Tracing the Genesis of Hybrid Warfare

Areesha Anwer[1]

Abstract

The literature on hybrid warfare is relatively new as the term was only coined in 2006 and the subject remains open for new findings and research. The combination of tactics used in hybrid warfare differentiates it from the conventional form of warfare and is now being adopted by states as a war-fighting strategy. However, the genesis of methods used in hybrid warfare can be traced back to the historical period. This study examines hybrid warfare by examining its concepts, mechanisms and instruments. It attempts to define hybrid warfare by drawing parallels between historical strategies and contemporary warfare, shedding light on the evolution of hybrid warfare starting from 300 BCE. It identifies IFIs, MNCs, cyberattacks and financial assistance as some of the pivotal instruments of hybrid warfare. The paper also explains the strategies of hybrid warfare being used by India against Pakistan.

Keywords: Hybrid Warfare, Genesis, Cyberattacks, Pakistan, India.

Introduction

Wars have transformed in the twenty-first century as in most cases war horns are no longer blowing. Rather, states are increasingly targeting their adversaries secretly. By the time a state is able to fully grasp its impact, it is already under the grip of undeclared hybrid warfare. The defense thus becomes challenging and the chances of escape become thin. This is the unforgivable nature of hybrid warfare where the aim is to damage and weaken a state from within and bring it to the brink of collapse.

The end of WWII marked the advent of a new era which was dominated by nuclear weapons and lethal technologies that resulted in the establishment of nuclear deterrence among the Nuclear-Weapon States (NWS). The specter of a nuclear holocaust or a full-scale conventional war fought with modern technological weapons led states to resort to unique contrivances, where the likelihood of large-scale nuclear or conventional wars was low. This shared concern gave rise to a new form of warfare in the international arena that uses strategies of both conventional and non-conventional means of war. Given

[1] Areesha Anwer is a Research Officer at the Center for International Strategic Studies Sindh, Karachi. She holds a Master's degree in International Relations from University of Karachi.

its Janus-faced characteristics, this unique type of warfare was named hybrid warfare. Bachmann and Jones find that hybrid warfare blurs the line between times of peace and war and attracts elements from existing categories of warfare including guerilla warfare, asymmetric warfare and compound warfare.[2]

Alongside kinetic means of warfare, non-kinetic means such as cyberattacks, disinformation and propaganda came into use by states under hybrid warfare. However, what remains integral to both hybrid and conventional forms of warfare is the pursuit of the ultimate goal which motivates actors to gain psychological and physical advantage over their opponents.[3] There is a lack of consensus concerning the definition of hybrid warfare due to the presence of mixed opinions on its complex nature and characteristics. Today, the strategies used in hybrid warfare fall somewhere between routine statecraft and open warfare. According to Christopher Paul, a senior social scientist at the RAND Corporation, "Hybrid warfare blurs the distinction between war and peace, and combatants and non-combatants."[4] Patrick Cullen, a senior research fellow at the Norwegian Institute of International Affairs, describes the baseline concept of hybrid warfare as "the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects."[5]

A hybrid warfare strategy is mainly focused on achieving political objectives through technological, cognitive, and information warfare. These objectives primarily rely on the use of propaganda or in other words *Psychological Warfare* that deals with perception management and exploitation of the thought process of the opponents. One of the glaring examples of hybrid warfare could be found in the Russia-Ukraine conflict of 2014.[6] The strategies used by Russia against Ukraine were that of hybrid warfare, comprising attacks on the military and political structure as well as in the cyber sphere.[7]

---

[2] Meredith Jones and Sascha Dov Bachmann, Syria – A Hybrid Warfare Case Study, Journal of Military and Strategic Studies, Volume 21 Issue 1.

