Digital Disinformation & Domestic Disturbance: Hostile Cyber-Enabled Information Operations to Exploit Domestic Issues on Twitter

Muhammad Rehan Rasheed [*] ***& Moazzam Naseer*** [**]

Abstract

State and non-state actors leverage social media as a tool for hybrid warfare strategies. It becomes a psycho-political weapon aimed at the adversary's vulnerabilities exhibited in socio-politico-economic fault lines. Twitter, like other social media platforms, is being increasingly used to spread disinformation. Apart from verified accounts and social media teams, bots can be used to enhance a challenging situation for their own benefit. The challenge that many data analysts have is not finding the data only, but sorting through it to segregate fake from the real. Pakistan has been targeted continuously by disinformation. This paper discusses how influence campaigns have been waged over digital platforms in recent years, using Pakistan as a case study to highlight one of the existing fault lines and discuss opportunities in the context of the growing role of social media in modern warfare. It also tries to address the role of belligerent state actors in shaping the psychological makeup of democratic population. This research provides analysis in to the worldwide influence operations and their role in international politics. It also provides

* Muhammad Rehan Rasheed is a PhD Scholar, Riphah Institute of Media Sciences, Islamabad, Pakistan.

** Moazzam Naseer is an Associate Professor, Institute of Media Sciences at Riphah International University, Islamabad, Pakistan

IPRI Journal XXI (2): 95-129
https://doi.org/10.31945/iprij.210204

insightful examinations of how democracies all over the world can overcome foreign manipulations. Finally, it is intended to aid analysts, scholars and policymakers for better understanding of information warfare in the context of cyber conflict.

Keywords: Online Communities, Digital Disinformation, Online Propaganda, Open-Source Intelligence, Social Media Intelligence, Social Network Analysis, Cyber-Enabled Information Operations, Hybrid Warfare

Introduction

Media platforms are essential tools for transmitting and receiving information. Rapid advancements in information and communication technologies in the latter half of the 20th century and the early 21st century, triggered the information age revolution. Together these technologies are altering the world of knowledge and information with implications for individuals, as well as the entire societies.

The digitization of information has had a significant impact on traditional media companies. Mass correspondence has changed to the point that anyone can communicate with the world without any hindrance. It doesn't matter if mainstream media outlets cover it or not. This allows anyone to collect and share information from all corners of the globe. While computing technologies make it easier for information to be shared through tools, such as social media, the disappearance of intermediaries further enables the manipulation and misrepresentation of facts.

Technology is not enough to bring about social change, but how people adopt and integrate technology can have a significant impact.[1] While computer and communication advances are certainly beneficial, they also open up the possibility of cybercrimes such as malicious access to electronically stored information, privacy abuse, fake news and propaganda.

The digital age has opened up new perspectives in the art of warfare. The operational environment and conduct of war are greatly affected by the new emerging technologies. Nowadays, cyber operations target individuals within a society, influence their beliefs and diminish trust in the democratically-elected government. In today's world, nation-states use their energies to learn the art of political and psychological warfare. It is gradually replacing the outdated and costly traditional methods. The

[1] Starr, Paul. "The creation of the media: Political origins of modern communication." Basic Books, Inc., 2005.

technological revolution has changed the way wars can be fought and waged. One of the most important landmarks in this revolution was the invention of social media, which created a network-centered approach as a center of gravity to defense and attack. These new tools and platforms are unleashed by the Internet in the form of social media which, with its unique nature gave propaganda a boom and opened new doors to influence the minds of the adversaries and allies in a way it was never imagined before.[2]

State and non-state actors can access online information regularly via social media, allowing them to influence networks within and outside the state. To harm national interests, discredit public institutions and sow domestic strife, adversaries are now trying to control and exploit social media trend mechanism. Social media platforms utilize algorithms to analyze the usage of words or phrases to generate the "trend list" of topics sorted by popularity. It is a simple way to look up the most popular topics of discussion at any time. The trending topics can send messages to a broad audience that is even not part of the usual social network of a person. Therefore, everyone would like to be on the top of trend list. "Commanding the trend" is a new and dangerous way to persuade via social media.[3]

This paper examines how adversaries used social media to hijack information during the time of any domestic issue and spread malicious propaganda to citizens. This case study shows how non-state actors and adversarial states use social media to spread hateful propaganda and terror threats against a country and its citizens. It also describes how state-level disinformation is spread and how social media is manipulated, with a particular focus on an issue that has been raised by an opponent country. The case study is supported by the investigation of hateful

[2] Michael Erbschloe, *Social Media Warfare: Equal Weapons for All* (Boca Raton: Auerbach Publications, 2017).

[3] Prier, Jarred. "Commanding the trend: Social media as information warfare." *Strategic Studies Quarterly* 11, no. 4 (2017): 50-85.

hashtags on Twitter, which is believed to be a part of the information warfare network of the hostile state. The study concludes with the implications of cyber-enabled foreign information operations and what can be expected in future. It also discusses how the state can deal with the increasing threat from adversaries who command the online trend.

Information Environment, Information Warfare & Information Operations

The victor in a battle is usually someone who has quick access to the most relevant information and can act quickly. Information Warfare supporters often quote Sun Tzu's famous maxim: "Know your enemy and know yourself. Then in a hundred fights you will never be at risk."[4]

The main objective of information warfare is to manipulate information without the target's knowledge so that they make decisions against their own interest. Although it is not new, it has innovative elements due to technological advancements. Information is disseminated quicker and on a greater scale. Technological advancements have been a catalyst for the development of information warfare, which has profoundly altered the information environment.

The information environment is the place where human and automated systems interact to view, orient, decide and act on information.[5] It is, therefore, the main environment for decision-making. Information warfare refers to a conflict between two or more people in an information environment.

The information environment is a collection of many social, cultural cognitive, technological, and physical attributes.[6] These attributes have an

[4] Tzu, Sun. Sun Tzu Art of War. Vij Books India Pvt Ltd, 2012.

[5] Theohary, Catherine A. "Information warfare: Issues for congress." Congressional Research Service (2018): 7-5700.

[6] Lin, Herbert. "The existential threat from cyber-enabled information warfare." Bulletin of the Atomic Scientists 75, no. 4 (2019): 187-196.

impact on knowledge, understanding, beliefs, views and ultimately the actions of individuals, groups, communities and organizations.

How humans use information to determine the outcome of the conflict is crucial to understand. Any well-known military theory from any age will reveal the crucial role of superior understanding about one's enemies and importance of using that knowledge wisely to gain an advantage. Information is the basis of understanding between the parties in a conflict. The information environment is the medium through which information flows and how the players use it to affect each other's decision-making.

