INFORMATION WARFARE AND TWITTER: A NEXUS OF INDIAN SHADOW NETWORKS ON BALOCHISTAN ISSUE

Ms Ayesha Chaudhary, Dr Zeeshan Zaighum, Mr Rana Faizan Ali[*]

Abstract

Owing to its several fault lines, Pakistan is one of the target countries of Fifth-Generation Hybrid Warfare (5GHW) attacks. These attacks are conducted by adversaries, both external and internal, more readily targeting the Balochistan province of the country, which is inhabited by a plethora of non-state actors and violent non-state actors. External adversarial powers seek to create shadow organisations to subvert the state through information operations. The paper aims to study shadow organisations subverting the state through information operations. It seeks to identify the shadow organisations in the digital security environment of Pakistan, followed by the exploration of the tactics employed by these organisations to disseminate content effectively, identify the themes used by these organisations in their textual content, and check the level of bot activity in the digital presence of these shadow organisations. The paper's findings placed the shadow organisations in the hashtag Balochistan Is Not Pakistan dataset. It identified the employment of the tactics (hashtags, mentions, retweets, bot activity) connecting shadow organisations, state-recognized terrorist organisations, and external adversarial countries, i.e., India. Furthermore, the themes identified in the dataset identified the frequency of employment, solidifying the assumption that the end goal is state subversion.

Keywords: Information Warfare, Shadow Organizations, Fifth-Generation Hybrid Warfare, State Subversion. Social Media

Introduction

Pakitan enjoys a robust geopolitical position that continually elevates it to the position of constructive participant at the regional and global levels. Numerous elements, including its strategic geographic location, nuclear power, close relationship with China and the creation of the China-Pakistan Economic Corridor (CPEC), have been cited as reasons for Pakistan's importance among significant nations. However, as foreign intelligence services use strategies to conduct disruptive warfare against the country, Pakistan faces the difficulties of contemporary warfare today. Pakistan's adversaries use hybrid warfare strategies that attack internal security to cause turmoil and confusion throughout the nation. The nation's internal security is being targeted by enemies who use electronic, print and social media, as well as unhappy individuals and non-governmental organisations (NGOs) as weapons for (5GHW). These adversarial forces actively participate in fostering

[*]Ms. Ayesha Chaudhary is a Researcher at School of Media and Mass Communication, Beaconhouse National University (BNU), Lahore. Dr. Zeeshan Zaighum and Mr. Rana Faizan Ali are Assistant Professors at School of Media and Mass Communication, Beaconhouse National University (BNU), Lahore.

sectarianism in Pakistani society. The results of this fifth-generation warfare, which Pakistan's enemies are waging against it, include social unrest, ethnic and sectarian divides, Pakistan's brand being tarnished internationally, economic instability and a host of other negative impacts.

The case study of propaganda campaigns against Pakistan's possession of nuclear assets makes way for the debate that because Pakistan is a responsible nuclear state, the use of kinetic combat options against Pakistan, especially in the case of India, has gone down tremendously due to Pakistan's deterrence of India's hostile intentions by it being a nuclear state which leaves its adversary with the option of indirect warfare to subvert the state. Simultaneously, one of the biggest targets of Indian propaganda campaigns has been Pakistan's military. Pakistan's enemies frequently accuse the Army and the Inter-Services Intelligence (ISI) of supporting non-state entities and engaging in regional hostilities. Notably, India continually holds the Pakistani Army and ISI responsible for any insurgent occurrences that take place within the Indian Illegally Occupied Jammu and Kashmir (IIOJK) under the Indian administration. India is using this as a strategic manoeuvre to hide its own human rights abuses in IIOJK and its provocative actions in Pakistan's Balochistan region.[1]

Foreign media has constantly shown prejudice towards Pakistan, neglecting to recognise and emphasise the great sacrifices made by Pakistan in its battle against terrorism. The United States has deliberately targeted Pakistan while cooperating with India and Israel because they see Pakistan's Army as a significant barrier to their foreign policy goals. As a result, the Pakistani military is under constant attack from several directions.[2] In Khyber Pakhtunkhwa, hybrid warfare strategies are being used, and Pakistan is being courted to become involved in the unrest in the Balochistan province.[3]

When viewing the combat situations in retrospect, it can be claimed that India has long favoured hybrid warfare to achieve its objectives. Since the creation of its intelligence organisation, the Research and Analysis Wing (RAW), it has consistently carried out subversive activities against Pakistan. RAW's interference in Pakistan caused internal heresy, which started soon after being founded in 1968.[4] Notably, in the 1970s, RAW masterminded the formation of the terrorist group Mukti Bahini to capitalise on political turmoil in the west wing of Pakistan, which led to the division of Pakistan. This organisation, which committed atrocious actions against the Pakistan Army, innocent bystanders, and the families of the armed forces, was actively trained, financed, and nurtured by RAW. RAW has consistently carried out covert operations against Pakistan since that time.[5] India maintains a twofold approach towards Pakistan in its pursuit of covert goals. First, it uses

diplomatic strategies to isolate Pakistan by erroneously ascribing its name to terrorism. Second, it encourages and supports terrorist activities on Pakistani soil, meddling in Pakistan's domestic affairs. To promote its own foreign policy goals, India frequently uses a variety of techniques to degrade Pakistan's standing in the international community.[6]

Interestingly, Pakistan is an ideal petri dish where indirect warfare can be cultured mainly because of the abundance of the elements that harbour indirect warfare. Firstly, Pakistan has an abundance of non-state actors (NSA) that exist within its geographical boundary, and this plethora of NSAs have been engaged in low-scale and high-scale insurgent activities, especially since 2001. Baloch Liberation Army, Tehreek-e-Taliban Pakistan, Baloch National Movement and Lashkar-e-Jhangvi are some examples of the more engaged NSAs in the country. The sponsorship of these actors from external benefactors, including states, intelligence agencies and militant organisations, coupled with the Pakistani state's inability to manage its political affairs, is what has resulted in the snowballing of NSAs, which makes the country a highly prone target of indirect warfare.[7]

The universe for the study is 'Twitter', as the study analyses the tweets captured from within Twitter using NVivo under the hashtag '#Balochistan is Not Pakistan'. All tweets under the hashtag #BalochistanIsNotPakistan will represent the study population. The tweets were captured using the Google extension NCapture on 26 May 2023, so tweets posted after that will not be part of the study's population where, as the study's analysis unit will be 'text' extracted from the tweets. The text being studied will include statements within the tweets, hashtags, mentions, and all analytical properties of the accounts tweeting, including their usernames and locations.