[3] Bastian Giegerich, "Hybrid Warfare and the Changing Character of Conflict", *Connections: The Quarterly Journal*, (2016)

[4] Muhammad Nadeem Mirza, Summar Iqbal Babar, "The Indian Hybrid Warfare Strategy: Implications for Pakistan", *Progressive Research Journal of Arts and Humanities*, 2020

[5] Patrick J.Cullen, Erik Reichborn-Kjennerud, "Countering Hybrid Warfare", *MCDC Countering Hybrid Warfare Project*, (2019)

[6] Tidy, Joe, "Ukraine says it is fighting first 'hybrid war'", BBC, accessed on 11 August 2023, retrieved from https://www.bbc.com/news/technology-60622977

[7] "What is hybrid war, and is Russia waging it in Ukraine?", The Economist, accessed on 11 August 2023, retrieved from https://www.economist.com/the-economist-explains/2022/02/22/what-is-hybrid-war-and-is-russia-waging-it-in-ukraine

The ongoing conflict between Russia and Ukraine also involves the strategies of hybrid warfare. Patterns of hybrid warfare could also be found in the Syrian conflict that started in 2011. The involvement of several parties including the United States, Russia, Iran and non-state actors such as Hezbollah and Da'ish set the stage for proxy wars in Syria. The actors involved in the Syrian conflict operated across numerous military domains such as land, sea, air, and space as well as cyber and information domains.[8]

The paper seeks to explain what sets hybrid warfare apart from traditional warfare methods. And which tools and tactics, both historical and contemporary, are involved in hybrid warfare? This study employs a qualitative research methodology and offers a comprehensive approach to understanding the complexities and subtleties found within the topic under investigation. By applying qualitative methods such as interviews, observations, and primary and secondary document analysis, the research seeks to uncover underlying patterns, concepts, and interpretations providing valuable insights into the subject matter.

Understanding the Concept

Hybrid warfare constitutes strategies that create multiple battlefields across the targeted state, albeit the attacks are designed to remain below the threshold of a full-fledged war. Hence, it is also known as multi-level and multi-dimensional warfare. The most crucial intangible tools of hybrid warfare are ambiguity and plausible deniability. The aim is to cause serious damage to the opponent by attacking it both horizontally and vertically. The attacks are launched keeping in view the Military, Politics, Economy, Civilian and Informational (MPECI) spectrum.[9] The MPECI attacks are set off simultaneously across Political, Military, Economic, Social, Infrastructure and Information (PMESII)[10] vulnerabilities of targeted states and entities with a view to causing paralysis in dealing with the crises. Hence, this lethal form of warfare is tantamount to "death by a thousand cuts." What distinguishes this type of warfare from a traditional one is the incognizance of the enemy of the multiple and simultaneous strikes being launched against it. By the time the consequences manifest themselves, the targeted state and entities are irreversibly damaged.

---

[8] Jones, Meredith, and Sascha Dov Bachmann. "Syria–A Hybrid War Case Study." *Journal of Military and Strategic Studies* 21, no. 1 (2021): 33-55.

[9] Patrick J.Cullen, Erik Reichborn-Kjennerud, "Countering Hybrid Warfare", *MCDC Countering Hybrid Warfare Project,* (2019)

[10] Ibid.

A state not only uses its existing capabilities but also develops new capabilities tailored to the specific vulnerabilities of the enemy state. These capabilities are then used collectively against the rival state to achieve certain political aims and objectives. Such tactics are used by both state and non-state actors.

Historical Linkages of Hybrid Warfare

Hybrid warfare transpires in the vacuum between the layers of traditional ways of thinking.[11] Evidence shows that hybrid strategies of war existed centuries before the term hybrid warfare was coined in 2006 by Frank G. Hoffman. However, the industrialization of war that led to the rapid advancement in the traditional military weapons, overshadowed these strategies and their significance in gaining victory. It was only after massive changes in the global geopolitical domain that marked a renaissance for these age-old strategies combined with conventional means of warfare. The concept of hybrid warfare strategies can be found in the work of a 300 BCE Hindu statesman and philosopher Kautilya, and in Sun Tzu's *The Art of War* – a 5th century BCE military treatise. *The Art of War* accentuates the comprehension of the strengths and weaknesses of the enemy. Making use of one's capabilities and developing new ones pertinent to the enemy's frailty is impossible without adhering to Sun Tzu's words of wisdom.

