



## THE EMERGENCE OF HYBRID WARFARE AND INTERNATIONAL SECURITY ENVIRONMENT: A CASE STUDY OF PAKISTAN

*Muhammad Ashraf Nadeem*  
MPhil Scholar  
Department of International Relations  
GC University  
Faisalabad – Pakistan  
[ashrafnadeembaloch@gmail.com](mailto:ashrafnadeembaloch@gmail.com)

*Sher Ali Kakar*  
Research Officer  
Balochistan Think Tank Network (BTTN)  
Quetta - Pakistan  
[sheralikakar@bttb.org.pk](mailto:sheralikakar@bttb.org.pk)

*Sikandar Azam Khan*  
Research Officer  
Balochistan Think Tank Network (BTTN)  
Quetta – Pakistan

*Dr. Ghulam Mustafa*  
Assistant Professor  
Department of International Relations  
GC University  
Faisalabad – Pakistan  
[ghulammustafa@gcuf.edu.pk](mailto:ghulammustafa@gcuf.edu.pk)

### Abstract

*In the modern world, hybrid warfare is considered a significant security challenge. This research paper primarily seeks to examine hybrid threats from a global perspective and uses Pakistan as a case study. This research has been conducted through secondary data analysis, using a qualitative method of discussion. The twenty-first-century security environment is characterized by the hybrid nature of warfare. Though hybrid warfare tactics are old, it is the technological advancement that has made them more and more effective and a preferred strategy of warfare. The media has become one of the main components of hybrid warfare. False news and fake*



*accounts have been used as a weapon in everything from Russian meddling in the US presidential election to online terrorist recruitment. Pakistan, being a nuclear-armed state and an important regional country, is facing the challenges of hybrid warfare. False news and misleading reports are being spread by hostile elements to harm Pakistan's image in the international community. This research aims to identify hybrid threats at a global level as well as examine their challenges to Pakistan.*

**Key Words:** Hybrid warfare, International Security Environment, Pakistan, Media, Indian Chronicles.

## Introduction

For six decades, nuclear weapons have avoided any major conflict between nuclear-armed states. Hence, non-conventional warfare emerged as the preferred strategy of warfare. This warfare is waged to weaken a state politically, socially, and economically. The twenty-first-century security environment is characterized by hybrid warfare. Hybrid Warfare refers to a military strategy that blends conventional warfare, so-called 'irregular warfare', and cyber-attacks with other influencing methods, such as fake news, diplomacy, and foreign political intervention (Weissmann, Nilsson, & Thunholm, 2021). Hoffman, in 2007, gave the first definition of hybrid warfare: "Hybrid wars incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder" (Hoffman, 2007, p. 14).

Technological advancement has changed the mode of warfare. The media has become the most important instrument of hybrid warfare. The media is used as a tool of warfare against a rival state for strategic objectives (Mitrovic, 2018). Hybrid warfare is used to undermine a state's peace and stability, particularly for a nuclear-armed state like Pakistan. Hostile countries employ HW tactics and strategies to weaken the country. In recent times, India, the arch-rival of Pakistan, has been making the best use of hybrid warfare strategies to exploit Pakistan's domestic fault lines, such as political, social, and economic, to weaken the country internally.

The emergence of hybrid warfare does not represent the end of conventional warfare. But it has become a complicated factor for defense planning in the 21<sup>st</sup> century (Hoffman, 2009). Technological advancement, during the last two decades, has complicated defense planning. Modern media tools such as Facebook, WhatsApp, Twitter, Instagram, etc. are new dimensions added to the domain of hybrid warfare. Internet and its confluence with



modern technologies have enhanced the accessibility of people to modern media tools. Social media tools are being used by hostile countries and non-state actors to spread fake news and misleading reports to achieve their nefarious designs.

Furthermore, the emergence of social media has made it easier to promote propaganda and spread fake reports, and falsify news faster than ever before. Social media is used without media ethics and the principal code of journalism, thus becoming an effective tool for adversaries to further their negative ambitions. Social media has become a source of unethical journalism and unjustified news is spread without verification of authenticity which influences the mindsets of individuals, jeopardizing the national unity of a country (Singer & Brooking, 2018).