Frictional Sea of Conflicts

Abbott provides a framework titled 'Frictional Sea of Conflicts' to visualise a fifth-generation hybrid war.[8] In this fictitious scenario, a group seeks to militarise a specific border region. However, because they are few and run the danger of being found, they exploit ongoing disputes and sway public opinion to advance their agendas. This framework includes the following components:

- **Shadow Organizations**: The group establishes two shadow organisations with opposing narratives to carry out their agenda covertly. These shadow organisations appear independent and outwardly support the government. One organisation aims to provoke and antagonise a particular population, while the other defends their

rights through information communication networks and fosters international connections in retaliation to the antagonistic.

- **Paramilitary Operations and 'Phony' Attacks**: Shadow organisations carry out paramilitary operations but avoid frontal assaults on the government. The violence against one organisation increases due to the organisation's calls for the expulsion or imprisonment of the former organisation. The former organisation's use of ICTs increases military readiness to protect its demographic.

- **Spectacular Terrorist Attack**: As a result of the increased friction, at some point, a big terrorist strike will take place. Abbott omits to describe the attack's specifics and consequences. However, this incident will increase border security and fuel calls for an immigration crackdown.

- **Unintentional Government Subversion**: The group secretly wants to subvert the US government. The group's objectives are in line with the increased border security and stricter immigration regulations implemented in the wake of the terrorist assault. As a result, the government unintentionally enacts policies that achieve the group's goals.

- **Victory of 5th Generation Warriors**: Abbott's visualisation of a successful fifth-generation war concludes by stating that the 5th Generation Warriors, represented by the group, have achieved victory without the government realising it was a war against them.

The "Frictional Sea of Conflict" can be defined as the environment created by the interplay of various actors and conflicts involved in this scenario. It represents a complex web of shadow organisations conducting covert operations and manipulating public sentiment, contributing to constant conflict and strife. This environment serves a group's purpose of achieving its objectives while evading direct attribution or recognition by the government.

Global Security Environment

Budania (2003) underlines the critical features of the global security environment and their impact on national security. He identifies geopolitical context as one of the primary components of the security environment. The author notes that the emergence of China and India as major economic powers has disrupted the energy equilibrium, which was previously situated in the West. The paper highlights military capabilities and intentions as another component of a security environment. For instance, India's security environment is directly threatened by its neighbouring

countries, Pakistan and China, which are fiscal-military states whose finances are heavily geared towards the sustenance of their military endeavours. Furthermore, insurgency within India, purported by terrorist organisations and insurgents, also poses significant security challenges for India. This challenge is further elevated by terrorist organisations like Lashkar-e-Taiba (LeT) and Jaish-e-Muhammad, who successfully demonstrated their ability to conduct strikes against India. The Mumbai Attacks of 2008 and the Pulwama Attack in 2019 serve as the prime example of their implication in terrorist attacks. Furthermore, unconventional warfare tactics like cyber-attacks have significantly impacted national security. Research reveals that cyber-attacks have recently compromised India's security of critical infrastructure and state institutions.

Indirect Warfare through Information Communication Technologies (ICTS)

Using ICTs in combat is potent and advantageous since they are practical and relatively cost-effective. This use does not come without its implications. The possible escalation in conflicts and casualties is one of the concerns associated with ICT-based warfare. Conflicts involving ICTs are white conflicts for the deploying army. The disadvantage of this benefit is that it makes war less complicated for a force that can employ these technologies, making it more convenient for governments and criminal or terrorist organisations to perpetuate ICT-based warfare globally.[9] In addition, governments must enact more stringent regulatory measures to protect their population from any covert attack as the deployment of ICT-based conflicts through civilian infrastructure has increased. However, this action could undermine privacy, anonymity, and freedom of speech and expression.[10]

Information Environment: Trend Creation and Trend Hijacking

Prier (2017) demonstrates different stakeholders' use of social media for modern-age information warfare. The author first unfolds the mechanism behind the spread of a narrative on social media. He explains the importance of the 'trend list' on social media sites like Twitter and Facebook in capturing the attention of the masses and setting agendas. Prior argues that these sites analyse hashtags, phrases, and keywords to create a list with topics sorted according to popularity amongst users. He then points out that foreign agents amplify the spread of propaganda on social media by using automatic bot accounts that insert the propaganda trend, eventually leading to greater engagement. Trend hijacking is another method used by IS to garner global attention. Likewise, during the 2014 FIFA World Cup, the hashtag #WorldCup2014 was trending globally on Twitter throughout the

championship. At one point, due to the hijacking by IS supporters and bot accounts, the majority of the tweets posted under the hashtag had content related to IS rather than soccer. They used the opportunity to market for a recruitment drive in their army and made threats of terror attacks on different tournament venues of the 2014 World Cup.[11]

Proxy Warfare

To target individuals and groups outside the geographical boundary of Syria and Iraq for terroristic operations, especially in territories where war is being waged against the Islamic State (IS), IS uses propaganda campaigns. An act of terror took place in Medan, Indonesia, in August 2016. The terrorist was a 17-year-old teenager, and the inspiration for the attack was allegedly drawn from IS's propaganda campaign on the Internet and the local police confirmed this allegation.[12]