An excerpt from Sun Tzu's *The Art of War*

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."[12]

Kautilya (Chanakya) back in 300 BCE wrote about non-traditional means of fighting a war. In his book *'Arthashastra,'* he classified wars into three types, namely *Open*, *Concealed*, and *Silent wars*. By 'Open war' Kautilya means the traditional wars fought at a designated time and place. By 'Concealed war' he means the use of guerilla stratagem, and finally by 'Silent war' he means spies and undercover operatives working to create an internal divide in the enemy state while the relations at the official level are established normally.[13] Silent

[11] Bastian Giegerich, "Hybrid Warfare and the Changing Character of Conflict", *Connections: The Quarterly Journal*, (2016)

[12] The Art of War, Sun Tzu.

[13] Muhammad Nadeem Mirza, Summar Iqbal Babar, "The Indian Hybrid Warfare Strategy: Implications for Pakistan", *Progressive Research Journal of Arts and Humanities*, 2020

war uses the tactics of stealth while repeatedly attacking the critical targets of the adversary, an ancient strategy yet similar to the methods of hybrid warfare.

Thomas Edward Lawrence also known as *Lawrence of Arabia* used non-conventional strategies to create the Arab-Ottoman divide. Edward Lawrence had command over the Arabic language and had an in-depth knowledge of both the Arabs and Ottomans. With his skills he was able to target the vulnerabilities of the Muslims of the Middle East, in particular the Arab-Ottoman divide, and mobilized the Arabs against the Ottomans.[14] This eventually led to the fall of the Ottoman Empire in the First World War.

Propaganda is a multifaceted concept and one of the most crucial weapons of hybrid warfare. In layman's terms, it means making the enemy think just the way you wish them to think. To quote Hitler, "The modern weapon of propaganda is for the masses."[15] The use of propaganda as an instrument of war remained part and parcel of Hitler's tactics during WWII. After assuming the position of Chancellor, Hitler established a Ministry of Propaganda and Public Enlightenment. The main objective of this body was to sell Nazi ideology by ensuring that the Nazi message was successfully communicated through art, books, films, radio, theatre, music, press, and educational materials.[16] His philosophy of propaganda justified using any means to achieve the desired end. He believed that "by propaganda with permanent and clever application, even heaven can be palmed off on a people as hell and the other way around, the most wretched life as paradise."[17]

Historical evidence of propaganda tactics employed in wars is not limited to Hitler. In his book *Mein Kampf*, Hitler reveals how he was inspired by the propaganda method used in wars by the Communists. Bolsheviks, when failed to achieve their objectives by military and economic means, used propaganda tactics to counter the Allied intervention during the civil war. The Soviet Union made propaganda an element of its domestic as well as foreign policy. *Agitprop* – a word coined by Lenin, translates as agitation and propaganda. Propaganda being the persuasion of the masses, and agitation being the aggressive form of persuasion.[18]

---

[14] Yassamin Mather, The Fall of the Ottoman Empire and Current Conflict in the Middle East, Journal of Socialist Theory, Volume 42, 2014 - Issue 3. https://www.tandfonline.com/doi/full/10.1080/03017605.2014.972151?needAccess=true

[15] Joseph S. Roucek (1942), Hitler's Propaganda as a War Weapon, *The Educational Forum*, (2008).

[16] Ibid.

[17] Ibid.

[18] Ibid.

The historical ways of fighting hybrid warfare, however, slightly differ from the modern methods of hybrid warfare. Hybrid warfare's novel aspect is the simultaneous use of multiple conventional and non-conventional instruments, launched against the targeted state while attempting to keep the existing deterrence undisturbed.

