WEAPONISATION OF SOCIAL MEDIA: A THREAT TO PAKISTAN'S NATIONAL SECURITY

Sajjad Hussain Awan*

Abstract

As the world progresses and develops in terms of economy, military, and technology, so do the battlegrounds of warfare. Information warfare has recently gained an unusual criticality through multiple instruments. One of these instruments is the social media platforms. It is being weaponised by certain quarters to undermine the country's peace, stability and progress. Weaponisation of social media means using and abusing social media data, involving wrong interpretation, spinning the information, and manipulating the facts against the state and society to deteriorate social cohesion, political stability, and economic progress. The resultant vectors of this, if not addressed, are unending propaganda, polarised society, radicalisation, extremist orientation and a protracted cycle of internal instability and even violence. Therefore, a combination of kinetic and non-kinetic means with social media as the key enabler of Fifth Generation Warfare is unfolding in a complex manner owing to hostile actors such as India, Tehrik-Taliban-Pakistan (TTP), BLA and others. Moreover, unfortunately, the country's political leadership is not manifesting the required political maturity to counter the situation's potential challenges. The paper seeks to deconstruct the linkage of social media and Pakistan's national security by identifying the gaps in the policies regarding infrastructure and implementation, which are the significant findings. The paper employed qualitative thematic analysis methodology with secondary data sources and grounded on Social Constructivism and Securitization Theories by triangulating the collected data.

Keywords: Social Media, 5th Generation Warfare, National Security of Pakistan

Introduction

In contemporary times, many countries such as the USA, China, Australia, France, Germany, the European Union, the Kingdom of Saudi Arabia, Singapore and India began to realise the criticality of social media. They started to take necessary measures to regulate the cyber domain of national security.[1] However, the case of some countries like Pakistan has been different even though the significant portion of the population of our country has increasingly been comprised of youth. The decision-making bodies in Pakistan could not anticipate the information revolution's potential gravity and therefore kept ignoring the need to formulate a holistic mechanism to deal with the potential threats.

*Mr Sajjad Hussain Awan is a retired Air Commodore from Pakistan air force. Owing to his meritorious services, the Air Officer was awarded sitara-e-Imtiaz by the government of Pakistan. He remained in service for more than three decades as a fighter pilot and currently serving at National Aerospace Science Technology Park (NASTP), Rawalpindi. The authors' email address is sajjad.hussain.awan@gmail.com

It is important to mention here that almost every technological revolution brought potential costs that used to demand precautionary and proactive measures to deal with the negative aspect and unintended consequences. In connection to Pakistan, no precautionary measures have been taken into account by previous governments to deal with this issue and take the information revolution for granted. Resultantly, the threat has gone unnoticed.

According to Sun Tzu, a renowned strategist of China, knowing your enemy means knowing yourself, and you will never be in peril in a hundred battles.[2] The timeless wisdom of Sun Tzu suggests that knowing the strengths and weaknesses of the enemy is a necessary condition to maintain peace and stability. In this regard, the information domain has emerged as the forefront of contemporary warfare. In other words, weaponisation of the information domain or social media has become an enabler of exploiting the existing fault lines or even may generate new fault lines. Weaponising of social media means to use or abuse the information in order to get the desired outcomes that pose threats to national security in the form of spreading hate speech, proliferation of fake news, spinning the information and cyber-attacks. The consistent and incessant campaign may result in a widened gap of mistrust and distrust between certain groups and the state. This situation could generate and amplify the anti-state narrative without a comprehensive regulating mechanism. About Pakistan, the social media platforms have turned against the state in two-fold manner. The first is related to the absence of a regulating mechanism, and the second is related to existing fault lines in unaddressed issues such as terrorism, downtrodden economic conditions, sub-nationalism and antagonistic civil-military relations. Though the state has taken some initiatives, such as the National Security Policy, the National Cybersecurity Policy, and a few others, the lack of proper implementation has left the space for social media manipulation.