Mumford defines proxy warfare as the engagement of external actors (state or non-state) in an existing conflict to influence its outcome.[13] While proxy warfare seems to have been the preferred combat tool since the end of World War II, this method of warfare evolved along with the changing security environment, making the variables of the security environment directly related to the alteration in the character of proxy warfare.[14] This purports that technological advancements, one of the critical elements of the security environment, directly cause proxy warfare alteration.[15]

Cyber Mode Proxy Warfare

Cronin (2020) argues that today's technology weaponises malcontent individuals and groups to act autonomously in their global intrusion, acting as proxies in different settings of power struggle and politically generated upheaval.[16] Affan discusses the effectiveness of this cyber mode of proxy warfare. He deems it adequate due to the general dependence of global masses on computer networks, making disseminating influential content highly effective. It manipulates social media users for them to become proxies by pushing them to fight against the enemies of IS. This model complicates the identification of the adversary and the battlefront, which is why IS's proxies like **Zale Thompson, Ivan Armadi Man Haron Manis,** etcetera can carry out terrorist attacks around the globe. The author believes that for IS to grow and develop outside of Iraq and Syria, it looks for a large Muslim population, a prominent Muslim millennial population, and an abundance of natural resources.[17]

State Subversion

Proxies are used to capture territories and carry out subversive activities that destabilise a state. Omand defines subversion as external interference in a country's internal affairs that aims to topple the established order on the aggressor's terms, whether by imposing a change in the government or policy. Subversion is an outside-to-inside threat involving external state stakeholders taking advantage of opportunities mainly offered by the political interior. In the last ten years, the digital medium's amplifying ability spurs a new worry about the possibility of subversive threats to be posed and carried out in cyberspace. For example, a noteworthy development could be that cyberattacks targeting vital infrastructure can be used to carry out the coercive or intimidating aspect of subversion.[18] One of the most credited examples of this phenomenon, which serves as one of the tools for digital subversion against a state, is the Russian interference in the presidential election of the United States in 2016, intending to damage the Democratic Party. The Russians gained access to the email accounts of crucial party staff members through hacking. They leaked 'dishonouring' information to influence voter opinion through social media by creating a damaging narrative.[19]

Shah, Rafique, & Butt present the India-Pakistan context to operationalise the concept of subversion. They argue that in the case of Pakistan, Muslim militant organisations inside the country have a benefactor/proxy relationship with external stakeholders, including sponsor groups and governments. They believe that the subversive activities carried out by these organisations aim to polarise the parties involved in dissent by manipulating the differences in Pakistani society. The ultimate aim of subversion remains the internal corrosion of the Pakistani state that creates an environment where the functions of the state deteriorate as a result of ineffective government operations. The study emphasises that India's interventionist strategies with subversive intent are significantly focused on the isolation of ethnic groupings through successful propaganda warfare. Traditionally, India's interventionist strategy has been shown in several ways, such as forming front organisations that infiltrate and influence different ideological groups, current political parties, and organisations. Another strategy is recruiting and using state institutions like the military, police, and other non-state actors, groups, and organisations.

Another provocative behaviour is organising civil demonstrations through strikes, agitation, and boycotts. Still, contemporary, various hybrid tactics are employed by India as a strategy to sow discord in the internal affairs of Pakistan. These strategies include cultural espionage, financial pressure, backing for local opposition organisations, disinformation campaigns, and criminal or terrorist

activity. India's employment of irregular or unmarked armies, cyber capabilities, and non-state proxies have been effective for their subversive operations. Pakistan and India's security environment has become more complicated due to the use of information and hybrid warfare as instruments for subversion, proxies, and insurgencies. The cultural invasion has evolved into the fifth generation of warfare with the emergence of digital technologies like the Internet, the World Wide Web, Darknet, digital data and social media platforms.

For years, propaganda, counterintelligence, and espionage have all exploited weaponised information. For instance, Pakistan's cultural fabric, including clothing, cuisine, and wedding trends, has been dramatically impacted by Indian television programs that are shown on Star Plus. Pakistan has become a target of Indian subversive plans and techniques, such as espionage, sponsorship, and assistance for dissident organisations, as a result of India's meddling in Pakistan's domestic affairs. The Baloch Liberation Army was funded by India to support terrorism in Balochistan and Sindh, as was made clear by the recent arrest and confession of Indian operative Kalbushan Yadav.[20] Pakistan has responded by taking counteractions to the problem. Furthermore, India's surveillance networks operating within Pakistan were revealed along with India's aim to disrupt and obstruct the China-Pakistan Economic Corridor, which is crucial for the economic prosperity of Pakistan.[21]

Indian involvement in Balochistan was justified by the Indian Prime Minister Narendra Modi and National Security Advisor Ajit Doval by using the 2008 Mumbai attacks as an excuse. However, Yadav's immediate arrest after the Security Advisor's statement led to his confession and acknowledgement of the fact that he had planned to meet with Baloch separatists to coordinate the carrying out of terrorist operations with their assistance.[22] Notably, the global flow involving proxy warfare and mass media can only be understood through 'shadow networks.' While the concept of shadow networks started as "shadow states," which characterised states with a strong presence of armed groups, it has broadened with the addition of globalisation dimensions.[23]