Instruments of Hybrid Warfare

i. Cyberattacks: Cyberattack is a novel facet of modern times, which subsumes under hybrid warfare. The cyber world is becoming one of the most crucial battlespaces where hybrid warfare is fought by states as well as non-state actors, acting either as victims or assailants in these burgeoning crimes. Identity Theft Resource Center stated that in 2021, the total number of data breaches was 1,291 as compared to 1,108 in 2020.[19] Global Threat Report 2022 reports an 82% increase in ransomware-related leaked data in 2021.[20] Amid the growing environment of uncertainty, this unprecedented threat has entangled the states in a security dilemma. States have been actively seeking to build counter capabilities against the rising threat of cyberattacks. NATO acknowledged cyberspace as the 5th battlespace at the 2016 Warsaw Summit and recognized cyberattacks as a potential Article 5 case of the Washington Treaty which set out that an attack on one state is an attack on all.[21]

The Identity Theft Resource Center (2023) tracked 2,116 data compromises in the first three-quarters of 2023.[22] Cyberattacks have both economic as well as political impacts. Estimates of the macroeconomic costs of cyberattacks are speculative. As long as any cyberattack has a limited scope and is short-lived, it is likely that macroeconomic consequences will be small.[23] Electronic Information Systems are an essential part of the modern economy. The failure of information circulation makes entire sectors of the economy vulnerable. Information security which is the safeguarding of computer systems and the

[19] Identity Theft Resource Center, 2021, https://www.idtheftcenter.org/post identity-theft-resource-center-to-share-latest-data-breach-analysis-with-u-s senate-commerce-committee-number-of-data-breaches-in-2021-surpasses-all-of-2020/#:~:text=However%2C%20the%20number%20of%20 data,to%21%2C108%20breaches%20in%202020).

[20] Crowdstrike, Global Threat Report 2022

[21] The unfolding Cyber war in Ukraine, Vision of Humanity, https://www.visionofhumanity.org/ukraine-cyberattacks-2022/

[22] Identity Theft Resource Center, 2023, https://www.idtheftcenter.org/post/q3-2023-data-breach-report-itrc-reports-data-compromise-record-with-three-months-left-in-year/

[23] The Economic Impact of Cyberattack, CRS Report of Congress, 2004, https://archive.nyu.edu/bitstream/2451/14999/2/Infosec_ISR_Congress.pdf

confidentiality, integrity, and availability of the data the systems contain, has long been recognized as a critical national security issue.[24]

Critical infrastructure is a prime target of cyberattacks. In May 2023, Western intelligence agencies and Microsoft accused China of spying on several telecommunications and transportation hubs in the US. In a counter statement, China claimed that the allegations were a "collective disinformation campaign" against China and that the US itself is "the empire of hacking."[25] In 2023, the personal information of 237,000 present and former federal government employees was exposed in a data breach at the US Transportation Department (USDOT). The 2022 distributed denial-of-service (DDoS) cyberattacks on fourteen US airport websites that disrupted their systems are claimed to have been carried out by a Russian-speaking hackers' group known as KillNet.[26] In 2019, a cyber-breach took place on Texas-based Solar Winds Inc., due to which affected companies based in the US reported an average of 14% impact on annual revenue, while the averages in the UK and Singapore stood at 8.6% and 9.1% respectively.[27] This is also called the spillover effect where a cyberattack targeted at one entity has a widespread impact on entities in other countries. The US claimed that the software used by Texas-based Solar Winds Inc. was breached and hijacked by Russia. These cyber incidents exposed the vulnerabilities of the civilian government networks of the US.

In 2023, hacktivists breached NATO's cybersecurity defenses by stealing 3,000 documents from the NATO database.[28] In May 2021, a cyberattack forced the US Company Colonial Pipeline to proactively close down operations and freeze IT systems which temporarily halted all pipeline operations.[29] In 2021, JBS Meat based in the US paid USD eleven million in ransom to call a halt to a major cyberattack. According to a report published by China's National Computer Virus Emergency Response Center in 2022, a top US spy agency stole Chinese user data and infiltrated the country's

[24] The Economic Impact of Cyberattack, CRS Report of Congress, 2004, https://archive.nyu.edu/bitstream/2451/14999/2/Infosec_ISR_Congress.pdf

[25] Reuters, 2023 https://www.reuters.com/technology/microsoft-says-china-backed-hacker-targeted-critical-us-infrastructure-2023-05-24/

[26] 'Russian-speaking hackers knock multiple US airport websites offline', CNN, Oct 10, 2022. https://edition.cnn.com/2022/10/10/us/airport-websites-russia-hackers/index.html

[27] Cybersecurity Study, Tech Republic, June 28 2021, https://www.techrepublic.com/article/cybersecurity-study-solarwinds-attack-cost-affected-companies-an-average-of-12-million/

[28] Significant Cyber Incidents, Strategic Technologies Program, Center for Strategic and International Studies, 2023.