Information operations is defined as the deliberate use of information against an adversary to influence his decisions and choices.[7] Influence operations is a non-kinetic hostile activity between two belligerents whose interests do not align.[8] It is more accurately described as hostile psychological manipulation which includes propaganda and persuasion. Influence operations consist of gathering tactical information about an enemy as well as the dissemination of propaganda to gain a competitive advantage.[9]

According to a US Congressional Research Service (CRS) report, information warfare is a strategy that uses information to gain a competitive advantage against adversaries. This includes both offensive and defensive operations. Strategy is the process of planning in order to achieve national goals and objectives. Operation links strategic objectives with techniques. The link of information warfare strategy is information operations. According to this report, information warfare is at the strategic

[7] Cohen, Raphael S., Nathan Beauchamp-Mustafaga, Joe Cheravitch, Alyssa Demus, Scott W. Harold, Jeffrey W. Hornung, Jenny Jun, Michael Schwille, Elina Treyger, and Nathan Vest, Combating Foreign Disinformation on Social Media: Study Overview and Conclusions. Santa Monica, CA: RAND Corporation, 2021. https://www.rand.org/pubs/research_reports/RR4373z1.html.

[8] Shallcross, Nicholas J. "Social media and information operations in the 21st century." Journal of Information Warfare 16, no. 1 (2017): 1-12.

[9] "Information Operations." RAND Corporation. Accessed September 19, 2021. https://www.rand.org/topics/information-operations.html.

level and information operations are used to implement strategies using different information-related capabilities.[10]

Cyber Operations & Cyber-Enabled Information Operations

Cyber operations can be used as a force multiplier in information warfare and social media is a powerful tool for communicating a narrative and generating confusion within a target audience. Cyberspace is the battlefield for waging information operations. However, cyber warfare is different from information warfare.[11] Both pertain to information, but they are two distinct phenomena. Cyber warfare refers only to the digitized and operationalized form of the information. However, information warfare has a wider scope in which information itself is the most powerful weapon.[12] The solutions for one don't necessarily apply to the other.

Nowadays, everything is being considered under the heading of cyber. It is important to know the differences between a few terminologies in order to fully grasp the concepts. During cyber conflict, the main target is information and information technology in cyberspace. Adversaries prosecute cyberwar by taking advantage of the technical flaws of information technology. However, cyber-enabled information operations make use of the information to target human mind.[13] In this case, adversaries are prosecuting cyber-enabled information operations through the technical virtues of information technology. Many Americans believed that Russian interference during the 2016 US election was an act of cyberwar. It was actually a cyber-enabled information operation in which Russia exploited social media platforms.[14] Russian operations benefited

[10] Theohary, C. A. (2020). (rep.). Defense Primer: Information Operations (pp. 1–2). Washington D.C., United States: Congressional Research Service.

[11] Whyte, Christopher, A. Trevor Thrall, and Brian M. Mazanec, eds. Information Warfare in the Age of Cyber Conflict. Routledge, 2020.

[12] Lin, Herbert, and Amy Zegart. "Introduction to the special issue on strategic dimensions of offensive cyber operations." Journal of Cybersecurity 3, no. 1 (2017): 1-5.

[13] Lin, Herbert. "Attribution of malicious cyber incidents: from soup to nuts." Journal of International Affairs 70, no. 1 (2016): 75-137.

[14] Lin, Herbert. "On the organization of the US government for responding to adversarial information warfare and influence operations." ISJLP 15 (2019): 1.

from the same algorithms that social media platforms use to increase user engagement with advertiser and user-generated content.[15]

According to the US National Security Presidential Directive-54 dated January 8, 2008, the definition of cybersecurity clearly specifies that the target is a computer and computer-related entity that need to be secured against cyber operations. However, cyber-enabled information operations can be described as the intentional use of information in the cyber domain to mislead or affect the decisions and choices made by the adversary. The human mind is the target of these influence operations. The success of cyber-enabled information operations depends on deceptive content and inauthentic attributions produced by the hostile actors. Cyber operations are successful because of the vulnerabilities in hardware and software that can be exploited to accomplish the goals. However, influence operations usually take advantage of the vulnerability related to cognitive and psychological biases in human beings.

Cyberspace is the battlefield for cyber operations. However, the information environment (physically, informational and cognitive) is the equivalent construct of information operations and it includes cyberspace in it. Psychological operations require access to the users and taking advantage of user vulnerabilities by using tailored content to exploit the fissures in the hostile arguments.

Both cyber operations and influence operations require intelligence. While the former relies on tactical intelligence of targeted computer and computer-related entities, the latter depends on strategic intelligence such as knowing the political situation and societal fault lines that could be exploited. The last thing that matters is the type of operation. Cyber-attacks and cyber exploitations can be considered cyber operations. However, propaganda, disinformation, leaks, as well as chaos-productions, are information operations.

[15] Cyber Operations vs Information Operations - CyCon 2019 Twilight Talk. natoccdcoe, 2019. https://www.youtube.com/watch?v=KyCDvEzq25s.

Social Media: A Psycho-Political Weapon

New domains of warfare emerged with the advent of the Internet and social media. The invention of social media has opened up new avenues for states to pursue their goals in foreign countries without engaging its force. This transition demonstrates a psychological dimension that weakens the roots of the enemy. The goals and objectives in the modern world are not total defeat but defeat in high politics, i.e. psychological tactics are used to coerce your enemy in order to achieve certain political goals and forcing adversaries to act on your will.[16]

In general, war is about achieving political objectives through other means. The psychological dimension of non-kinetic warfare reveals the growing dependence on psycho-political tools that attack the enemy's mind. This is where non-kinetic fronts allow psychological and informational weapons to be used in modern-day war. It is not a new idea and the target is the human mind.[17]

States around the world have turned to economic, technological and information war after realizing that conventional wars and physical battles are not cost-effective and are casualty intensive. These transformations have created proxy wars, cyberspace breaches, information operations and propaganda exploitation. To incite social unrest, information operations and propaganda are used. The media acts as a force multiplier and can be used by external actors to exploit internal fault lines within a state. The rise of non-kinetic warfare has been evident with the technological development of communication tools. Due to the expansion of new war front, it is likely that future decades will see social media play a predominant role as a psycho-political weapon of warfare. Because of its enormous reach, social media has proven to be an effective weapon against the center of gravity in any state i.e. the people's will and morale

[16] Paul W. Blackstock, *The Strategy of Subversion: Manipulating the Politics of Other Nations* (Chicago: Quadrangle Books, 1964).
[17] Charles Roetter, *The Art of Psychological warfare: 1914-1945* (New York: Stein and Day, 1974).

to fight. Social media has changed the way wars are waged, fought, and consumed in the 21st century.[18] It can be used to wage psychological and political warfare and mainly aims to disrupt a state's social, economic, and political system by creating strategic narratives or changing perceptions. These are precisely the reasons why states in modern times prefer to use social media against their adversaries to achieve political or military goals.

