of unfavorable, offensive content should be done. This can be carried out by using sentiment analysis and interaction analysis on the social media either by engaging researchers or data analysis software/ algorithms.
    1. The second step is identifying the creators, spreaders and facilitators of such content.
    2. The identification of these accounts/ individuals can be done by using social network analysis tools.
    3. The third step is deterrence that can be achieved either by coercing counter narratives or by the strict implementation of the law.
    4. The last step is preventing the public discourse from being exploited. Primitive and proactive approach to monitor public discourse on digital as well as traditional media can be very effective in this regard.
    5. Lastly, the monitoring of social media should be strategically carried out by keeping in mind the contemporary trends and practices of SOCMINT.
- Mid-Term: For mid-term collective and individual sensation should be built.

1. The first step is to incorporate immersive experience activities which may include augmented reality (AR) and virtual reality (VR) technologies.
2. The second step is perception management which can be achieved through fostering strategic relationships with communities and community leaders to encourage institutional advocacy at individual and societal levels. Traditional media and digital media, civil society, and educational institutions can be effective in encouraging and promoting in building military–public relationships.
3. The third step is the alignment of favorable public discourse on the elements of Clausewitz Trinity. The alignment can be characterized by trusting the state institutions and supporting state priorities.

- Long–Term: For the long term collective political memory should be formed.
  1. The first step can be achieved through running a powerful and holistic narrative-building campaign; a whole of nation and whole-of-government approach must be designed among and between the elements of the Clausewitz Trinity.
  2. The second step can be achieved by strengthening institutional analysis.

References

Acemoglu, Daron, Ali Cheema, Asim I. Khwaja, and James A. Robinson. "Trust in State and Non-State Actors: ." *Evidence from Dispute Resolution in Pakistan*, 2019: 97.

Actors, "Non-State. *Non-State Actors.* n.d. https://www.escr-net.org/resources/non-state-actors#:~:text=Non%2Dstate%20actors%20include%20organizations,paramilitary%20and%20armed%20resistance%20groups.

Amnesty International. "Forensic Methodology Report." *How to Catch Nso Group'S Pegasus*, 2021: 83.

Andrade, Robert O., and Sung Guun Yoo. "Journal of Information Security and Applications ." *Cognitive Security: A comprehensive study of cognitive science in cyber security*, 2019: 47-67.

Bagozzi, R. P., and U. M. Dholakia. "Antecedents and purchase consequences of customer participation in small group brand communities." *International Journal of Research in Marketing*, 2006: 45 - 61.

Bin, Guo, Ding Yasan, Sun Yueheng, Ma Shuai, and Li ke. "The Mass, Fake News, and Cognition Security." *The Mass, Fake News, and Cognition Security*, 2019: 11.

Brikse, Inta. "The Role of Media in Society: A Critical Discourse Analysis." *The Information Environment: theoretical approaches and explanations*, 2015: 48.

Floridi, Luciano. "Semantic Conceptions of Information." *Stanford Encyclopedia of Philosophy*, 2005.

Glascott, Julia Anna. "Trinity And the Law of war." 2017.

Huang, Linan, and Quanyan Zhu. "An Introduction of System-Scientific Approaches to Cognitive Security." *An Introduction of System-Scientific Approaches to Cognitive Security*, 2023: 23.

Hutchins, Elizabeth L. Toth and Amber L. "The Role of Social Media in Strategic Communication." *Journal of Strategic Communication*, 2013.

Johnson, Brian David, Alida Draudt, Jason C. Brown, and Lieutenant Colonel Robert J. Ross. "INFORMATION WARFARE AND THE FUTURE OF CONFLICT." *Threatcasting*, 2019: 208.

Khan, Khurshid. "Understanding Information Warfare and its relevance to Pakistan." *Understanding Information Warfare and its relevance to Pakistan*, 2011: 22.

Libicki, Martin C. "What is information warfare?" *Center for Advanced Concepts and Technology Institute for National Strategic Studies*, 1995: 110.

Longely, Robert. *An intoduction to Psychological Warfare* . 12 6, 2021. https://www.thoughtco.com/psychological-warfare-definition-4151867.

Martin, and Moosely. *RAND*. 2017. https://www.rand.org/topics/psychological-warfare.html#:~:text=Psychological%20warfare%20involves%20the%20planned,and%20behavior%20of%20opposition%20groups.

Mattox, John M. "A just war approach." *The Clausewitz Trinity in information age*, 2008: 14.

Paganini, Pierluigi. "NON STATE ACTORS IN CYBERSPACE: AN ATTEMPT TO A TAXONOMIC CLASSIFICATION, ROLE, IMPACT AND RELATIONS WITH ASTATE'S SOCIO-ECONOMIC STRUCTURE." *CCSSII*, 2022: 5-6.

Press, USAWC. "South Asia in 2020: Future Strategic Balances and Alliances." In *Strategic Culture*, by USAWC PRESS, 490. Michael R. Chambers Dr., 2002.

Ronfeldt, John Arquilla and David. "Networks and Netwars: The Future of Terror, Crime, and Militancy." In *THE ADVENT OF NETWAR (REVISITED)*, by John Arquilla and David Ronfeldt, 26. 2000.

Searle, John Rogers. "Expression and Meaning: Studies in the Theory of Speech Acts." *Cambridge University Press*, 1979: 59-61.

Smith, Peter Wilfred Hesling. "Speech Act Theory, Discourse Structure and Indirect Speech Acts." 1991: 245.

Techslang. *What is Cognitive Security?* 3 7, 2022. https://www.techslang.com/definition/what-is-cognitive-security/.

Tenny, Steven, Janelle M. Brannan, and Grace D. Brannan. "Qualitative Study." In *Qualitative Study*, by Steven Tenny, Janelle M. Brannan and Grace D. Brannan. StatPearls Publishing LLC, 2022.

Waltzman, Rand. "Weaponization of Information." *The need of COGSEC*, 2017: 10.