Similarly, information warfare through the weapon of social media is an act attacking the adversary's information system that causes confusion and fear simultaneously as it blurs the vision of the masses by the assistance of manipulative techniques. The proliferation and propagation of misinformation, disinformation and fake news are the standard stratagems of fifth generation warfare. Apart from many other essentials, fifth generation warfare involves the massive use and abuse of the information domain to out-power the enemy. Martin Libicki counted seven types of information warfare. These include economic information warfare (EIW), command-and-control warfare (C2W), intelligence-based warfare (IBW), electronic warfare (EW), hacker warfare, psychological warfare (PSYW) and cyber warfare.

Nevertheless, if taken together in an organised manner, they are bound to be part and parcel of fifth generation warfare that poses profound implications for the national security architecture of a particular state.[3]

Social media (SM) has evolved since its inception, especially in the last decade, which has altered how information, communication, connectivity, and news are conceived, presented, and perceived.[4] Thus, exposing information, state institutions, and national security matters related to the masses, the state, and non-state actors impact human security. Consequently, SM has emerged as both an enabler for 5th Generation Warfare (5GW)[5] and a significant challenge to the country's national security. Unlike traditional warfare, 5GW leverages digital dominion, psychological manipulation, and information warfare to influence societies and states. Hence, SM provides an ideal platform to internal and external anti-state actors to spread their desired narratives to cause subversion, fuel anti-state sentiments and discredit its institutions, stimulating multifaceted challenges such as polarisation, extremism and terrorism to national security.[6] Nations across the globe face this menace, especially those with weak digital governance like Pakistan.

Therefore, the paper has investigated the following queries in pursuit of holistic understanding of the aforementioned complexities.

- The first and foremost question in this regard is to interrogate linkage of Social Media (SM) and 5th Generation Warfare (5th GW).
- Second question before the study is to map the Social Media landscape of Pakistan.[7]
- In third place, another area of concern is exploring the key challenges SM poses to National Security and the country's existing Regulatory Framework.
- Last, what pragmatic remedies should be created to tackle this critical issue?

Against this backdrop, the notion of security has been changed from the traditional conception of security that emphasises the military aspect. In contrast, the new security concept is not solely dependent on the military. For this reason, social media as one of the non-traditional security aspects is becoming more critical. That is to say, security is now restricted not only to the protection of the country's territorial integrity but also to the protection and defence of other non-traditional aspects of security such as cyberspace. Over time, different schools of thought advanced multiple abstractions and theoretical rationales to define national security.

Taking this evolution of national security, the study argues that the conception of national security is dynamic and evolving. By the same token, Pakistan's national security is limited to pure military aspect and digital or social media platform protection.

Methodology

The paper is grounded in qualitative methodology. For this purpose, qualitative thematic analysis has been selected to interpret the data. The paper relies on secondary data sources such as books, research articles, research reports, official documents and news articles from credible platforms. Contextually, qualitative and quantitative forms of data have been collected while analysing the themes of this research. Nonetheless, a deductive approach has been employed, where related data has initially been explored based on the research questions and objectives set in advance. Subsequently, correlation of social media platforms, manipulation and development of narratives are incorporated. To evaluate this research, the thematic analysis technique was employed to explain various perspectives regarding social media and its linkages with national security by using relevant data from the reviewed literature. Consequently, themes relating to national security and social media complexities have been extracted and analysed.

Theoretical Framework

As for the theoretical relevance of this paper, this research paper incorporated the theory of securitisation and social constructivism in the context of Fifth Generation Warfare to examine the dangers emanating from the abuse or harmful use of social media and its implications for Pakistan's national security. The securitisation theory postulates that a society or nation securitises itself through the speech acts of leaders who disseminate information that involves threats. Thus, this should be securitised to secure both masses and the state. Moreover, Ole Weaver[8] argues that the start and development of securitisation are the consequence of the dynamics of social construction that are proliferated to generate a specific type of frame of reference to achieve a particular perception. Since social media plays a critical role in generating and constructing perception of a phenomenon to further embed in collective social behaviour, the construction of threat perception through manipulation of narratives and discourses by social media algorithms. Accordingly, anti-state elements are heavily using social media platforms to malign and to target the state through increasingly negative perception.[9] On the other hand, from Pakistan's perspective, an equal or more excellent social construction is necessary to deal with the issue.