Disinformation is an informational tool in an information warfare strategy and it has become more widespread and pernicious with the advent of social media.[19] Information warfare is a struggle for reality. Truth and facts are often the most vulnerable victims. Nowadays, adversaries have realized that they don't need to convince you of their point of view. They simply need to get you to question yours. All they need is to get your doubts to last long enough for them to be able to attain what they want.

The book of Peter W. Singer and Emerson Brooking is the most pertinent literature on the subject ***"Like War: The Weaponization of Social Media."*** The authors explain the phenomenon of weaponization using social networking sites at its center. They claimed that technology, politics, and war have all come together to create a new battlefield, which is now played out on our mobile phones. Brooking and Singer also argued that social networking is transforming the modern world and history.[20]

Today, each and every state is at risk from this type of warfare. Like any other state, Pakistan is vulnerable too due to the existing internal fault lines in socio-politico-economic and military settings. These new media tools are being used by the adversaries to further exacerbate the internal

[18] David Patrikarakos, 'War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-First Century,' (New York: Basic Books, 2017).

[19] Stengel, Richard. 'Information wars: How we lost the global battle against disinformation and what we can do about it,' *Atlantic Monthly Press*, 2019.

[20] P. W. Singer and Emerson T. Brooking, 'Like War: The Weaponization of Social Media,' (New York: Eamon Dolan/Houghton Mifflin Harcourt, 2018).

schisms and create chaos and instability through polarization in the society.

The 2010's: The Rise of Cyber-Enabled Information Operations

The decade of 2010s saw technological breakthroughs and significant societal shifts.[21] There has been an exponential rise in cyber-enabled information operations after the advent of popular social media platforms. Modern technologies were prominent in the wave of protests that swept across the Middle East in the early 2011. The Project based at the University of Washington on *Information Technology and Political Islam* discovered that online revolutionary conversations often preceded mass protests on ground and social media played an important role in shaping political debates during the Arab Spring.[22] Social media companies, governments and activists formed a triangle that influenced social media use during the Arab movement.[23]

The implications of online social networks in the Middle Eastern context have far-reaching implications that go beyond the direct comparisons with other regions. As the spread of social media networks increases, there will be new opportunities and vulnerabilities in the developed world as well.

Russia successfully ensured a new age of geopolitical competitiveness through influence operations. Cyberspace is often used in conflict to eliminate the communication systems of an enemy. However, the conflict with Ukraine has shown that cyberspace is capable of being used to conduct narrative-driven operations where the main targets are not the

[21] https://www.globalxetfs.com/a-decade-of-change-how-tech-evolved-in-the-2010s-and-whats-in-store-for-the-2020s/

[22] Howard, P. N., Duffy, A., Freelon, D., Hussain, M. M., Mari, W., & Maziad, M. (2011). Opening closed regimes: what was the role of social media during the Arab Spring?. *Available at SSRN 2595096*.

[23] Alkhouja, M. (2016). Social media for political change: the activists, governments, and firms triangle of powers during the Arab movement. In *Social Media and Networking: Concepts, Methodologies, Tools, and Applications* (pp. 55-66). IGI Global.

machines or networks but minds of the people.[24] Ever since Russian troops began their annexation of Crimea in February 2014, the Kremlin's campaign against Ukraine has heavily relied on information warfare and the innovative use of social media.

Though, social media had been seen as encouraging democratic discourse about political and social issues. However, powerful communication network has come under scrutiny for allowing adversaries to use online discussions and manipulate public opinion. An example of this is the US Congressional investigation of the Russian interference in 2016 US Presidential Elections. Russia has been accused of using bots, trolls, and propaganda to spread disinformation.[25] As part of an official investigation into the Russian interference in 2016 US Presidential Election, the U.S. Congress also published a list of these accounts.[26] Despite years of preparation for cyber conflicts against US military forces and critical infrastructure, the US government was not prepared for the Russian information operations that could impact the 2016 US presidential election.[27]

According to Diego Martin and Jacob Shapiro's *Empirical Studies of Conflict Project* at Princeton University, Russia had launched more than 20 campaigns across 13 countries by 2016, and nearly 90% of these campaigns were on Twitter.[28] A US Senate Minority Report in January

---

[24] Lange-Ionatamishvili, Elina, Sanda Svetoka, and Kenneth Geers. "Strategic communications and social media in the Russia Ukraine conflict," *Cyber War in Perspective: Russian Aggression against Ukraine* (2015): 103-111.

[25] ICA, ICA. Assessing Russian Activities and Intentions in Recent US Elections 2017-01D. Technical report, Office of the director of national Intelligence, 2017. Available in :< https://www. dni. Gov/files/documents/ICA_2017_01. Pdf.

[26] Badawy, Adam, Aseel Addawood, Kristina Lerman, and Emilio Ferrara. "Characterizing the 2016 Russian IRA influence campaign." Social Network Analysis and Mining 9, no. 1 (2019): 1-11.

[27] Francois, Camille, and Herb Lin. "The strategic surprise of Russian information operations on social media in 2016 in the United States: mapping a blind spot." *Journal of Cyber Policy* 6, no. 1 (2021): 9-30.

[28] Martin, Diego A., and Jacob N. Shapiro. "Trends in online foreign influence efforts." Princeton University, Princeton, NJ, Working Paper (2019).

2018, suggested that Russia could have had an influence on the Brexit campaign.[29] Similarly, the Russian Foreign Ministry also summoned the US ambassador for alleged interference in the Russian elections 2021.[30] US and Russia are accusing each other on many occasions along with their allies. Nowadays, the world is engulfed with influence operations from east to west and these have been fairly intense in their severity.

One of the most famous influence operations was the one in which US presidential candidate, Trump hired the services of the British consulting firm Cambridge Analytica. This company harvested the personal data of millions of Facebook Users without their consent and used it for analytical support to the 2016 Trump presidential campaign.[31] It was the biggest data leakage in social media history.

In a Reuters report released on January 12, 2021, titled, "Inside Israel's Social Media Campaign to woo the Middle East,"[32] the main theme is about influence operations on Arabs to embrace Jewish state by a special team in Israel's Foreign Ministry. The mission statement of the team is *"Using social media for convincing Arabs to embrace the Jewish state."* The team is reaching 100 million people a month through social media accounts, more than double the number a year ago. Israeli Ministry official said, the rate of negative commentary on social media had dropped to 75% in January 2021. Ofir Gendelman (spokesman Israel's Prime Minister) said that there is an increasing numbers of Arabs view

[29] Wintour, Patrick. "Russian Bid to Influence Brexit Vote Detailed in New US Senate Report." *The Guardian*. January 10, 2018. https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed-us-senate-report.

[30] *Al Jazeera*. "Russia Summons US Ambassador over 'Election Interference'." Elections News |, September 10, 2021. https://www.aljazeera.com/news/2021/9/10/russia-summons-us-ambassador-over-election-interference.