Shadow Networks

In her "shadow networks" theory, Nordstrom introduces a new facet to geopolitics. She highlights the growing participation of regional armed groups in transnational institutions and organisations that facilitate acquiring weapons, funding, and technologies needed to carry out their activities. Nordstrom claims that these shadow networks cover a wide variety of conduct that is not just restricted to illegal activities; instead, it takes place beyond the purview of recognised governmental institutions.[24] Rozema contends that the subversive activities of

shadow organisations are inextricably linked to global dynamics rather than being restricted to only local issues. The author believes this link is created through the worldwide dissemination of ideologies, participation in illegal global networks, and the dissemination of imaginations made possible by contemporary communication techniques. Rozema further discusses that these global ideologies impact the actors involved in warfare: the shadow network that binds the benefactor, the shadow organisation, and the mass media. The benefactor's combat strategy influences the shadow organisation's methodology, and the drive behind the perpetuation of subversive activities is a direct result of the narratives disseminated and the rhetorics employed through information operations.[25] This two-fold impact enables the state and non-state actors to control territories, people, and natural resources through alliances, participation in international economic networks, and the use of force as a result of the growth of these "shadow networks" or "non-state networks" that extend beyond war and peace."[26]

Shadow Organizations in Pakistan's Digital Security Environment

Since the hashtag under study is #BalochistanIsNotPakistan, the shadow organisations identified are individuals and groups participating in information dissemination under the selected hashtag. The identification of shadow organisations has been made based on the differentiation between the terrorist organisations and separatist groups officially recognised by the state in Balochistan and the individuals/groups involved in information dissemination under the hashtag, not recognised by the state as insurgents or militants. The list of state-recognized terrorist organisations is as follows:

- Baloch Raaji Aajoi Sangar (BRAS)
- Baloch Republican Army (BRA)
- Baloch Republican Guards (BRG)
- United Baloch Army (UBA)
- Lashkar-e-Balochistan (LeB)
- Baloch Liberation United Front (BLUF)
- Balochistan Liberation Front (BLF)
- Baloch Liberation Army (BLA)
- Baloch National Movement (BNM)
- United Baloch Army (UBA)
- Baloch Student Organization Azad (BSO-A)
- Baloch National Liberation Army (BNLA)
- Balochistan United Army (BUA)
- Balochistan Bunyad Parasat Army
- Balochistan Musalla Defah Tanzeem (BMDT)

- Balochistan Republican Party Azad
- Balochistan Waja National Liberation Army

The Twitter accounts engaged in the dissemination of content directly linked with the agendas of these organisations act as their shadows, acting in individual capacity while simultaneously pushing forward the narrative of the aforementioned terrorist organisations. The shadow organisations/individuals identified in the digital security environment of Pakistan through the hashtag #BalochistanIsNotPakistan are as follows:

- Rsiagra
- Danojowa
- Newsintervene
- Neerajindiansd
- Theaadiisingh
- Drnaseembaluch
- a_belutsch
- Hani_baloch7
- 9_0_9_0_1
- gatherer_news
- sohrabhaider7
- hanibalochtbc
- naseerzenab
- zahirabaloch
- Shanajahmed8
- Baluchistan
- missionkarima25
- e_sopore
- nobatmarri
- shakir86456347
- urviewsurnews
- yas28982593nida
- metadata
- bnmkhuzdar
- iamsultanmarri
- jasmcv8
- miryar_baloch
- patilsushmit
- saptashwa7
- tripth9991

- vbmpgermany
- balochzagh
- asadbalocc
- babarfangirll56
- bajwa_loser
- P_srinivasan
- aneesabaloch6
- balochmahira00

The overarching agendas of the state-recognized terrorist groups in Balochistan are secession, anti-Pakistan propaganda, separatism, recovery of missing persons and drawing of attention to human rights violations carried out by the security forces of Pakistan. All the shadow organisations/individuals identified share either one or more of the agendas of the state-recognized terrorist organisations. The claim that these shadow organisations do not just act in individual zones and are part of a shadow network can be proven using a Twitter sociogram.

**Figure 1: Twitter Sociogram Showcasing a Shadow Network**
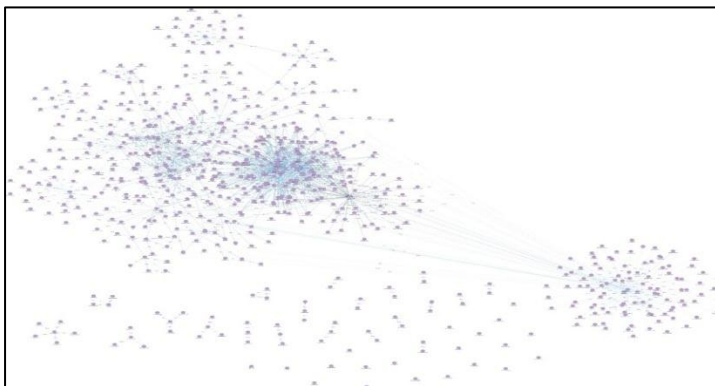
(Source: Author's compilation)

A breakdown of the sociogram shows the vertices connecting other accounts with that of 'BalochFreedomF.' BalochFreedomF is a state-recognized terrorist organisation that also acts as a shadow of its benefactors. These vertices reveal the link between shadow accounts and the state-recognized terrorist organisation, Baloch Freedom Front. In the figures below, it is pretty evident that there is a linking line between shadow organisations/individuals like MeerakQadeer, VBPMGERMANY, MissionKarima25, NeerajIndianSD, etc., and BNMKhuzdar and BalochFreedomF. The figures below not only connect the dots between a state-recognized terrorist organisation and its shadow organisations but also showcase the shadow network formed under the hashtag #Balocistan Is Not Pakistan by highlighting MissionKarima25, MeerakQadeer, VBPMGERMANY and Hani Baloch

TBC, BNMKhuzdar, Balochzaag, identified shadow individuals/organisations, association with one another.