The emergency of hybrid warfare has changed the international security environment drastically. The objective of this research is to identify hybrid threats and explore the complexity of the hybrid conflict. The study focuses on hybrid war challenges from a global perspective and uses Pakistan as a case study, focusing on media as a component of Hybrid Warfare.

## **Literature Review**

The change in the mode of warfare in the twenty-first century has spurred a debate between scholars, political scientists, analysts, and military officials in an attempt to understand the nature of modern warfare. Most scholars believe that warfare tactics have not changed, but they have evolved to a modern level as a result of technological advancement.

Weissmann, Nilsson, & Thunholm (2021) discuss different aspects of Hybrid warfare which includes the perspective of key western actors such as NATO, the United States, and the European Union. Also, an analysis of Russia and China's hybrid warfare capabilities has been the focal point of the study. In addition, the authors discuss a range of global case studies which includes the Baltic States, Taiwan, Ukraine, Iran, and Catalonia – which are drawn upon to demonstrate the employment of Hybrid Warfare tactics and how they have been countered in practice.

Munkler (2005) is of the view that the classical model of inter-state warfare has been replaced with intra-state warfare hence states have begun to lose their absolute authority on organized violence and have been replaced by military entrepreneurs. It is important to understand the tactics of new wars as a whole to understand Fifth Generation Warfare and its growing challenges at the global level. The new era of warfare has witnessed terrorist



attacks followed by bomb blasts, and the creation of widespread outright fear among the very social fabric of a state.

Kaldor (2013) has examined primary differences between conventional warfare associated with the ascent of a modern state as well as aspects of the cold war. Through regional and contextual transformations remain, the author states that the structural features of warfare consist of a flagrant disregard for the system, violence is now directed against civilians rather than military and sporadic, unsystematic attacks rather than on defined lines. This is a clear indication of departure from the first three generations of warfare.

Tahir & Afridi (2019) have highlighted the emerging role of the internet and technologies in warfare. The emergence of the internet joining together with communication and information technology is playing a central role in modern warfare. It has been used as a tool to produce waves of hyper information thus allowing the foes to impose hybrid warfare from various platforms.

Kalshall (2019) explains in detail the point of attack through fifth-generation warfare. He says, in hybrid warfare, enemy states hit the most important and sensitive areas of a rival state. Institutions and other sensitive areas like language and ethnic issues are the main targets of the fifth generation of warfare. The author calls fifth generation warfare, a soft war that is being fought through print, electronic and social media. Youth must be aware of these tactics; otherwise, state institutions will be destroyed.

Svetoka (2016) believes that the advancement of information technology has created an additional layer of complication in the domain of warfare. Modern technological tools have made it easier to impose war and achieve strategies objectives against a rival state. The author further states that, in the twenty-first century, both states and non-state actors use hybrid war tactics to achieve their political and strategic goals employing cyber-attacks, political and economic coercion, and disinformation campaigns.

Danyk, Maliarchuk, & Briggs (2017) explore modern tools of warfare. The authors believe that information and cyber-attacks are the main components of hybrid warfare. According to them, development in the domain of information technology is the main factor in transforming the theoretical and practical paradigms of war and conflict. The author focuses hybrid nature of modern warfare. According to the author, the hybrid nature of warfare when combined with the traditional concept of conflict and security is often called hybrid warfare.



The above-mentioned studies cover important aspects of hybrid warfare. This research paper discusses the media as one of the components of this warfare in global as well as in Pakistan's context.

### **Research Methodology**

This research paper is based on qualitative research. Data for this study has been collected through secondary sources. Owing to a lack of resources, primary data was not collected. For secondary sources, the researcher used books, scholarly articles, research journals, and newspapers to gather relevant data for this research. The collected data is then analyzed through a critical approach and qualitative method of discussion. This method enabled the researcher to gain an in-depth understanding of the topic and collect secondary data from credible sources to understand hybrid warfare.

### **International Security Environment and Hybrid Warfare**

With the advancement of technologies, the use of hybrid warfare tactics has expanded dramatically, playing a role in international affairs constantly (Mecklin, 2017). Information is deemed one of the key components of power, diplomacy, and domain of warfare. In the twenty-century, the development and proliferation of information communication technology have made the availability of information platforms increasingly widespread. The modern media tools have enabled users to instantly receive and project information in real-time. In turn, this has profound impacts on economic systems and political processes (Brown, 2018).