[31] Wilson, Richard. "Cambridge analytica, Facebook, and Influence Operations: A case study and anticipatory ethical analysis." In European conference on cyber warfare and security, pp. 587-XX. Academic Conferences International Limited, 2019.

[32] Farrell, Stephen, Maha El Dahan, Lisa Barrington, and Zainah El Haroun. "Inside Israel's Social Media Campaign to Woo the Middle East." Reuters. January 12, 2021. https://www.reuters.com/article/israel-gulf-normalisation-int-idUSKBN29H1FY.

supporting "Israel as an ally" and many publicly show their support on social media. The team also targets Israel's adversaries such as Iran, Hamas and Hezbollah.

Another Reuter's report of July 9, 2021, titled *"How Vietnam's 'influencer' army wages information warfare on Facebook"* explained the establishment of state sponsored thousands-strong 'Force 47' army unit, who are fighting the fierce online battles against the opposite views.[33] A similar model has already been implemented in the UK to form a hybrid warfare division to focus intelligence, surveillance, cyber warfare and digital propaganda. According to the Head of the Field Army, Lieutenant-General Ivan Jones in August 2019, said: "The character of warfare continues to change as the boundaries between conventional and unconventional warfare become increasingly blurred." It is the first designated information warfare grouping of UK Army to address the needs of an arena where both insurgents and hostile states should be engaged in highly destructive asymmetric campaigns often using social media.[34]

India's History of Spreading Disinformation against Pakistan

India's use of disinformation as a tool for spreading propaganda against Pakistan is well-documented and there are strong evidences of digital attack by the Indian troll armies in the past. In December 2020, EU DisInfo Lab, (an independent non-profit organization based in Brussels focused on tackling sophisticated disinformation campaigns) had uncovered the scale of the Indian influence operations, including

[33] Pearson, James. "How Vietnam's 'Influencer' Army Wages Information Warfare on Facebook." Reuters. July 9, 2021. https://www.reuters.com/world/asia-pacific/how-vietnams-influencer-army-wages-information-warfare-facebook-2021-07-09/.

[34] Lye, Harry. "British Army Announces New Cyberwarfare Division." Army Technology, August 1, 2019. https://www.army-technology.com/news/british-army-cyber-warfare-division/.

systematic disinformation and propaganda campaigns against Pakistan at a global scale that support the Indian geo-political interests.[35]

The report describes the disinformation campaign launched from India as "15 years' huge operation running since 2005, targeting international institutions and serving the Indian interest - using resurrected media, dead think tanks and *NGOs*. Even dead people were resurrected." This report revealed that 750+ fake media outlets and 550+ domains were found covering 119 countries. These were used by the Indian propagandists for spreading anti-Pakistani content via unusual Press agencies. They also amplify material that was shared by the politicians and obscure think tank that supported the Indian geopolitical goals against Pakistan. Researchers also discovered 265 sites that were pro-Indian and tracked them back to a Delhi-based Indian holding firm, Srivastava Group. This network is active in Geneva and Brussels, producing and amplifying content that aims to undermine Pakistan. They coordinated demonstrations against Pakistan each year during the UN Human Rights Council sessions and also used the hashtag of the HRC live broadcast to spread disinformation against Pakistan. The report also provides many policy recommendations and urged the international community that this should be a wake-up call for the decision-makers all around the world to create a framework that can sanction those who abuse international institutions.

[35] Machado, Gary, Alexandre Alaphilippe, and Roman Adamczyk. "Indian Chronicles: Deep Dive into a 15-Year Operation Targeting the EU and UN to Serve Indian Interests." EU DisinfoLab. EU Disinfo Lab, December 9, 2020. https://www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15-year-operation-targeting-the-eu-and-un-to-serve-indian-interests/.

Figure 1:
Tweet of EU DisinfoLab

Figure 2: How Pro India Network Spread Disinformation

Background - Case Study

On April 12, 2021, the leader of *Tehreek-e-Labbaik* (TLP), a religious political party, Saad Rizvi was detained as a pre-emptive measure to avoid potential public violence. TLP had already called for a nationwide protest on April 20, 2021, to demand the end of diplomatic relations with France

and expulsion of its ambassador from the country. Their demand is a reaction to an incident in October 2020, when a French teacher of history was killed for displaying blasphemous sketches insulting Prophet Muhammad (peace be upon him). The attacker was shot by French police when they tried to arrest him. French President Emmanuel Macron condemned the attack on the teacher and vowed not to give up the blasphemous cartoons. Most leaders of the Muslim nations at that time, including the Pakistani prime minister had condemned the French president's remarks but it did not mollify the TLP hardliners. They wanted stricter action against France.

The Government of Pakistan's move to detain the leader of TLP on April 12, 2021, did help to maintain peace at large. However, hostile forces launched a social media campaign to incite violence inside the country. Indian social media influencers posted fake / doctored videos and images in complete disregards to international laws / norms with a potential of major unrest/chaos. They promoted a hashtag #CivilWarInPakistan, where prominent Indian personalities and trolls posted fake and doctored images and videos of mob violence within Pakistan. They also shared doctored video of soldiers from Pakistan claiming to join the violent protestors. This was a clear interference by India into Pakistan's internal security affairs. This campaign was orchestrated to incite hatred and mistrust against the government. It creates an alternate reality in which civil war is erupting and Pakistan is engaging in illegal activities and high handedness towards its own citizens.

It is well-documented that India used disinformation to spread propaganda against Pakistan. There is also a proof of coordinated digital attacks by India Troll Armies in the past. Previously, the Indian twitter accounts circulated claims that there was a civil war in Karachi (Pakistan) in October 2020. Multiple Indian news websites also reported the story, despite the fact that there was no truth to this claim. In October 2020, the same hashtag #CivilWarInPakistan was used by the Indian trolls. They also promoted fake news, which was widely circulated on the Indian

websites and social media claiming that a civil war had broken out in Karachi, Pakistan. The credibility of the Indian media was seriously damaged when *BBC* reported in October 2020, that videos and reports by the Indian media about the civil war in Pakistan were fake.[36] BBC also reported a Twitter account @drapr007. It was apparently the first to tweet fake news. Last October 2020, #CivilWarInPakistan got more than 18,700 tweets and #CivilWarinKarachi over 3,384 tweets.[37] Major media outlets in India, including *Zee News*, *CNN18*, and *India Today* built up stories on unverified tweets and videos. They reported a civil war in Sindh (Pakistan) and spread the fake news by retweeting it wildly.

Figure 3*: Indian Twitter account @drapr007 posted fake news*

Many *Pakistani* ministers lodged complaints with Twitter, asking the micro-blogging site to immediately take action against accounts spreading false information against Pakistan. Pakistan Telecommunication Authority (PTA), approached Twitter to alert its moderation teams, and make sure that it is not being used for propaganda purposes. PTA regretted that some accounts were used in spreading untrue stories. They were twitter verified and were still operating with immunity.