In this regard, one way of dealing with it is through positive construction by educating the masses through speech acts of socio-political leadership and shunning those accounts disseminating false construction through best practices to deal with the issue.[10] The paper's recommendations are incorporated in the above context to address this concern.

Linkage of Social Media and 5th Generation Warfare: An Appraisal

Fifth Generation Warfare (5th GW) involves the domains of information & cyber while minimising or avoiding the use of conventional military systems, aiming at achieving small objectives through hacking, medium objectives through terrorist activities and strategic objectives like regime change.[11] Since the advent of the 21st century, which is heavily engulfed by an unprecedented flow of information, narratives and discourses are being considerably created and manipulated through the proliferation of false and unverified information. In this construct, social media platforms have become the master tool and prime enabler as well as weapon of choice with a hostile state and the anti-state actors. It has been observed that almost every aspect of life is being heavily shaped by the use and abuse of social media platforms, as the numerical strength of social media users is rapidly increasing, if not exponentially. With the growing technological advancement, the nature and character of warfare are also in transition, whereby the information domain of warfare is gaining unprecedented significance. Thus, social media's gradual weaponisation to haunt the national security architecture has become the order of contemporary times.

a. **Key Attributes**

Specific attributes of social media in this regard must be described here. For instance, social media platforms have unparalleled global outreach that has transformed how people connect, share information, and engage across borders, creating a truly interconnected and interdependent world. On the other hand, they also involve psychological connection in the form of mass addiction due to low cost and ubiquitous aspect, where every individual with a smartphone is the recipient of uninterrupted information. Moreover, using specific algorithms and artificial intelligence has created 'Echo Chambers'[12] to target audiences. Furthermore, these platforms are available at a negligible cost with high yield as dissemination of information on social media platforms becomes global in moments and millions of people can reach viewership in very little time. Another attribute is information manipulation by social media to influence the cognitive domain and induce behavioral change.[13]

Finally, the relevance and application of information manipulation is being operated in the grey zone with plausible deniability, beyond international laws or established journalistic rules.

b. **Social Media: An Enabler for 5th GW**

Due to its attributes, social media is the most agile enabler of 5th generation warfare. The key attributes given above make SM a perfect instrument available to the opposing forces to conduct subversion, polarisation and radicalisation operations targeting core values of any society/nation in pursuance of one's national objectives without attribution and a physical battle. The attributes such as global reach, ubiquitous speed, concentration, and flow through manipulation of information heavily influence and shape the opinion of masses, which follow the path of action accordingly. In this manner, the frequency of social media as an enabler of 5th generation of warfare has increased manifold.

Social Media Mapping of Pakistan

The magnitude and extent of social media usage in Pakistan are significant in estimating its impacts.[14] The greater the number of social media users, the higher the impact of social media would be. The extent of its reach is dependent on its users. According to PTA, there are 54.18% broadband users in Pakistan.[15] The nationwide percentage of important social media users is as follows. At the first place, the number one social media in Pakistan is Facebook. It occupies 48.12% of users in the social media space. It is followed by WhatsApp, which has an occupancy space of about 24.97%. In third place, Twitter/X/ X is at 2.37%.[16] Twitter/X/, despite occupying slightly above 2% of users, Twitter/X/has a profound impact on perception management and the spread of propaganda. Additionally, during the year 2021-22, nation-wide 72.9 million active social media users were recorded with annual growth rate of 4.3%, representing 31.5% of the total population.[17] While the population between 25 and 54 years is 34.7% of the total population of Pakistan[18], that matters the most in perception management and political affairs of any society, indicative of the societal interconnectedness almost in entirety.[19] Though not all social media users are involved in anti-state narratives, a certain percentage with varying degrees are involved in the said activities. It is important to mention here that the data or information created by the users remains present and gets concentrated over the period if not addressed.