[29] The New York Times, 2021 https://www.nytimes.com/2021/05/08/us/politics cyberattack-colonial-pipeline.html

telecommunications infrastructure.[30] The report also claims that the National Security Agency (NSA) of the US Department of Defense carried out a cyberattack known as man-in-the-middle attack on the Northwestern Polytechnical University, where digital communication between two parties was hacked. A DDoS cyberattack was carried out in 2022 on the Finnish Parliament that blocked access to the Parliamentary website. On 20 June 2019, the US Cyber Command conducted online attacks against an Iranian intelligence group that American officials believe helped plan the attacks against Japanese-owned oil tankers on 13 June 2019.[31]

The threat of cyberattacks on nuclear sites places the issue of global strategic stability in a completely new light. In 2010, Israel targeted the Iranian nuclear site 'Natanz Facility' through a virus named *Stuxnet* that hacked the spin of its cylinders.[32] Importantly, a cyberattack on a nuclear site can lead to catastrophic results. Due to these developments in cyberspace, numerous states have enhanced their cyber resilience capabilities. In 2018, the US expanded the role of nuclear weapons by declaring that it would consider nuclear retaliation in the case of "significant non-nuclear strategic attacks."[33] In 2021, President Biden issued a National Security Memorandum on "Improving Cybersecurity for Critical Infrastructure Control Systems."[34] On 16 June 2021, President Biden gave a list to Russian President Vladimir Putin consisting of sixteen critical infrastructure sectors such as energy, financial services, IT, healthcare, nuclear reactors, materials and waste sector that should be off-limits to cyber or attack by any other means.[35] On 19 January 2022, he signed another National Security Memorandum to improve the cybersecurity of National Security, Department of Defense and

[30] CNBC, 2022, https://www.cnbc.com/2022/09/27/china-alleges-us-nsa-hacked-infrastructure-sent-data-back-to-hq.html

[31] US Carried out Cyberattacks on Iran, The New York Times, https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html

[32] TRT World, 2021 https://www.trtworld.com/magazine/here-s-how-israel-hacked-iran-s-nuclear-facility-45838

[33] Scott Sagan and Allan Weiner, "The U.S. says it can answer cyberattacks with nuclear weapons. That's lunacy.", The Washington Post, 2021 https://www.washingtonpost.com/outlook/2021/07/09/cyberattack-ransomware-nuclear-war/

[34] The White House, 28 July 2021, https://www.whitehouse.gov/briefing-roomstatements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

[35] Biden gave Putin list of 16 critical infrastructure entities 'Off-Limits' to cyberattacks, Fox Business, 16 June 2021, https://www.foxbusiness.com/politics/biden-putin-critical-infrastructure-entities-off-limits-cyberattack

Intelligence Community Systems.[36] The 2016 Information Security Doctrine of Russia broadly defines Russia's threat perceptions regarding its national security and security in the information sphere. It also discusses the need to secure its systems from cyber espionage and cybercrimes. The Cyberspace Administration of China, in conjunction with twelve other government departments, issued New Measures for Cybersecurity Review on 4 January 2022.[37] In 2021, Pakistan launched its "National Cyber Security Policy 2021," which provides for retaliatory measures against aggression on the critical infrastructure of the country.[38]

ii. Financial Assistance: Financial approach is gaining ascendance over the military approach[39] and geo-economics is seen as the sub-variant of geopolitics.[40] Economy has become the new battlefield. In *War by Other Means*, Robert Blackwill and Jennifer Harris argue that aid as an instrument of geo-economics has been around as long as diplomacy itself. According to Blackwill and Harris, aid deployed in the shape of military aid, bilateral development assistance, or humanitarian assistance has always been used to buy strategic influence.[41] However, in modern times economic subversion is also acquired through economic instruments such as investment policy, trade policy, aid, financial and monetary policy, as well as economic and financial sanctions.