Figure 2: Activity within Shadow Organizations/Individuals
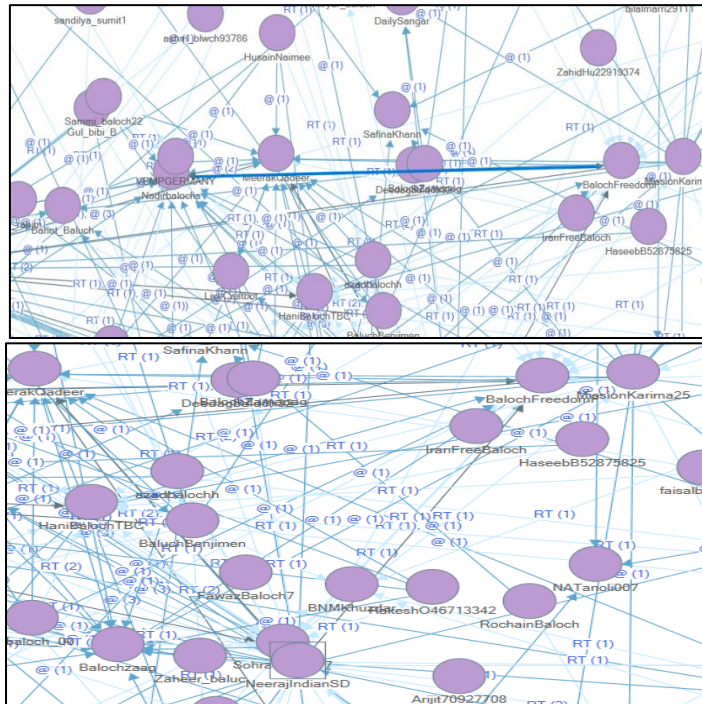
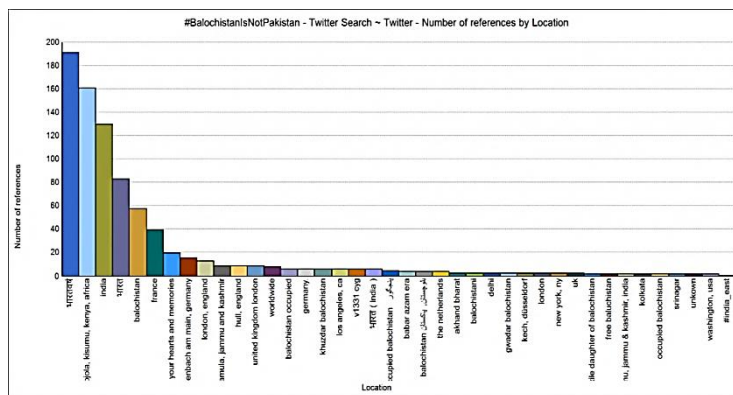(Source: Author's compilation)

The more critical thing To look for is Not The intra-proxy network but rather the benefactor seeking to subvert the Pakistani state using these shadow organisations. This relationship can be evident from the tactics employed by shadow organisations for information dissemination. The figure below showcases the benefactor/proxy relationship between the hostile country, India, and its shadow organisations within Balochistan.

Figure 3: Benefactor-proxy relationship between India and Balochistan
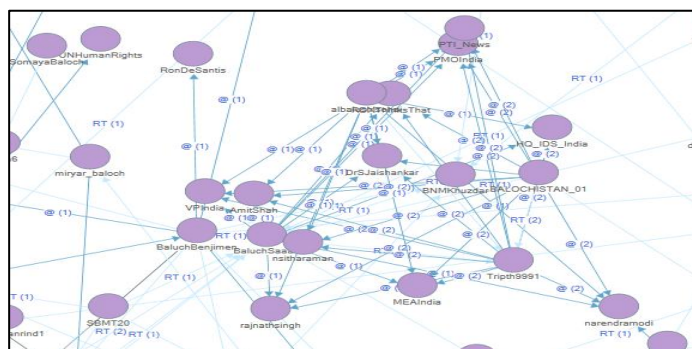
The use of mentions and hashtags enabled the content to become transnational. The location-based analysis of shadow individuals/organisations revealed many geographical spaces from where the content was disseminated. The figure below showcases the locations where the information was posted under the hashtag.

**Figure 4: Location of Tweets**

(Source: Author's compilation)

The locations that could be identified according to the number of references are Kenya, India, Balochistan, France, Germany, United Kingdom, Jammu and Kashmir, Los Angeles, Netherlands, New York, and Washington. The locations with the highest reference counts are India, Kenya, and Balochistan. The interesting point in this analysis is that while India plays the role of benefactor in the Balochistan issue, Kenya's presidential candidate, Danojowa, uses the Balochistan issue for political leverage, and the content disseminated from within Balochistan can be attributed to the identified shadow organisations.

The tactics employed for effective dissemination of content from these locations consisted of mentions, hashtags, employment of themes, and bot activity. The first tactic under analysis is the use of mentions. It is essential to know that these mentions served four agendas.

The first group of mentions targeted international human rights and media organisations to involve those organisations in the internal matters of Pakistan to increase pressure on the state and defame the state globally to damage the country economically and politically, which is state subversion. The international organisations mentioned within the dataset of 1127 tweets are the UN, FATF News, World, UNWomenChief, Boblancia, BarrickGold, and HRW. The exact frequency of their mentions is 193, 190, 4, 4, 10, 3, and 6 references, respectively. Another major

group identified in the mentions embedded in the tweets is of individuals and organisations belonging to Pakistan's biggest adversary, India, as shown in the figure below.