The digital revolution and an explosion of information have created technological opportunities to influence and manipulate. Besides, cyber-attacks, subversion, and sabotage have complicated security planning in the era of modernization (Buchanan, 2020). Social media tools have become today's spyware, propaganda amplifiers, and instruments of modern warfare. The traditional megaphones and leaflets have changed to cyber-attacks and smartphone tweets, spreading without geographic barriers, manipulating opinions, and destabilizing cohesion (Rosenberger, 2020).

Mass media are essential to democratic society; when we relate it to war on terror the results are evident by reshaping the perspective of public opinion (Simons, 2010). Numerous examples involve the change in public opinion, the most recent example being the Trump election monitored through cyber operations. The influence of media tools to transform public opinion has widely been used by state and non-state actors alike. The mass media used for influencing people is one of a kind, but there have been more



instances where this tool has been used over and over again. It is now considered the central element in warfare, where wars have been more political than military involvement. Keeping that under debate, the world is now more prone to the mass media to gain subjective as well as objective gains.

Hybrid warfare includes cyber breaches, funding to paramilitary troops, interference in the electoral process, disinformation and false news, murder and abduction, encouraging religious and political groups to increase social tensions and violence (Marovic, 2019). Hybrid warfare is now the new domain that is employed by states to achieve their motives without engaging directly. Hybrid warfare tactics differ significantly from traditional military engagements in which conventional strategies are employed; however, states employ irregular and cyber warfare tactics.

According to the Norwegian Policy Institute Policy Brief of 2016, hybrid warfare actors use their power in numerous ways. The areas that reciprocate invariably with each other are MPECI (military, political, economic, and civilian and information) and PMESII (political, military, economic, societal, and informational and infrastructure) (Cullen, 2016). The state made use of these instruments on the battlefield in Chechnya and Lebanon, and later in Afghanistan and Iraq. While non-state actors' use of HW was made by Hezbollah in combining characteristics of conventional and unconventional warfare strategies to challenge the military practices in novel ways (Cullen, 2016). The characteristics of HW are sophisticated amalgamating it with modern weapons capability (like deploying UAVs, anti-ship missiles, cyberspace with effective command and control).

The phases of HW vary in number and on the type of cases it comes in contact with. In the case of Russian HW, Berzins cites two Russian writers (Tchekinov and Bogdanov) categorizing an eight-phase model that emphasizes non-kinetic, and psychological aspects of HW that precedes kinetic domain (Berzins, 2014). These phases provide an outlook to see war with different perspectives; however, when they have strictly applied the basic essence of the strategy it loses effect. By far the fact that achieving political means does not only require military means, but the new domain of psychological and cognitive spaces is also largely at play. It was Russia's HW that led them to annex Crimea to its territory while the EU and US were unable to protect the integrity of Ukraine at the very best.

There exists a chunk of data available on how war has changed its traditional aspect i.e., bloodshed; however, the tools employed have changed (HW). In recent times, war has been indirect in approach i.e., weakening the enemy from inside than actually confronting them (Faber & Faber, 1927). This has been observed in proxy's war during the cold war



and in Afghanistan, Syria, and during Arab Spring, where the authoritarian regimes were brought down to their knees paving the way to democratic norms. The strategy proves effective where the cultural differences are weak and the masses can be persuaded to accept what is right and what circumstances dictate. Resultantly, achieving the outcomes without engaging in war and even losing the troops.

### **The US and Russian Hybrid Tactics**

Media in the context of warfare specifically focuses on the non-kinetic war without engaging military power. The term hybrid warfare came into existence when Russia annexed Crimea in 2014 (Center, 2019). Meanwhile, when Russian President Vladimir Putin came into power, he signed the Doctrine of Information Security on September 12, 2000. The immediate effect of this doctrine was to ensure the international audience was not misled about state policies and opinions about the Russian outlook. This new law paved the way to embed control of the media. Like Russia, most countries follow the same agenda of not risking their national sovereignty. This is because non-state actors will probably use it against them.

From Russian interference in the US election to online recruitment for terror groups such as ISIS, false news and fake accounts are being used to create hype, incite violence, and manipulate outcomes (Singer & Brooking, 2018). The Russian interference in the U.S. election through hybrid tactics such as social media got much attention around the world. Russia used social media accounts to spread misinformation about the electoral process and candidates. Social media platforms such as Facebook, Twitter, YouTube, etc. were used to spread propaganda and influence the 2016 US election. The US claimed that Russia used millions of social media posts through social media platforms (BBC, 2018).