[36] Hussain, Abid. "India Buzzes with Fake News of 'Civil War' in Pakistan." *BBC News*, October 22, 2020. https://www.bbc.com/news/world-asia-54649302.

[37] Newspaper's Staff. "PTA Asks Twitter to Punish Those behind Anti-Pakistan Propaganda." *DAWN*. October 23, 2020. https://www.dawn.com/news/1586573.

Figure 4: *PTA Notification*

Figure 5: *Pakistani Minister complained to Twitter*

Figure 6: *Michael Kugleman South Asian expert) exposed Indian*

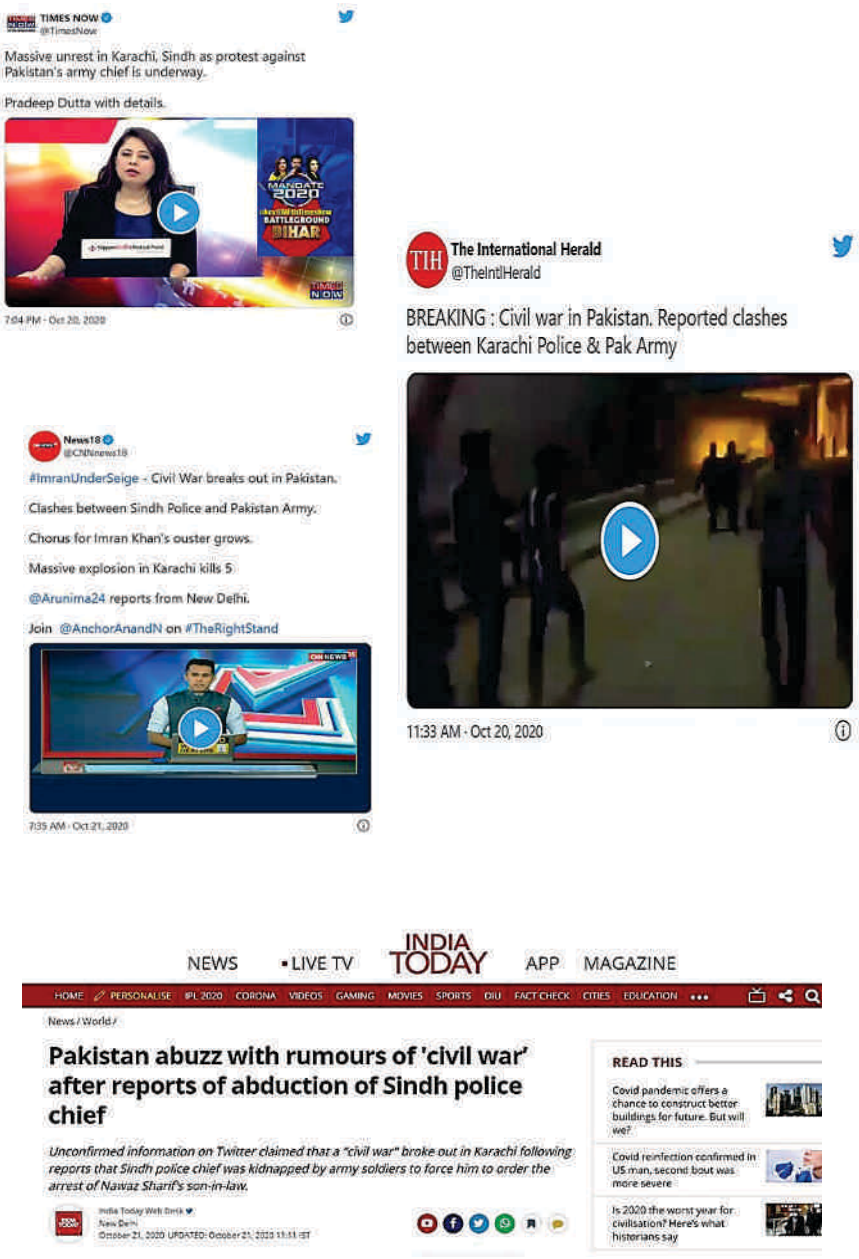

Figure 7: Major Indian Media outlets involved in spreading propaganda

Method

Our understanding of how online troll networks are organized has improved due to social network analysis (SNA), which has provided viable means for tracking, destabilizing, and disrupting them on social media. Through networks and graph theory, SNA tries to understand a community by mapping the links that connect them as a network, then pulling out key accounts and groups inside the network and associations between the accounts.

An exploratory SNA was employed in this study. Exploratory SNA combines quantitative and qualitative methodologies, transforming the network's numeric data into a graphic display, followed by a narrative description of the pattern and network structure.[38] Exploratory SNA allows researchers to determine the relationship between actors,[39] their roles, communication patterns, and network subgroups.[40] The study focused on all the tweets that had the hashtag #CivilWarInPakistan. The data were collected from microblogging Twitter. The time limitation was turned on in the process because the same hashtag #CivilWarInPakistan was run in October 2020, and supported by the Indian trolls, including fake news which had been widely circulating on the Indian sites and social media. Therefore, in order to keep the data specific to the latest incident, the tweets were extracted from the period of April 12 to 20, 2021. A total of 81,557 tweets containing the hashtag #CivilWarInPakistan were retrieved.

The tweet data from the scrapping process is visualized using Gephi software to find out influential actors and relationships among actors on

[38] Teddlie, Charles, and Abbas Tashakkori. "A general typology of research designs featuring mixed methods." Research in the Schools 13, no. 1 (2006): 12-28.

[39] Borgatti, S. P., M. G. Everett, and J. C. Johnson. "Chapter 13. Analyzing two-mode data." Analyzing Social Networks; Sage Publications Limited: London, UK (2013): 231-248.

[40] de Jong, M. D., & Zwijze-Koning, K. H. (2009). Communication network analysis. In O. Hargie & D.Tourish (Ed.), Auditing organizational communication (hal. 149–166). New York: Routledge.

the network. Gephi is a tool that reveals the degree of graphic representation, centrality, and community participation and cluster formation among the network users.[41] The network analysis includes two major components: nodes and edges which can be seen by looking at the Gephi network visualization. The network is a collection of nodes connected by edges, where a node represents an individual or actor on the network and an edge indicates a link between nodes.

The centrality of the actor pointed out by the node's size is an important component in the network analysis.[42] The centrality indicates how important or influential an actor is on the network. There are a few ways to evaluate network centrality, but this study used two: degree centrality (both in-degree and out-degree) and betweenness to identify dominating actors in the #CivilWarInPakistan debate.

The most fundamental metric for networking is Degree Centrality, which measures the amount of connections or ties with a single actor. The more edges that a node owns, the more central the node's position on the network.[43] For directed ties, actors have 'in' and 'out' degree values for centrality scores. A node with a high centrality score is frequently referred to as a hub and an active network entity.