Figure 5: Number of References of Mentions
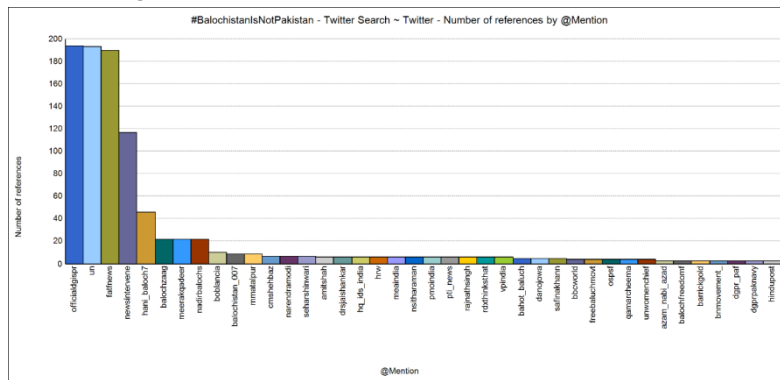
(Source: Author's compilation)

India has been known to nurture the separatist and insurgent groups of Balochistan.[27] These mentions solidify the assumption of a benefactor/proxy-like relationship between India and these shadow organisations. The Indian individuals and organisations mentioned within the dataset are Newsintervene, Narendra Modi, Amit Shah, Dr Jaishankar, Hq_ids_india, media, PMO India, Rajat Singh, rdxthinksthat, VP India, and hindupost. The exact frequency of the mentions is 117, 7, 6, 6, 6, 6, 6, 6,6, 6, 3 respectively. The third group mentioned targeting individuals and institutions in the state of Pakistan. Since the target of the subversive information operations is the Pakistani state, the mentions act as an affirmative for the assumption based on empirical evidence collected through the thematic analysis of the textual content in the dataset of the hashtag. The mention with the highest frequency in the dataset is dgispr, accounting for 194 mentions. The other mentions that point towards the assumption that the disseminated content was directed towards the Pakistani state and its institutions are cmshehbaz, pti_news, dgpr-paf, dgpr-paknavy, and ospsf. The frequency of the mentions is 7, 6, 3, 3, and 4 references in the respective order. The fourth group that mentions targeted involves state-recognized terrorist organisations whose agendas are pushed forward by the identified shadow organisations. These mentions affirm the connection between the non-state militant actors and shadow organisations. The accounts linked with the terrorist organisations mentioned in the dataset include freebaluchmovt, balocfreedomf, and the BLM movement. The exact frequency of the mentions is 4, 3, and 3, respectively. The remaining mentions target the shadow organisations. The deduction that can be made is creating a shadow network through the mentions to

reinforce a collective effort to conduct the information operation. The shadow organisations mentioned did not necessarily contribute to the dataset of the hashtag #BalochistanIsNotPakistan. Still, due to overlapping agendas, the shadow network extends to information perpetuation outside the hashtag. The shadow individuals/organisations mentioned are newsintervene, hani_baloch7, balochzaag, meerakqadeer, nadirbalochs, Balochistan_007, mmtalpur, seharshinwari, bahot_baloch, danojowa, safinakhann, qamarcheema, and azam_nabi_azad. The exact frequency of the mentions accounts for 117, 46, 22, 22, 22, 9, 9, 7, 5, 5, 5, 4, and 3 references in the respective order.

The second tactic for effective information dissemination was using various hashtags in the dataset of the hashtag under study. The majority of the hashtags posted had direct relevance with the themes identified in the textual content of the dataset with the aim of trend creation, and the rest were used as a means for trend hijacking. The themes identified and the number of tweets posted under each identified theme within the dataset are as follows:

Identified Themes	Number of Tweets
Anti-Pak Army Content	36
Anti-State Propaganda	112
Baloch Women	27
Balochistan, A Separate State	218
Balochistan's Developmental Issues	12
Ethnic Content (Anti-Punjabi)	9
Forced Disappearances	89
Language-Based Critique	2
Nuclear Program of Pakistan	118
Sectarianism	1
Terrorism Perpetuated by Baloch Insurgents	208

(Source: Author's compilation)

These themes represent the areas That the Baloch shadow individuals and organisations use to subvert the Pakistani state; the identified themes also resonate with the narratives used by the benefactor, i.e., India, to subvert the Pakistani state. They also represent some of the points of contention between the two countries: the hostile country is India, and the target state is Pakistan. For instance, India, due to the implications of conventional warfare, uses information warfare to spread the narrative containing false information regarding the dangers of Pakistan being a terrorist state and having possession of nuclear weaponry.[28] This narrative spread fear regarding the misuse of atomic assets, making the international community view Pakistan as a security threat.[29]

The identified themes are spread further using hashtags. The hashtag with the most references in the data is #BalochistanIsNotPakistan. The total number of references to the hashtag is 556, which directly corresponds with the dispersal of the content under the hashtag. The hashtags, free Balochistan; Pakistani; Balochistan; Baloch; Pakistan; danojowa; danojowaforpresident; Iowa; and 27marchblackday; had a respective reference count of 227, 194, 155, 43, 33, 25, 25, 25, and 13 references. All the hashtags above resonated with the source of the dataset and the identified theme, *Balochistan, A Separate State.* The hashtag 'blah' had a reference count of 189 and was the only hashtag directed towards a state-recognized terrorist organisation. The hashtags check, illegal, and the project had a high reference count of 166, 162, and 162 and mainly were posted without any textual content supporting the hashtags in the dataset. Since there was no textual content, the researcher did not create a theme for classifying these three hashtags. Sanctionpakistan, stop genocide, Pakistan under siege, and Balochistan bleeds are some of the hashtags that resonate the most with the theme, *Anti-State Content.* The exact reference count of these hashtags is 166, 161, 5, and 4, respectively. The hashtags Pakistan army and Pak army, with a reference count of 62 and 10, resonated the most with the theme, *Anti-Army Content.* Hashtags, nuke after math in Balochistan and not Pakistani nukes with a reference count of 49 and 24 references resonated with the theme, *Nuclear Program of Pakistan.* The hashtags, justice for najma Baloch and save Baloch women, with reference counts of 9 and 8, resonated the most with the theme, *Baloch Women.* All the hashtags above were used for trend creation and outreach of the disseminated information. The rest of the hashtags accounted for a total reference count of 772 references, and some of the examples of these hashtags include free Indhu desh; gb is not Pakistan; free Afghanistan, free Pashtunistan, Germany, UK, loyafghanistan, etcetera. These hashtags were not directly linked with the source dataset. Thus, their usage within the dataset only points towards trend hijacking, which can be crucial in capturing the attention of the masses and setting agendas.