Challenges Posed by Social Media to National Security

Unlike in previous times, the growing significance of cyberspace in the context of social media users is posing critical challenges to the country's national security.[20] In other words, physical territory used to be critical for a state's national security; however, the criticality of virtual space has increased manifold in the information age. The country's cyberspace or virtual space is as important as physical space. Given the context, the important challenges posed by social media to the national security of Pakistan mentioned and explained in the following paragraphs;

a. The first and foremost challenge social media poses to the country's national security is political instability. Triggering political instability and polarisation through false propaganda against government policies and generating negative perceptions are causing panic, mistrust, and confusion between people and the state and amongst state institutions, impacting the nation's and state institutions' morale. Radicalisation, polarisation, sectarianism, extremism and terrorism are the natural consequences of these hostile social media activities. For instance, sectarian hate speech by the religious leadership of TLP and others.[21] It has been observed in the collected data that many of the terrorist outfits are using the social media platform for promoting their narratives and even recruiting. Sub-nationalists in Baluchistan, such as the BLA and the BLF, are also using X (former Twitter) against the government and state institutions to weaken the social fabric and national integration. Generating anti-state sentiments, hatred against ideology, maligning state institutions, proliferating chaotic emotions and inciting violence through fake news, false propaganda, news spinning and concerted disinformation campaigns are attributes of the social media abuse pattern.[22]

   In 2020, the Economist reported that 81 countries waged "organised disinformation campaigns."[23] It is rightly observed that by the former Chief of Army Staff (COAS) "We are facing the challenge that has been imposed on us in the form of the fifth generation or hybrid war. Its purpose is to discredit the country and its defense forces and spread chaos", he said. "We are well aware of this danger. We will surely win this war with the nation's cooperation."[24]

b. The country's economy is another critical target of negative social media campaigns. Disrupting economic activity through the spread of fake news, propaganda, disinformation, and misinformation adversely distresses the

business environment and impinges upon FDI, trade, and corporate activities.

One of the recent reasons behind low Foreign Direct Investment (FDI) is yet another testimony as the economic disruption is disguising the pivot of fifth generation warfare. Therefore, the eventual objective for non-state actors and hostile agencies is to weaken the economic pace of growth so that this could trigger an anarchic situation in the country.[25] Furthermore, according to General Zubair Mahmood Hayat, "Indian spy agency RAW had established a cell in 2015 being executed from Afghanistan dedicated to sabotage CPEC projects in Pakistan."[26] In addition, propaganda campaign against nuclear weapons of the country, targeting armed forces of Pakistan, hybrid warfare by foreign hostile agencies, efforts to undermine Pakistan's position related to Financial Action Task Force (FATF) and propagating the separatist narrative of sub-nationals in Baluchistan are other manifestations.[27]

To materialise their nefarious designs, the typical pattern and tools are doctored images, fake news, orchestrated campaigns, misinformation, disinformation, anti-state narrative, propaganda, and manipulative perception management; undermining the credibility of state and its institutions aim to accomplish the following: manipulating public opinion, sometimes even the intellectuals, societal polarisation, dissemination of radical ideologies, recruitment and mobilisation, violence and acts of terrorism, cyber espionage, intelligence gathering and cyber-attacks to target digital infrastructure and sensitive installations.[28] The whole exercise is to tarnish the social fabric, undermine national integration through political instability, and disrupt the economy through harmful use of social media.