The critical role of social media in the events of the Arab Spring, which Russia attributes to covert US influence campaigns, as well as the growing importance of the social media arena in the Kremlin's ambitions for hegemony within Russia and US influence operations in Russia, led to Russian adoption of social media as a key component of its evolving security posture. The Russian government's incorporation of social media-based information operations into its hybrid warfare is due to two factors. First, the regime increasingly sees domestic propaganda campaigns as a critical pillar of its survival. Second, the Russian security apparatus deemed it vital to keep pace with its NATO rivals, particularly the US, who have, over many years, preferred the use of hybrid tactics and influence operations (McCombie, Uhlmann, & Morrison, 2020).



## **The Hybrid War Challenges to Pakistan**

Pakistan is one of the most important geostrategic locations in the world. Being the sole nuclear power in the Muslim world, it has a special status in the region as well as in global politics. Since Pakistan became a nuclear power in 1998, hostile countries, particularly India, have been waging indirect warfare against Pakistan. Pakistan has developed credible capabilities to deter nuclear and conventional aggression, hence it is being targeted with modern tools of warfare such as terrorist attacks, covert operations, and subversive actions, cyber-attacks, and media campaigns including electronic, print, and social media.

### **Role of Social Media**

Adversaries are using social media as a weapon to break the social cohesion of Pakistani society. Whenever a difficult situation arises in the country, the anti-state elements become active through social media and attempt to influence the mindsets of the people to give rise to an anti-state narrative. In 2018, TLP protesters took to the streets and blocked roads in some cities in Pakistan over the verdict in the Asia Bibi case. The protests were not given coverage by the national media, but social media apps such as WhatsApp and Facebook were used massively to create hype among the masses and generate uncertainty in the country. These tools provide anonymity, which makes the situation complex by giving equal space to people with intense views to propagate their ideas publicly without unveiling their identities (Geo News, 2018).

Moreover, in April 2021, Tehreek-Labbaik Pakistan (TLP) held mass demonstrations on the issue of perceived “blasphemy”. The TLP protest in the country was exploited by Indian media and a propaganda campaign was started. As violent activities continued in some cities of the country, the Indian media propagated it as a civil war in Pakistan. During TLP’s protest, more than 300,000 tweets originated from India within three and a half minutes. According to Minister for Information and Broadcasting Fawad Chaudhry “So much so that during the TLP protest, a huge number of tweets originated from the Indian city of Ahmedabad, which is known as an information technology city” (Dawn, 2021).

The adversaries are attempting to damage Pakistan's image in the international community. They are trying to give rise to a narrative that Pakistan is an unsafe country. In July 2021, a fake news story about the alleged abduction of the Afghan ambassador's daughter was circulated on social media. Fake social media accounts were used to give rise to the anti-Pakistan narrative. Moreover, these accounts were used to propagate the incident of the alleged abduction of the Afghan ambassador’s daughter. Pakistan was targeted with hybrid



warfare and an entire network of information warfare was used against the country. Hashtags were trended to create negative impressions against Pakistan to portray it as an unsafe country. Some accounts were found operating from inside Pakistan, while the rest were operating from Afghanistan, India, and the west (Dawn, 2021).

The incident about the alleged abduction of the Afghan Ambassador's daughter in Islamabad was part of a conspiracy to damage Pakistan's image. The investigation revealed that it was "not a case of kidnapping." According to the reports, the conspiracy originated from Afghanistan and the India to distort the facts about the incident. According to Interior Minister Sheikh Rashid Ahmed, "There is a drastic difference between the complaint (of Silsila Alikhil, the daughter of Afghan Ambassador to Pakistan Najibullah Alikhil) and the investigation, which proved that no person sat in her taxi, and it is not a case of kidnapping in the light of our probe" (The Nation, 2021).

### **Anti-Pakistan Trends Over Social Media**

Operating anti-state trends through social media has emerged as a means to create hype. Numerous rival nations have established a huge network of websites that is spreading fake news-based trends against Pakistan. Unfortunately, some groups in Pakistan are playing at hands of hostile countries and most of the time they have been found spreading fake-news-based trends initiated by India and Afghanistan.