Another tactic used to fuel trend creation and trend hijacking is bot activity. The bot activity report for the dataset was generated using botometre, a machine learning algorithm that generates scores on a scale of 1 to 5, indicating the likelihood of an account being a bot account; the higher the score, the greater the possibility. 27.5 per cent of the shadow accounts identified in the dataset have a bot score higher than 2.5, making them prime suspects for being bot accounts.

The data indicates that India and Kenya are hostile countries engaging with shadow organisations and state-recognized terrorist organisations to perpetuate information operations against the target country, Pakistan. The hashtag #Balochistan is not a Pakistan dataset, which revealed a shadow network of 40

shadow organisations. The state-recognized terrorist organisations visible within the shadow network are BNM Khuzdar and Baloch Freedom. The shadow organisations employ Twitter APIs (Hashtags, mentions), Bot Activity, and Nodes (themes) embedded within the textual content—the identified 11 nodes (themes) embedded within the textual content of the dataset. The detected bot activity in the Twitter accounts of shadow organisations is 27.5%. The mentions include global financing, advocacy, and media organisations; Indian state institutions and government officials; Pakistani state institutions and government officials; state-recognized terrorist organisations; and shadow organisations. Twenty-four hashtags within the tweets posted resonate with the identified nodes (themes) from the dataset with the aim of trend creation. Fourteen hashtags within the tweets posted are not relevant to the source or the identified nodes (themes) from the dataset and were used with the aim of trend hijacking.

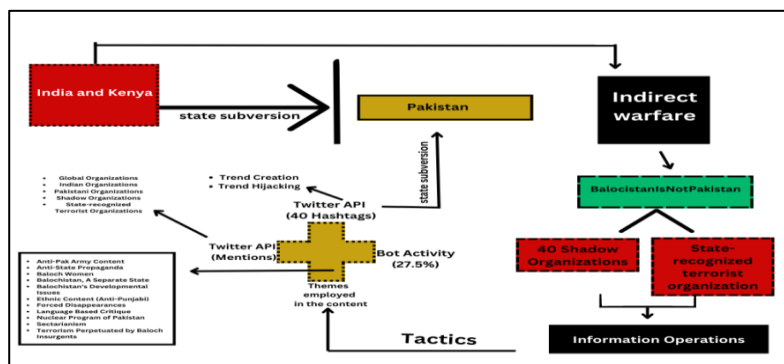**Figure 6: Conceptual Framework (Created by the Researchers)**
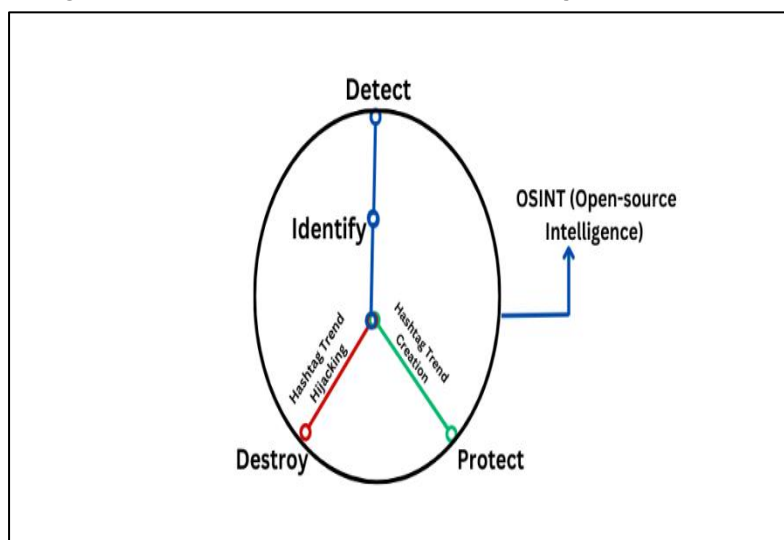
(Source: Author's compilation)

Recommendations

To counter the information operations perpetuated by Baloch shadow organisations subverting the Pakistani state involves a four-tier strategy.

Figure 7: Recommendations to Counter Information Operations (Created by the Researchers)

(Source: Author's compilation)

The first step of the strategy is to detect information operations being conducted in the digital security environment using social media intermediary platforms and content detection within these platforms. The second step of the strategy is to identify the source of the content dissemination and the sources' linkages and associations with different individuals and organisations. The third step of the four-tier strategy involves protecting the information environment by employing hashtag trend creation. This strategy will help counter propaganda and defamatory narratives. The strategy's last step will be destroying the effectiveness of information and the shadow network. The content will be dismantled by hijacking hashtag trends embedded in the information operation. On the other hand, detecting shadow networks will be crucial in destroying those networks, as publicly revealing their identity will demolish their credibility. All the steps of the four-tier strategy can be conducted through open-source intelligence.

Conclusion

The paper aimed to study the shadow organisations perpetuating information operations against the state. The study zoomed in on the existence of shadow organisations in Balochistan and analysed the conduction of information operations against the Pakistani state. The information operations perpetuated were in the sub-domain of the digital security environment, i.e., the information environment. The dataset analysed was from the hashtag #BalochistanIsNotPakistan. A network of shadow organisations was identified upon analysis of the collected data. The network of these organisations could be attributed to various hostile countries and hostile organisations.