Existing Regulatory Framework

Before we proceed to pragmatic solutions or recommendations, it would be plausible to include and examine the existing regulatory framework regarding the management of security situations relating to the use of social media. Many policies have been introduced and employed in a partial manner that could not bring the desired result for the betterment of the country's security situation. The role of certain documents, institutions, and organisations, such as the Ministry of Information, the Pakistan Telecommunication Authority, and the National Security Policy, has also been of critical importance.[29] The important components of the existing regulatory framework are given below:-

a. The most important component in this regard is National Security Policy. National Internal Security Policy[30] formulated to counter online threats to national security, proposing severe punishment for propagating terrorism and extremism. However, it could not be executed owing to the absence of political will in policy implementation.[31] A better formulated policy than NISP-2014 proposed implementing a national cyber security strategy through civil-military collaboration to oversee the regulations of SMNs with the aid of the PTA.[32] It was undermined, questioning its legitimacy based on its approval on the last cabinet meeting of the last government on the last day in office. The policy has been viewed as more about point scoring than addressing core internal security issues.[33] In this regard, National Security Policy (NSP)-2022[34] has identified hybrid war as a threat to national security, explicitly using SMNs as a tool. However, its implementation is awaited.

b. Second is the National Action Plan. Though the 14th point of the National Action Plan-2014 and Point No 2 of Revised NAP-2021 aimed to regulate social media, the law-making remains to be seen. It seeks to address the growing disinformation and propaganda campaigns through social media trickery.

c. Thirdly, the Prevention of Electronic Crime Act (PECA)-2016 was introduced. However, it was more related to issues of public concern like online harassment, sexual content, intellectual property stealing, financial scams, and hacking. The act could not be implemented in its essence, being vague, drafted poorly, and violating articles four and 10-A of the Constitution of Pakistan.[35]

d. Fourthly, according to the Citizen Protection Rules (CPR)-2020, all social media networks were to open an office in Islamabad and a focal person to address complaints from citizens and the state. However, SMNs' compliance with these rules and establishment of SM offices have yet to be seen.[36]

Moreover, the existing legal framework struggles to effectively regulate anti-state SM content based on mal-intentions and holding accountability for those misusing the platforms. Defamation Law 2002 is redundant, and PECA-2016 needs a remodeling, especially regarding articles four and 10-A of the Constitution of Pakistan; efforts were made to upgrade it in 2021 and 22, which Parliament/IHC nullified. Another instance is the non-availability of legislation by parliament to implement the law of land on social media applications through certifications.

Moreover, Paradoxical legislation, non-aligning national laws on social media with international standards on freedom of expression adds complexity to regulatory efforts.[37]

Furthermore, lack of automated tools and algorithms and a heavy reliance on manual or human-based social media monitoring renders our monitoring mechanism virtually ineffective. The role of social media algorithms played extremely negative roles in technologically advanced countries, such as the presidential elections of the USA in 2016 and the Brexit episode. In the said events, the hostile agencies selected the target audience and the impacted masses' opinion during the election campaign and the referendum. The Russian and Chinese elements were alleged after the investigation conducted in the affected countries.[38]

Additionally, the absence of a national firewall hampers the country's influence and oversight while exposing it to external threats and anti-state social media campaigns. Pakistan is far behind in its national protection framework and a specific mechanism like a digital firewall that could filter menaces like propaganda and nefarious campaigns. Social media is outpacing regulatory frameworks and oversight mechanisms, making it difficult for authorities to monitor and control the spread of manipulated information that directly threatens national cohesion, human security, and thus national security.

Recommendations

Formulation of adaptable and flexible comprehensive national policy identifying threats, weaknesses and evolving trends to preempt emerging challenges is needed based on monitoring, countering disinformation/misinformation, protecting critical infrastructure, enhancing cybersecurity and capacity building. Suggested policy guidelines and relevant contours are as under:-

The foremost step in this regard is proactive social media monitoring, which involves specialised tools like Artificial Intelligence (AI) to track keywords, hashtags, and mentions across various platforms, analyze sentiment, engage with the audience, and respond promptly to mentions while ensuring compliance with privacy and legal regulations.