In 2021, some of the most circulating trends over social media were #State KilledKarimaBaloch; and #RapistArmyBalochistan. Furthermore, India media on aired videos propagating those women were unsafe in Pakistan. Besides, on 14<sup>th</sup> August 2020, around 150,000 anti-state trends against Pakistan were tweeted from India on #Balochistansolidarityday - the target of some 145,000 tweets was from Pakistan. India's National Investigation Agency (NIA) supports these trends. Trends that remain faster and remain on the trend panel for long period have a larger number of Tweets originating from India. Since 7<sup>th</sup> August 2021, there was a concentrated effort underway to trend #Sanction Pakistan by Afghan accounts. Accounts from Afghanistan have been found using #Sanction Pakistan that was part of their propaganda campaigns. On 8<sup>th</sup> August, the Afghan accounts managed to trend it in Afghanistan. On 9<sup>th</sup> August, Indian accounts became part of this campaign and started publishing articles on their content farm portals that were used to trend hostile hashtags against Pakistan (Ministry of Information and Broadcasting, 2021).

### **Indian Propaganda Campaigns and Balochistan Province**



India has been meddling in Balochistan for a long. In many cases, the Indian national media has been found spreading fake news and misleading reports against the province. India is using media as an instrument of warfare against Pakistan including electronic, print, and social media (Nadeem, Mustafa, Kakar, & Kakar, 2021).

The Indian media is pursuing the political objectives of its government which aim to damage national unity of Pakistan, spreading fake and misleading reports about Balochistan province. It is spreading fake reports about alleged “deep-rooted and festering political, economic and human rights problems of Balochistan”, highlights militant attacks and bomb blasts in the province, and runs articles that try to shed light on Pakistan's so-called Balochistan problem (Khan, 2012).

### **Indian Chronicles: India`s Disinformation Campaign against Pakistan**

Hybrid warfare against Pakistan to malign, destabilize, and damage its image in the global community by spreading false and fake news. In 2005, the Indian Intelligence agency established a fake front entity, the Srivastava Group (SG), with headquarters in New Delhi. This group has been managing the network of propaganda for the last fifteen years. The main purpose of the group is to use fake reports and spread false news about Pakistan, which was highlighted by ANI, a leading news agency in India.

In 2019, a 15-years disinformation network of India was exposed which is operating hundreds of fake news outlets aiming at influencing the European Union and United Nations with anti-Pakistan content. The network was behind a disinformation campaign against Pakistan, coordinating and demonstrating social media campaigns every year during UN Human Rights Council Sessions. On September 10, 2019, the “Pakistan Stop Genocide” campaign was organized in front of the United Nations during the 42<sup>nd</sup> session of the UN Human Rights Council. Moreover, the network also comprised fake NGOs to propagate misleading reports. The report by EU DisinfoLab says: “We have uncovered an entire network of coordinated UN-accredited NGOs promoting Indian interests and criticizing Pakistan repeatedly. We could tie at least 10 of them directly to [the] SG family with several other dubious NGOs pushing the same messages” (Machado, Alaphilippe, & Adamczyk, 2020).

### **Way Forward and Recommendations**

Hybrid threats are likely to grow in complexity, intensity, and scope in the future. Disinformation, cyber-attacks, subversion, and other hybrid challenges will be exacerbated by rapid technological advancement and growing global connectivity. The global system is shifting from unipolarity to multipolarity which is likely to give rise to sub-conventional



warfare, by proxies and hybrid conflicts; subjection of Pakistan to these threats will also increase in the future (Nisar, 2018).

Hostile countries have waged hybrid warfare against Pakistan, and the country is facing multiple threats. Since Pakistan is a nuclear power, conventional warfare against the country is unlikely. The adversaries will continue to impose indirect warfare to damage the peace and stability of the country.

At present, the media is being used as an instrument of warfare against Pakistan by hostile countries, particularly India, which is running media campaigns complementing the agenda of the Modi-led BJP, whose beliefs in warmongering as a political dividend strategy for political gains are of grave concern. The role of the Indian media is based on biased content against Pakistan, particularly against the Muslim identity. Such strategies need to be shifted to ensure sustainable peace and stability in the region. In this context, the role of the international community is crucial. It should play a role in promoting peaceful journalism and must develop a collective code of journalism.