The paper revealed the Indian and Kenyan stakeholders' contribution to perpetuating the information operation through the hashtag. The hostile organisations leading the narrative of shadow organisations were state-recognized terrorist groups, i.e., Baloch Freedom Front and Baloch National Movement Khuzdar. Further analysis disclosed the presence of bot activity within the dataset, and 27.5% of the Twitter accounts engaged in disseminating the information operation had a bot score of more than 2.5 on a range scale of 0-5. In addition to bot activity, the shadow network consumed various features of Twitter, such as mentions and hashtags. It employed 11 different themes in the textual content of the dataset to effectively perpetuate the operation. All the tactics employed aimed to antagonise the Pakistani state and its security institutions using advocacy for the rights of Balochis as a tool to network globally to create a global narrative of the Pakistani state being a repressive, oppressive, illegal invader that commits war crimes.

References

1   Azad, T. M. "Understanding The International Propaganda Patterns Against Pakistan." *Institute of Regional Studies Islamabad* (2020): 209-233.

2   Nadeem, Muhammad Ashraf, Ghulam Mustafa, and Allauddin Kakar. "Fifth Generation Warfare and its Challenges to Pakistan." *Pakistan Journal of International Affairs* 4, no. 1 (2021).

3   Azad, T. M. "Understanding The International Propaganda Patterns Against Pakistan." *Institute of Regional Studies Islamabad* (2020): 209-233.

4   Hardgrave, Robert L., and Stanley A. Kochanek. "India: Government and politics in a developing nation." *Cengage Learning* (2007).

5   Khattak, M. U., Muhammad Khan, and Ghulam Qumber. "Evolution of New Indian Military Strategy: Implications for Pakistan." *Margalla Papers* 23, no. 1 (2019): 139.

6   Nadeem, Muhammad Ashraf, Ghulam Mustafa, and Allauddin Kakar. "Fifth Generation Warfare and its Challenges to Pakistan." *Pakistan Journal of International Affairs* 4, no. 1 (2021).

7   Abidy, Syed Maqbool Hussain. "Non-state actors in Pakistan: Their destabilizing role in political crisis faced by the region." *Imperial Journal of Interdisciplinary Research* 3, no. 4 (2017): 1534-1537.

8   Abbott, Daniel. "The Handbook of Fifth-Generation Warfare." *Ann Arbor: Nimble Books* (2010).

9   Arquilla, John, and Douglas A. Borer, eds. *Information strategy and warfare: A guide to theory and practice*. Routledge, 2007.

10 Denning, Dorothy Elizabeth Robling. *Information warfare and security*. Vol. 4. New York: Addison-Wesley, 1999.

11 Prier, Jarred. "Commanding the trend: Social media as information warfare." In *Information warfare in the age of cyber conflict*, pp. 88-113. Routledge, 2020.

12 Deutsche, W"Penyerang Bunuh Diri Gereja Katolik Medan 'Terobsesi' ISIS – DW – 29.08.2016." n.d. Dw.com. Accessed July 25, 2023. https://www.dw.com/id/penyerang-bunuh-diri-di-gereja-katolik-medan-terobsesi-pimpinan-isis-al-baghdadi/a-19510515.

13 Mumford, Andrew. *Proxy warfare*. John Wiley & Sons, 2013.

14 Wither, James Kenneth. "Outsourcing warfare: Proxy forces in contemporary armed conflicts." Security and Defence Quarterly 31, no. 4 (2020): 17-34.

15 Ivanovic, Zoran. "Changing the character of proxy warfare and its consequences for geopolitical relationships." *Security and Defence Quarterly* 31, no. 4 (2020): 37-51.

16 Kronin, Audrey Kurth. "Power to the People: How Open Technological Innovation Is Arming Tomorrow's Terrorists." (2019).

17 Affan, M. "The threat of IS proxy warfare on Indonesian Millennial Muslims." *Indonesian Journal of Islam and Muslim Societies* 8, no. 2 (2018): 199-224.

18 Omand, David. "The threats from modern digital subversion and sedition." *Journal of Cyber Policy* 3, no. 1 (2018): 5-23.

19 US Office of the Director of National Intelligence. "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution." (2017).

20 Khetran, Mir Sherbaz. "Indian interference in Balochistan." Strategic Studies 37, no. 3 (2017): 112-125.

21 Ayaz, Ahmed. "Understanding the RAW-NDS nexus against Pakistan." *Defence Journal* 20, no. 9 (2017): 17.

22 Shah, Ahsan, Sadia Rafique, and Khalid Manzoor Butt. "Subversion: Challenging Nations' Capacity in Pakistan-India Context." *Journal of Indian Studies* 8, no. 1 (2022): 113-124.

23 Hansen, Thomas Blom, and Finn Stepputat, eds. *States of imagination: Ethnographic explorations of the postcolonial state*. Duke University Press, 2001.

24 Nordstrom, Carolyn. "Shadows and sovereigns." In *The Criminology of War*, pp. 89-108. Routledge, 2017.

25 Rozema, Ralph. "Forced disappearance in an era of globalization: biopolitics, shadow networks, and imagined worlds." *American Anthropologist* 113, no. 4 (2011): 582-593.

26 Hansen, Thomas Blom, and Finn Stepputat, eds. *States of imagination: Ethnographic explorations of the postcolonial state*. Duke University Press, 2001; Nordstrom, Carolyn. *Shadows of war: Violence, power, and international profiteering in the twenty-first century*. Vol. 10. Univ of California Press, 2004.

27 Khetran, Mir Sherbaz. "Indian interference in Balochistan." *Strategic Studies* 37, no. 3 (2017): 112-125.

28 Saud, Adam, and Nehal Kazim. "Disinformation and Propaganda Tactics: Impact of Indian Information Warfare on Pakistan." *Journal of Indian Studies* 8, no. 2 (2022): 335-354.

29 Mahadevan, Prem. "India and Global Discourse on State-sponsored Terrorism." *Rising Powers Quarterly* 1, no. 3 (2017): 185-201.