At the second place, promote media literacy and digital citizenship education through education institutions, organising workshops & seminars (with current and actual examples of SM anti-state contents based on mal-intention) and print/ electronic media to empower citizens to critically assess information on social media and navigate online spaces responsibly.

The Singapore approach can be adopted as per Pakistan's SM environmental dictates. Australia's "It Stops with Me[39]" campaign encourages community members to report suspicious online activities and engage with law enforcement agencies to prevent extremist activities.[40]

Besides, public-private partnerships foster collaboration with social media companies, technology firms, civil society organisations, and academia to develop and implement solutions collectively to address social media-related security challenges. Similarly, engage in international cooperation and diplomacy, especially with China, through agreements, memorandums, and intelligence exchange programs to counter cross-border threats from social media, including disinformation campaigns and cyberattacks. The Chinese model of local SM platforms (like WeChat) constraining external influences may be studied.[41]

On the other hand, invest in strengthening national cybersecurity capabilities to protect critical infrastructure and sensitive data from cyber threats on social media platforms. Israel, known for its robust cybersecurity measures, has developed a thriving ecosystem of cybersecurity startups[42] and research institutions. These efforts have strengthened the country's ability to defend against cyber threats.

Nevertheless, constantly assessing social media-related threats to national security should prioritise them based on risk assessments, and allocate resources accordingly. After resource allocation, advanced technological means such as use of artificial intelligence to meet the challenges are crucial in this context. More specifically, there is a dire need for a national data protection policy that should be protected and defended through multiple digital protective layers. In addition, the dissemination of narratives having anti-state and against the state institutions impressions is on the rise by certain social media platforms of political parties, which needs to be dealt with through strict implementation of the aforementioned regulating policies.

Promoting a national security culture is another significant area, emphasising individual and collective responsibility for safeguarding the nation's security interests online and offline. The United Arab Emirates established the Hedayah Center[43], which focuses on countering violent extremism and promoting tolerance through various initiatives, including online campaigns that challenge extremist narratives. In this bargain, an evaluation framework should be institutionalised to assess the effectiveness of social media security strategies and adjust them based on lessons learned and emerging threats.

Germany has enacted the NetzDG law, requiring social media platforms to remove hate speech and illegal content within 24 hours or face significant fines.[44] This legislation encourages social media companies to take a proactive role in countering harmful content.[45]

Implementing existing regulatory framework with the aforementioned modifications in line with emerging challenges (aligning with international norms) could hold social media companies accountable for content moderation, data privacy, and cooperation with law enforcement while respecting free speech and privacy rights. The UK's Counter-Terrorism and Border Security Act[46] includes provisions to combat online radicalisation by making viewing or streaming extremist content illegal. This legislation aims to deter individuals from engaging with extremist material online. In this regard, the Ministry of Information & Broadcast (MoIB) should promote startups on their social media platforms through Ignite Fund (medium to long term). As a short-term measure, Chinese social media platforms (WeChat & TikTok) may be promoted (in the event of a ban over WhatsApp & YouTube over non-compliance). MoIB should conduct a feasibility study to acquire expertise for establishing its own 'National Firewall' from China (in short to medium term), while benefiting from their experience of 'Great Firewall'.[47]

Addressing inadequacies of PTA, FIA and other related agencies through legislation, capacity building and institutional restructuring/ reforms, completing workforce inadequacies, addressing the shortage of specialists' pool, consumer protection, international collaboration to remove disrespectful content, etc. Moreover, "Global Internet Forum to Counter Terrorism (GIFCT)"[48] has developed a shared database to create 'digital fingerprints of terrorist content'. The Government of Pakistan should engage in this context with this forum to prevent SM exploitation.