India has continued to promote negative perceptions about Pakistan using a well-organized and effective way to portray it as an epicenter of terrorism with an extremist society. As part of hybrid warfare strategies, the Indian national media, information, and IT experts are making inroads into global media houses. Taking advantage of its progress in the field of information technology, the Indian domestic film industry, and significant international outreach, it is actively propagating anti-Pakistan content.

Disinformation campaigns could harm the country's national unity. Steps should be taken to counter internal and external threats and counter foreign propaganda. The support of the people of the country is crucial for success against the hostile elements. We, as a nation, have to fight this war. An effective national security strategy in collaboration with both civilian and military leadership is vital to deter this warfare.

Unidentified users on social media applications are spreading misleading posts, influencing the mindsets of people. Steps should be taken to prevent such users with an effective social media strategy.

Political parties play a crucial role in shaping public opinion. Political parties in Pakistan should play a role in promoting national unity and countering the anti-state narrative.

We are confronted with the war of fake narratives. A firm unity between the nation and state narrative is required to counter this war.

---



## **Conclusion**

Over the past two decades, the international security environment changed radically. While the probability of conventional conflict still exists, but the hybrid war has become the primary means of destroying a rival state. Hybrid warfare tactics are not a new phenomenon, but it has become more and more frequent and a preferred strategy of warfare in the modern world. In a digital and social media oriented society, fake news and disinformation have become a dangerous weapon. On one hand, media plays significant role in promoting awareness and social and economic progress. However, on the other hand, it has diversified the threat domain from conventional to hybrid, creating challenges to the twenty-century security environment.

The nuclear and conventional capabilities of Pakistan have deterred any kind of military attack against it. Hence, it has been the target of hybrid war for the last two decades. Hostile countries are using the media as a weapon against Pakistan. Through the media, they are propagating anti-Pakistan content intending to damage the morale of its army and security agencies, creating resentments among the Pakistani population, creating hatred in Pakistani society, portraying Pakistan as an unsafe country, creating sectarian and ethnic violence, and ultimately achieving their nefarious designs of pushing the country towards anarchy and chaos.

The hostile elements have joined hands to push the country towards violence and chaos. Most of the time, India has been found operating from fake social media accounts against Pakistan to spread hatred in Pakistani society and incite people against the state institutions and security agencies. Media war has become a preferred strategy for the adversaries particularly Indian have been using it as the instrument of warfare against Pakistan. A 15-year Indian global disinformation network against Pakistan was exposed in 2019 that was using media to distort realities and propagate negative perceptions against the country. Media warfare has socio-political implications for Pakistan. The entire land has been deemed the battlefield due to its broader spectrum of propaganda and uncertainty. This warfare targets Pakistan's territorial integrity, cultural identity, ideological and ethnic cohesion, and economy.



## References

- BBC. (2018, December 17). Russia 'meddled in all big social media' around US election. Retrieved from <https://www.bbc.com/news/technology-46590890>
- Berzins, J. (2014). Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy. *Centre for Security and Strategic Research*.
- Brown, J. (2018). An Alternative War: The Development, Impact, and Legality of Hybrid Warfare Conducted by the Nation State. *Journal of Global Faultlines*, 5(1), 58-82.
- Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of*. Harvard University Press.
- Centner, C. (2019). Russia's hybrid warfare. *The Washington Post*.
- Cullen, E. R.-K. (2016). What is Hybrid Warfare? *Norwegian Institute of International Affairs*, 4.
- Danyk, Y., Maliarchuk, T., & Briggs, C. (2017). Hybrid War: High-tech, Information and Cyber. *Connections The Quarterly Journal*, 16(2).
- Dawn. (2021, June 29). India behind anti-Pakistan propaganda on social media, minister tells NA. Retrieved from <https://www.dawn.com/news/1632082>
- Dawn. (2021, July 19). 'Pakistan being targeted through hybrid warfare,' NSA Yusuf says in briefing on Afghan 'abduction' incident. Retrieved from <https://www.dawn.com/news/1636032>
- Faber & Faber. (1927). The Indirect Approach. In B. L. Hart, *The Strategy of Indirect Approach*. London.
- Geo News. (2018, November 11). FO denies social media reports of Asia Bibi leaving Pakistan. Retrieved from <https://www.geo.tv/latest/218139-fo-denies-social-media-reports-of-asia-bibi-leaving-pakistan>
- Hoffman, F. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies.