Economic subversion remains the most brutal hit on an already vulnerable economy. Hence the erosion of the economic strength of a country is perhaps the most important element, probably the hardest to reverse once it is accomplished.[42] Monetary and fiscal policies proposed by International Financial Institutions (IFIs) often lead to large economic imbalances. Such a

[36] The White House, 19 January 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

[37] China issued new measures for cybersecurity review in 2022, White & Case,8 February 2022, https://www.whitecase.com/insight-alert/china-issued-new-measures-cybersecurity-review-2022

[38] National Cyber Security Policy 2021, Ministry of Information Technology and Telecommunication, 2021. https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20 Security%20Policy%202021%20Final.pdf

[39] Edward N. Luttwak, From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce, *The National Interest*, 1990.

[40] Mikael Wigell, Antto Vihma, Geopolitics versus Geo-economics: the case of Russia's geo-strategy and its effects on the EU, *International Affairs*, 2016

[41] Robert Blackwill and Jennifer Harris, *War by Other Means*, 2016

[42] Dr Ashfaque Hasan Khan, Seminar on *Regional Environment and Imperatives of Security*, NUST Institute of Policy Studies (NIPS), 6 June 2022.

situation also occurs due to the austerity packages attached to bailout funds that overlook the recipient country's unique economic status and cultural background and follow a one-size-fits-all approach.[43]

iii. MNCs and International Financial Institutions (The Debt Trap): International Financial Institutions **(**IFIs) grant massive loans to economically fragile states and entangle them in an unending vicious cycle of aid. This incapacitates a country's ability to protect its national security. The structural adjustment programs of IFIs which at face value are meant to economically develop a state, have proven to be crucially harmful to those same countries.[44]

The European Network on Debt and Development known as 'Eurodad,' released a report in 2008 titled "Critical Conditions: The IMF Maintains its Grip on Low-Income Governments.*"* The report finds that "since the Conditionality Guidelines were approved, the IMF has not managed to decrease the number of structural conditions attached to their development lending. Moreover, the Fund continues to make heavy use of highly sensitive conditions, such as privatization and liberalization. Eurodad's analysis finds that a quarter of all the conditions in Fund loans approved after 2002 still contain privatization or liberalization reforms."[45]

In 2019, the International Policy Centre for Inclusive Growth released IMF policy prescriptions and conditionalities titled "Is the Washington Consensus Dead?" It states, "The simple truth is that conditionalities are paternalistic. They are meant to alter behavior and induce changes in economic, political, and social structures. They also serve as a sort of collateral; in some cases, they are a form of coercion to ensure adoption of otherwise unpalatable reforms."[46]

Moreover, there have been several cases in history where Multinational Corporations (MNCs) have pursued assertive measures against some states leading to regime change. In his book "The New Confessions of an Economic Hitman" (2016), John Perkins argues that international corporations and banks have coerced poor countries into receiving massive development loans so that they were endlessly indebted to these organizations.[47] To prove his

---

[43] Tarek Radwan (Ed.), "The Impact and Influence of International Financial Institutions on the Middle East and North Africa", Friedrich Ebert Stiftung, 2020.

[44] Ibid.

[45] Nuria Molina and Javier Pereira, "Critical Conditions: The IMF maintains its grip on low-income governments", *Eurodad*,2008.

[46] Degol Hailu, "Is the Washington Consensus Dead?", *International Policy Centre for Inclusive Growth*, 2009.

[47] John Perkins, *The New Confessions of an Economic Hitman*, (London: Penguin Randomhouse UK, 2016)

argument, Perkins cites several examples where economically debilitated countries were encouraged through a carrot-and-stick approach to accepting massive development loans. For example, the 1951 regime change that took place in Iran was a result of a rebellion that transpired under Mossadegh's rule, against a British Oil Company that was exploiting Iranian petroleum resources and responded with threats and sanctions on Iran in response to Mosaddegh's decision to nationalize the Iranian petroleum assets. Fearing a military response, England sought help from the US. Washington, instead of dispatching Marines, sent CIA Agent Kermit Roosevelt, grandson of former US President Theodore Roosevelt. Kermit enlisted local people to organize a string of riots and demonstrations in Iran. He also used payoffs and threats to create an unpopular and inept impression of Mossadegh amongst the masses.[48]