A node that becomes an intersection of many other nodes in delivering and receiving messages is the node that is central or influential, according to the principle of betweenness centrality. A higher node's level of betweenness indicates that the node has many accounts or users on the network. Thus, it allows discovering a node that can act as a possible broker between two groups in the network.

---

[41] Kennedy, Helen, Giles Moss, Chris Birchall, and Stylianos Moshonas. "Guide to tools for social media & web analytics and insights." Working Papers of the Communities & Culture Network+ 2 (2013).

[42] Golbeck, Jennifer. Analyzing the social web. Newnes, 2013.

[43] Gerdes, Luke M., ed. Illuminating dark networks: the study of clandestine groups and organizations. Vol. 39. Cambridge University Press, 2015.

Buzzword visualization is used to locate the topic of discussion in the network. A buzzword is a term that is widely known and used to describe a subject.[44] The buzzword is assigned to concepts on social media that are understood and utilized collectively. Kilyeni went on to say that a buzzword might be context-specific, meaning it was established to describe a particular notion or issue that was addressed on social media.[45] A buzzword analysis was conducted by identifying high-frequency terms on the network #CivilWarInPakistan. The central tendency of a topic of discussion that frequently surfaced on the network can be visualized.

Findings

There is a strong evidence of coordinated digital attack by India netizens. The Indian trolls have sent thousands of tweets using the hashtag #CivilWarInPakistan and the percentage of indigenous content was very less. Their instigative content was gathered and analyzed. Findings suggest that these organized online groups, operated from India, propagated violent and provocative hashtags to sabotage Pakistan's effort to manage the internal law and order situation. Following are the main findings:

a. Tweets that contain keywords **#CivilWarInPakistan** have been extracted from the period of **April 12 to 20, 2021,** accounted for **81557** with **7,120 tweets per hour** being generated at the peak of the trend.

b. **86%** of tweets in the hashtag are retweets, a telling sign of artificial and organized amplification of any trend.

[44] Zhang, Jianwei, Seiya Tomonaga, Shinsuke Nakajima, Yoichi Inagaki, and Reyn Nakamoto. "Prophetic blogger identification based on buzzword prediction ability." *International Journal of Web Information Systems* (2016).

[45] Kilyeni, Annamaria. "Likes, tweets and other “friends”: Social media buzzwords from a terminology perspective." Procedia-Social and Behavioral Sciences 192 (2015): 430-437.

c. The hashtag was shared by **26,828 unique user accounts** and majority of them are from **India**. Fifty-five per cent of tweets were coming from India on this hashtag.

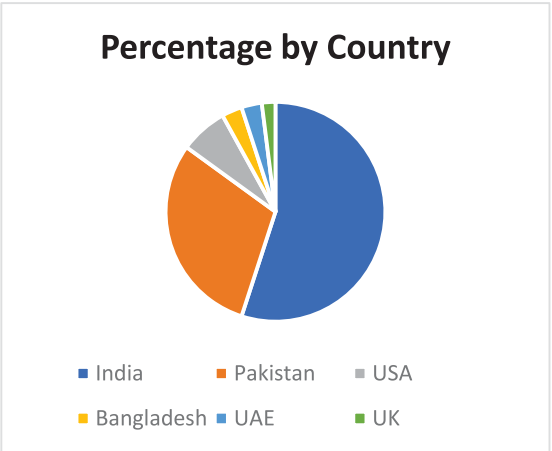

Figure 8: Percentage of Participation by Country

d. New Delhi contributes the highest number tweets. There are many other Indian cities in the list of top ten contributing to the hashtag.

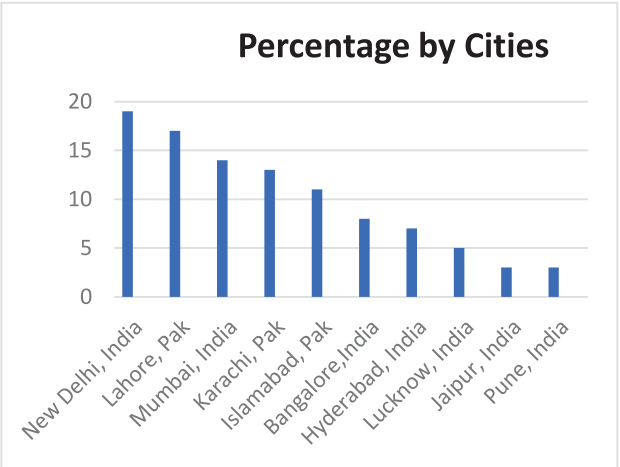

Figure 9: Percentage of Participation by Cities Country

e. Each node with the same color (each dot is a Twitter user) in figure 10 indicates strong online connections between same-color Twitter users. It is evident that more than 10,000 Indians tweeted with the hashtag where more than 1913 worked as a part of different teams who incited violence in Pakistan in an organized and aggressive manner.

Figure 10:
Same color shows a network of a single team spreading disinfo i.e. green, purple, blue, orange & pink etc colors shows Indian trolls who propagated violence as organized groups.

f. **Figure 11** gives exact Twitter handles of the most active Indian Twitter users who propagated the instigative hashtag and fake news along with doctored videos in the digital sphere.

Figure 11:
India's Top Trolls involved in instigation of violence in Pakistan

g. Around **1551** accounts in this trend were created since **January 2021**, out of which **438** were made in **April 2021**. It was also found

that there is a mix of *Pakistani* and Indian accounts. *Pakistani* accounts were either fake / anonymous or being used by anti-government user accounts (activists from opposition parties against the present government).

h. The accounts spreading disinformation about a non-existent civil war also contribute to hashtags **#TLPNationWideProtest** and **#Stop_Gov_terrorism**.

i. Some of the accounts have been deactivated by the users to avoid the reporting and ban, but their instigative messages have been saved for reference. For instance, Twitter handler **@Kaala_Nag** sent hundreds of tweets containing instigative content and fake news, but this handle was deactivated within days of spreading violence.

Figure 12:
Deleted Tweets of @Kaala_Nag – an Indian acct

j. Based on the out-degree centrality values, the nodes with the biggest size or the most central actor are **@VictoriousNamo**, **@Intolerant_KD** and **@Jvl52** respectively. Other actors that are also vital in this network are **@tum_and_hum**, **@srdmk01**, **@saffronhindoo**, **@Piyali53880331**, **@Ritam92560836**, **@Unknown14318773**, **@Kaala_Nag** as well as **@Jvlmk**.