- Hoffman, F. (2009). Hybrid Warfare and Challenges. *JFQ*, 1(52).
- Kaldor, M. (2013). *New and old wars: Organised violence in a global era*. John Wiley & Sons.
- Kelshall, C. (2019). Violent Transnational Social Movements and their Impact on Contemporary Social Conflict. *The Journal of Intelligence, Conflict, and Warfare*, 1(3).
- Khan, K. (2012, December). Understanding information warfare and its relevance to Pakistan. *Strategic Studies*, 32, 138-159. Retrieved from <https://www.thenews.com.pk/print/758438-how-india-destablises-balochistan>
- Machado, G., Alaphilippe, A., & Adamczyk, R. (2020). *Indian Chronicles: deep dive into a 15-year operation targeting the EU and UN to serve Indian interests*. Retrieved from <https://www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15-year-operation-targeting-the-eu-and-un-to-serve-indian-interests/>
- Marovic, J. (2019, November 28). Wars of Ideas: Hybrid Warfare, Political Interference, and Disinformation. *New Perspectives on Shared Security: NATO's Next 70 Years*.
- McCombie, S., Uhlmann, A., & Morrison, S. (2020, October 13). The US 2016 presidential election & Russia's troll. *Intelligence and National Security*, 35(1), 95-114. Retrieved from <https://doi.org/10.1080/02684527.2019.1673940>
- Mecklin, J. (2017). Introduction: The evolving threat of hybrid war. *Bulletin of the Atomic Scientists*, 73(5).
- Ministry of Information and Broadcasting. (2021). Ministry of Information and Broadcasting Government of Pakistan. Retrieved from <https://dmw.gov.pk/storage/report/DETAILED%20ANALYTICS%20REPORT%20-%20Anti%20Pakistan%20Trends%20PTM,%20Indian,%20Political%20Parties%20and%20Fake%20News%20Nexus%20June%202019%20-%20August%202021.pdf>
- Mitrovic, M. (2018, September 10). The Genesis of Propaganda as a Strategic Means of Hybrid Warfare Concept. *Vojno Delo*, 7(1). Strategic Research Institute.
- Munkler, H. (2005). *The New Wars*. Cambridge University Press.



- Nadeem, M. A., Mustafa, G., Kakar, S. A., & Kakar, A. (2021, April). Balochistan and Fifth Generation Warfare: Role of External Powers. *JRSP*, 58(2), 140-146.
- Nisar, M. (2018). 5 GW AND HYBRID WARFARE ITS IMPLICATIONS. Retrieved from <https://bdex.eb.mil.br/jspui/bitstream/123456789/2827/1/MO%200023%20-%20MAAZ.pdf>
- Prier, J. (2017). Commanding the Trend: Social Media as Information Warfare. *Strategic Studies Quarterly*, 11(4).
- Rosenberger, L. (2020, June). Making Cyberspace Safe for Democracy: The New Landscape of Information Competition,. Foreign Affairs. Retrieved from <https://www.foreignaffairs.com/>.
- Simons, G. (2010). *Mass Media and Modern Warfare: Reporting on the Russian War on Terrorism*. London: Routledge.
- Singer, P. W., & Brooking, E. T. (2018). *The Weaponization of Social Media*. Houghton Mifflin Harcourt.
- Svetoka, S. (2016). *SOCIAL MEDIA AS A TOOL OF HYBRID WARFARE*. NATO Strategic Communications Centre of Excellence.
- Tahir, I. A., & Afridi, M. K. (2019). Fifth Generations Warfare (5GW)-The New Dimensions of Enemies Launched Warfare and Security Concern of Pakistan. *Global Regional Review (GRR)*, IV(1).
- The Nation. (2021, July 21). Afghan Ambassador's daughter was not abducted: Sh Rashid. Retrieved from <https://nation.com.pk/21-Jul-2021/afghan-ambassador-s-daughter-was-not-abducted-sh-rashid>
- Tsu, S. (2016). *The Art of War*. Cosimo Classics.
- Weissmann, M., Nilsson, N., & Thunholm, P. (2021). *Security and Asymmetric Conflict in International Relations*. Bloomsbury Publishing.