Conclusion

The weaponisation of social media platforms is a war of information and perception that is being waged against the country's national security apparatus. With its global outreach, social media has proven to be an effective enabler to affect and manipulate human minds, posing multiple challenges in national security. Nations enjoying territorial protection, at times don't even realise being targeted with information warfare, which is creating a divide between the state and its citizens, disturbing strands of national security. To cope with the challenges posed by social media to national security, the state and its institutions should adopt a proactive approach to develop policies and strategies for monitoring social media platforms, countering disinformation, developing critical advanced digital infrastructure and enhancing cybersecurity to safeguard national digital frontiers.

Although the state has recently taken some initiatives from legislation to policy formulation, there are gaps in implementing those policies. This type of gap has remained business as usual regarding strict implementation of the National Action Plan and NACTA. On the other hand, there is a need for constant engagement of youth and credible members of the intelligentsia and socio-politico leadership to sensitise and inform the youth regarding information warfare. Last but not least, communication gap between the country's leadership and the public, smooth flow of the political process, employment opportunities and speedy justice should go hand in hand for long-term results.

Endnotes

[1] Ang, Peng Hwa. "How Countries Are Regulating Internet Content." *Nanyang Technological University, Singapore*, January 3, 2016.

[2] aud, Adam, and Neha Kazim. "Disinformation and Propaganda Tactics: Impact of Indian Information Warfare on Pakistan." *The Beacon Journal* 2, no. 1 (2021-2022): 6-27. ISSN: 2616-7743.

[3] Saud, Adam, and Neha Kazim. "Disinformation and Propaganda Tactics: Impact of Indian Information Warfare on Pakistan." *The Beacon Journal* 2, no. 1 (2021-2022): 6-27. ISSN: 2616-7743

[4] Boyd, Donah M., and Nicole B. Ellison. "Social Networking Sites: Definition, History, and Scholarship." *Journal of Computer-Mediated Communication* 13 (2008): 210-230

[5] Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, February 1999.

[6] Ariel, Yaron, and Ruth Avidar. "Information, Interactivity, and Social Media." *Atlantic Journal of Communication* 23 (2015): 19-28.

[7] Asim, Muhammad, and Hashmat Ali. "Impact of Social Media on National Security in the Face of Globalization: Pakistan's Perspective." *Pakistan Journal of International Affairs* 2, no. 1 (2019): 1-25.

[8] Buzan, Barry, and Ole Wæver. "Liberalism and Security: The Contradictions of the Liberal Leviathan." *Copenhagen Peace Research Institute*, April 1998.

[9] Kirshner, Jonathan. "Globalization and National Security." In *Globalization and National Security*, edited by Jonathan Kirshner, 1-35. New York & London: Routledge, 2006.

[10] Hamourtziadou, Lily. "Security Challenges of the 21st Century: New Challenges and Perspectives." *Journal of Global Faultlines* 6, no. 2 (2020): 121.

[11] Ibid p-46

[12] An environment where a person only encounters info or opinions that reflect or reinforce his own

[13] Biały, Beata. "Social Media—From Social Exchange to Battlefield." *The Cyber Defense Review* 2, no. 2 (2017): 75.

[14] Khan, Muhammad Khalil, and Cornelius P. Pratt. "Strategic Communications: The Pakistan Military's Use of Social Media Against Terrorism." *Media, War & Conflict* (2020): 1-36.

[15] PTA

[16] Ibid

[17] Al Abd, Saad. "National Security and Its Linkage with Social Media: Lessons for Pakistan." *JSSA* Vol. VIII, No. 2 (2023): 80-103. .

[18] Ibid

[19] Hassan, Kiran. "Social Media, Media Freedom, and Pakistan's War on Terror." *The Commonwealth Journal of International Affairs* (2018): 3.

[20] Erbschloe, Social Media Warfare; Bialy, "Social Exchange to Battlefield;" Bhosale and Bhange, "Understanding Social Media Tools."