Serial No.	Twitter Handle	Out-Degree
1.	Victoriousnamo	271
2.	Intolerant_KD	244

3.	Jvl52	220
4.	Tum_And_Hum	210
5.	Srdmk01	179
6.	Saffronhindoo	166
7.	Piyali53880331	149
8.	Ritam92560836	140
9.	Unknown14318773	140
10.	Kaala_Nag	132
11.	Jvlmk	129
12.	Proudindab	127
13.	Shivam44575933	125
14.	Itsrishabsays	121
15.	Govindakamaki	116
16.	Tarun33864349	106
17.	Amrendra_Kk	104
18.	Anantvijay1729	102
19.	Fascistchikna	98
20.	Pseudo_Liberal_	97

Table 1: *Top user accounts (Out Degree Centrality)*

k. For hashtag #CivilWarInPakistan, **@Jvlmk**, **@kashmir_watch**, **@Defence_360**, **@Kaala_Nag**, **@HunarTweets**, **@alam_mujaid**, **@IFENewsAgency**, **@GUY_WITH_BEARD7**, **@majorgauravarya**, **@KreatelyOSINT** and **@DefenderOfInd** were the accounts that get mentioned (*in-degree centrality*), making their edge's number higher as compared to other nodes on the network.

Serial No.	Twitter Handle	In-Degree
1.	Jvlmk	5464
2.	Kashmir_Watch	2049
3.	Defence_360	1435
4.	Kaala_Nag	942
5.	Hunartweets	446
6.	Alam_Mujaid	423
7.	Ifenewsagency	401

8.	Guy_With_Beard7	358
9.	Majorgauravarya	354
10.	Kreatelyosint	324
11.	Defenderofind	293
12.	Krishanpandit02	282
13.	Hindust2021	275
14.	Mahesh10816	265
15.	Iserious9	248
16.	Iamaslamkhan2	239
17.	Bharatojha03	231
18.	Pseudo_Liberal_	204
19.	Imohit1509	196
20.	Frontalwarrior	187

Table 2: *Top user accounts (In-Degree Centrality)*

l. Based on the principle of betweenness centrality, the most central nodes are **@Kaala_Nag**, **@srdmk01**, **@backpackingmonk**, **@ProudIndAB**, **@Unknown14318773**, **@Pseudo_Liberal_**, **@kakar_harsha**, **@Jvlmk**, **@saffronhindoo**, **@HunarTweets**, **@kashmir_watch** and **@Jvl52** respectively.

Serial No.	Twitter Handle	Betweenness Centrality
1.	Kaala_Nag	306556.1498
2.	Srdmk01	174327.2473
3.	Backpackingmonk	143859.8362
4.	Proudindab	133881.5769
5.	Unknown14318773	127581.8544
6.	Pseudo_Liberal_	114945.7862
7.	Kakar_Harsha	90829.61942
8.	Jvlmk	87575.77084
9.	Saffronhindoo	77326.66223
10.	Hunartweets	75930.3958
11.	Kashmir_Watch	75526.27746
12.	Jvl52	71830.30063
13.	Kalki_C	60088.03272

14.	Govindakamaki	52090.98987
15.	Intolerant_Kd	49557.50085
16.	Javidtalk	44293.77972
17.	Cestmoiz	43819.76678
18.	Defenderofind	34870.29909
19.	Hindust2021	31939.21294
20.	Alam_Mujaid	29428.34133

Table 3: *Top user accounts (betweenness centrality)*

m. Following list contains Twitter handles of accounts who were actively engaged in paddling fake news and creating chaos in Pakistan. The list is in descending order showing the most active users first and mentioned top 100 handles.

Top 100 Twitter User Accounts

VictoriousNamo	Gif_baaz	Boogeyman009	DangerAlert34
Intolerant_KD	kalki_c	Pankaj80986649	ViviLovesIndia
Jvl52	AzamHoor	baghla1983	shyamsundar_n
tum_and_hum	Secularism14	hinduamitpandit	uc_navneet
srdmk01	KChaita49697812	dshah071	busybee22383944
saffronhindoo	javidtalk	143BJP	Rishav01k
Piyali53880331	DevNarayanSS2	nothingtodo1111	Defence_360
Ritam92560836	VinodD89389312	Omnamohvasudev	HunarTweets
Unknown14318773	MokshBaba	Whisky28638669	Me_is_Chauhan
Kaala_Nag	Prathamesh524	jiteshsinght	futuristic_in
Jvlmk	AkhandB48802573	PankajS58944850	BHARATfirst_
ProudIndAB	mrpaidtroller	Observe17166183	backpackingmonk
Shivam44575933	krishnasharmaP	Darkstuff99	Dharmik2021
ItsRishabsays	srjthakur20	ChiBabaIndia	kashmir_watch
GovindaKamaki	AnshSin87939881	DNobody101	AshishS37970857
Tarun33864349	ItReve6	pkgFULLpkg	Aspirant0106
amrendra_kk	sanjaykharwar	HandsomeMolana	monty_chadha
AnantVijay1729	AdityaN18872038	subodhmishra92	pawanme3513
fascistchikna	KAMALJE68452437	NeerajDIndian	ArnabTalukder
Pseudo_Liberal_	raguveer00009	anandgujarathi	anil_breatheart
AgnosticTheist5	_RajaBhai	NdSolanki	DefenderOfInd
Unknown40436578	sundar45678	iRameshwarArya	Proudly26290119
Hindust2021	s4AIBCPDATA	FlankerFoxy	DhamaManeesh
Ramesh03328910	WinnieIthePOOH	NRaj2020	IndicIndiaVedic
tanna_tasha	shivusoni424	amitkumar0019	Mhendrapratap99

Table 4: *Top 100 Accounts*

Figure 13: Top Trend in Pakistan

Figure 14: Top Influencer Account

n. Following are the word cloud and the list of frequently used words in the hashtag: -

Figure 15: Word Cloud

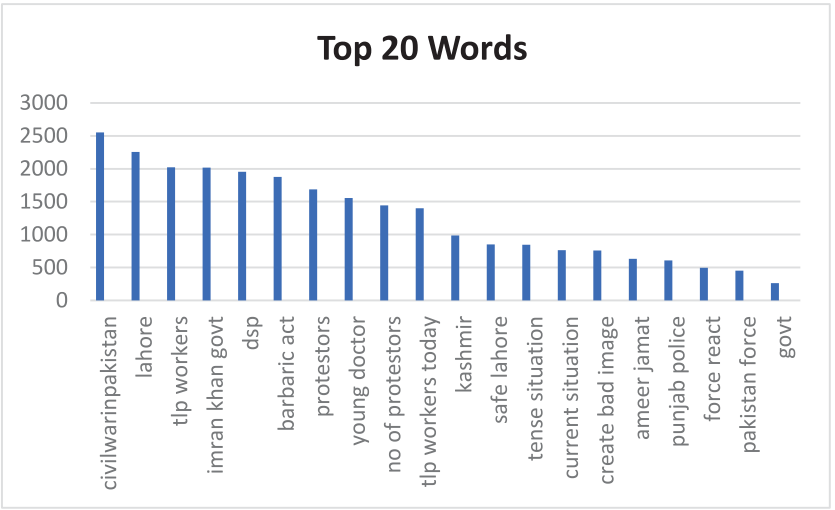

Figure 16: Top 20 Words of the Hashtag

Discussion

In response to this trending hashtag on Twitter, the Ministry of Interior of Pakistan instructed authorities on April 15, 2021, under cybercrime legislation to locate and arrest any person who posted, shared, or commented against Pakistan on the internet. The ministry also instructed the PTA to block access to social media platforms temporarily. It stated that the government had defeated terrorists, agitators, and others who spread unrest via social media due to timely actions.[46] However, this incident has highlighted many challenges to the authorities and analysts. The challenge that many data analysts have is not finding data but sorting through it. Therefore, there is a dire need to enhance the capabilities of the government authorities in order to take action against these accounts and pursue the case along with the technical evidence.