[21] Basit, Abdul. "Barelvi Political Activism and Religious Mobilization in Pakistan: The Case of Tehreek-e-Labaik Pakistan (TLP)." *Politics, Religion & Ideology* 21, no. 3 (2020): 374-389.
[22] "The News." "Social Media Rife with Anti-State Propaganda: COAS." *The News*, December 30, 2023.
[23] "The Economist." "A Growing Number of Governments Are Spreading Disinformation Online." *The Economist*, January 13, 2021.
[24] Yasin, A. "Army Will Win Hybrid War with Nation's Help: Bajwa." *Dawn*, September 7, 2020.
[25] Al Abd, Saad. "National Security and Its Linkage with Social Media: Lessons for Pakistan." *JSSA* Vol. VIII, No. 2 (2023): 80-103.
[26] "Dawn." "RAW Running $500 Million Cell to Sabotage CPEC," Says Gen Zubair Hayat. *Dawn*, November 14, 2017
[27] Nadeem, Muhammad Ashraf, Dr. Ghulam Mustafa, and Dr. Allauddin Kakar. "Fifth Generation Warfare and Its Challenges to Pakistan." *Pak. Journal of International Affairs* 4, no. 1 (2021)
[28] Khan, Hamid (Almashriqi). "Critical Study of Propaganda & Hybrid/5th Generation War for the Purpose of Narrative Building."
[29] Rafiq, Amna. "Challenges of Securitizing Cyberspace in Pakistan." *Strategic Studies* 39, no. 1 (2019): 90-101.
[30] National Security Policy of Pakistan (NISP)
[31] Ihsan Ghani, Pakistan Response to Extremism and Terrorism
[32] Al Abd, Saad. "National Security and Its Linkage with Social Media: Lessons for Pakistan." *JSSA* Vol. VIII, No. 2 (2023): 80-103.
[33] Ihsan Ghani, Pakistan Response to Extremism and Terrorism
[34] NSP 2022-2026
[35] Khan, Easha Arshad. *The Prevention of Electronic Crimes Act 2016: An Analysis*.
[36] Al Abd, Saad. "National Security and Its Linkage with Social Media: Lessons for Pakistan." *JSSA* Vol. VIII, No. 2 (2023): 80-103.
[37] Shaheen, Salma. "Fake News, Escalation, and Polarization: Pakistan's Disinformation Vulnerabilities." *South Asian Voices*, May 12, 2022.
[38] Yerlikaya, Turgay, and Seca Toker Aslan. "Social Media and Fake News in the Post-Truth Era: The Manipulation of Politics in the Election Process." *Insight Turkey* 22, no. 2 (2020): 177-196.
[39] "New Racism. It Stops with Me Campaign." *Australian Human Rights Commission*..
[40] Al Abd, Saad. "National Security and Its Linkage with Social Media: Lessons for Pakistan." *JSSA* Vol. VIII, No. 2 (2023): 80-103.
[41] erlikaya, Turgay, and Seca Toker Aslan. "Social Media and Fake News in the Post-Truth Era: The Manipulation of Politics in the Election Process." *Insight Turkey* 22, no. 2 (2020): 177-196.
[42] Centers for Countering Extremism." Government of the United Arab Emirates. Accessed from https://u.ae/en/about-the-uae/culture/tolerance/centers-for-countering-extremism/.
[43] Centers for Countering Extremism." *Government of the United Arab Emirates*.
[44] Lahoti, Sugandha. "Facebook Fined $2.3 Million by Germany for Providing Incomplete Information About Hate Speech Content." Published July 3, 2019.
[45] Al Abd, Saad. "National Security and Its Linkage with Social Media: Lessons for Pakistan." *JSSA* Vol. VIII, No. 2 (2023): 80-103.
[46] "Bills - UK Parliament." *UK Parliament*. Accessed [Date you accessed the document].
[47] Shen, Fei. "Great Firewall of China." In *Encyclopedia of Social Media and Politics*, edited by Kathy Harvey, Vol. 2, 599-602. SAGE, 2014.
[48] Global Internet Forum to Counter Terrorism (GIFCT). *Research and Terrorism*. Accessed September 24, 2023.