Social network analysis has revealed organized activity by the Indian accounts to incite violence and chaos in Pakistan. It is one of the best

[46] Ali, Kalbe. "Social Media ACCESS Restored in Pakistan AFTER Blockage to 'Maintain Public Order'." DAWN.COM, April 17, 2021. https://www.dawn.com/news/1618552.

solutions to get the exact nodes that are responsible for spreading disinformation. Therefore, the authorities must integrate such kind of analysis for necessary defensive measures to be taken at various tiers to best prepare for these cyber-enabled information operations in the future. The capacity building of state institutions is required to monitor such threats in the cyber domain in the future and then build response as a part of the National Computer Emergency Response Team (CERT).

This hashtag #CivilWarInPakistan is also analyzed by many independent organizations. One of the organizations named "Digital Rights Monitor," which analyzed the trend mentioned above, reported that 61 % of the tweets mentioning this trend originated in India.[47] New Delhi contributes the highest number by generating 10% of the total volume of tweets. In addition, Indian cities of Mumbai, Bangalore, Hyderabad, Lucknow, Pune and Jaipur are also among the top ten cities contributing to the hashtag. The results of the analysis done by Digital Rights Monitor are very much similar to the result of this study which further authenticate the data used in the research.

Similarly, G5iO, Pakistan's premier Internet observatory under Islamabad Policy Research Institute (IPRI), also undertook extensive data analytics to deconstruct coordinated disinformation and information operations against Pakistan. Evidence indicates extensive use of bots, coordinated network behavior and fake news pushed across multiple social media platforms. According to G5iO, hashtag #CivilWarInPakistan consists of total 92,976 tweets with 40.26% bot activity. The report states that the top tweeting location is India and the trend initiated by the Twitter handle @theedge37 (This Twitter account is suspended now).[48]

---

[47] Baig, Asad. "Misinformation Warfare - #CivilWarinPakistan Trends with 61% Tweets Coming from India; New Delhi Contributes the Highest Number." Digital Rights Monitor, April 18, 2021. https://www.digitalrightsmonitor.pk/misinformation-warfare-civilwarinpakistan-trends-with-61-tweets-coming-from-india-new-delhi-contributes-the-highest-number/.

[48] "Disinformation and Propaganda Campaign to Sabotage Afghan Peace Process." G5iO, August 2021. https://g5io.ipripak.org/2021/08/10/disinformation-and-propaganda-campaign-tosabotage-afghan-peace-process/.

This research shows that the hashtag #CivilWarInPakistan is following a similar trend again. It further validates the scale of the Indian disinformation and propaganda against Pakistan at the global scale. Both Indian Twitter accounts and the Indian websites are showing up as high influencers.

The surprising aspect of these accounts in this study is their detailed insight into Pakistani politics. It is a deliberate Indian effort to incite violence in Pakistan. Therefore, such cases should be taken up using diplomatic channels (through the Ministry of Foreign Affairs). The dossier should be made available publically with sufficient supporting data and evidence. The world organizations must also be sensitized regarding these online activities after the confirmation of data from the researchers through independent forums, i.e., universities, NGOs, think tanks and government departments. This is having serious implications and the world should take tangible actions against the state-level planned negative influence operations in the region because it is having potential harm in terms of violence and loss of life.

The emerging environment and challenges posed by the social media urge the establishment of institutions aiming to conduct data research at the national level. There is a dire need to support and establish new ventures (public and private) to address threats posed by social media-led warfare. Similarly, Open Source Intelligence (OSINT) capabilities must be developed to provide insights of online data for the purpose of addressing specific intelligence requirement as a decision-making tool which is crucial for public, policymakers and researchers to understand and mitigate future operations.

EU DisinfoLab, a non-governmental organization that tackles disinformation campaigns, says regarding social media companies that the

world cannot continue the status quo of arbitrary platforms decision-making, which differs from month to month and country to country.[49]

It is recommended that social media companies are required to register with state's authority, open office and, appoint a focal person within the state for better coordination in the future. Similarly, database servers are to be established within the state borders for the purpose of data protection. Social media companies should devise mechanisms in order to identify unlawful content and stop online streaming of hate speech, incitement and violence.

For the removal or blocking of illegal content, strict implementation of rules is also necessary. It is imperative to clearly define freedom of expression so that the authorities can take action against content that harms the integrity, security, and defense of the country. Any content that harms the public order or is against morality and decency should be removed immediately. The world is increasingly aware of the dangers of disinformation and new rules are needed to improve our online environment.

Conclusion

This paper has examined the dangers of information warfare as it relates to military, diplomacy and civilian stakeholders. The study tries to understand the efforts of an actor to spread negative perceptions about the adversary in cyberspace. It is necessary to study information warfare as an important strategic concept which can enlighten cyber policy-makers over different areas of international political practices. There is a dire need to enhance the capabilities of the government authorities in order to take action against these accounts and pursue the case along with the technical evidence. Pakistan must re-evaluate the definitions of hate speech,

[49] "Open Letter to EU Policy-Makers: How the Digital Services ACT (DSA) Can TACKLE DISINFORMATION." *EU DisinfoLab*, September 2, 2021. https://www.disinfo.eu/advocacy/open-letter-to-eu-policy-makers-how-the-digital-services-act-dsa-can-tackle-disinformation/.

disinformation and freedom of expression. These definitions are right now blurred and influenced by social media companies and few nation-states. Social media platforms must ensure tight content oversight and the crackdown on fake accounts and orchestrated campaigns against other countries and societies inciting violence and hatred. Pakistan and social networking platforms need to renegotiate and validate the content filtering framework in light of recent conflicts. Due to the country's vulnerability in social issues and inability to develop cyber security strategies, Pakistan has been seen as an open target by its rivals. It is important that the state institutions work harder to create a unified and coordinated strategy and policies against hate, discrimination, fake news and other cyber threats. Disinformation warfare exists and must be stopped. It will lead to bigger issues in the future if it is not countered. Pakistan needs to act now before it is too late.■