In 1954, regime change took place in Guatemala. United Fruit Company, an American MNC owned by Zapata Oil – George Bush's company – launched a major public relations campaign in the US. The campaign was directed at convincing Congress and the American public that Jacobo Arbenz, who was a democratically elected President of Guatemala, was in fact part of a Soviet plot and that Guatemala was a satellite state of the Soviet Union. Arbenz was a man of the poor, who promised to pull them out of starvation, and for that, he implemented a comprehensive land reforms project. The CIA organized a coup in 1954, the US bombed Guatemala and Arbenz was overthrown.[49] The strategy adopted by huge corporations and IFIs is very similar to the strategies used today in hybrid warfare, aimed at weakening a state internally. These organizations use propaganda, civil unrest, operatives, as well as hard power to accomplish their ultimate goals.

Indian Hybrid Warfare Strategies against Pakistan

Due to its strategic location, Pakistan has faced many serious challenges as well as benefitted from opportunities. Its location at the crossroads of South Asia, Central Asia and West Asia has always attracted the attention of global powers. The absence of cordial relations between Pakistan and India also poses additional security challenges to Pakistan including in the realm of hybrid warfare.

The 2018 'Land Warfare Doctrine' of India states that India would adopt hybrid tactics to damage its adversaries. The Doctrine mentions addressing hybrid threats with enhanced capabilities for complete retaliation.

[48] Ibid.
[49] Ibid.

Furthermore, it draws attention towards the use of 'information tools' in hybrid warfare, while aiming to achieve "full-spectrum Information dominance over the adversary."[50] To counter cyber threats, the Indian Land Warfare Doctrine asserts the importance of cybersecurity and states that the existing cyber warfare capabilities will be upgraded to develop cyber deterrence.[51] The use of 'deception' as a tool of hybrid warfare has also been alluded to in the Doctrine. The Doctrine mentions the use of 'Psychological Warfare' which also includes social media platforms for perception management.[52]

The Doval Doctrine of '*Defensive Offence'* was proposed by India's incumbent National Security Advisor Ajit Doval in 2014. Doval was of the view that a defensive offence could work best to defend India. He stressed that through defensive offense India would work on the vulnerabilities of the enemy. This is evident in India's foreign policy towards Pakistan as India has attempted but failed to diplomatically isolate Pakistan. It blames Pakistan for terrorism in India and meddles in Pakistan's internal politics among other tactics. The two axioms of the Doval Doctrine are: (i) Accept reality as it is and not as you wish it was; and (ii) You can never defeat an enemy that you cannot define.[53] Importantly, his Doctrine points out that all wars cannot be won through the might of the armed forces and defines terrorism as a tactic to achieve political and ideological objectives. The Doctrine also mentions that India should work on the vulnerabilities of the enemy.[54] Doval Doctrine also notes that the defensive offense mode will benefit India much more than the defensive mode in which India can end up in a stalemate with its enemy.

India used Afghan soil against Pakistan during the presence of foreign forces for two decades and invested about USD three billion in Afghan infrastructure, training of Afghan forces and establishing a network for its lasting foothold to accomplish its overt and covert plans.[55] India provided support and training to Dai'sh and TTP elements to use them as proxy tools against Pakistan and in the region.[56] In 2016, the Indian spy network was

---

50 Land Warfare Doctrine, 2018

51 Ibid.

52 Ibid.

53 Understanding the Doval Doctrine, Op India, 10 October 2016, https://www.opindia.com/2016/10/understanding-the-doval-doctrine-of-defensive-offence/

54 Understanding the Doval Doctrine, Op India, 10 October 2016, https://www.opindia.com/2016/10/understanding-the-doval-doctrine-of-defensive-offence/

55 Mir Sherbaz Khetran,"Indian Interference in Balochistan: Analysing the Evidence and Implications for Pakistan" *Strategic Studies*, 2017.

56 Ibid.

exposed in Pakistan, as a result, eight members of the Indian High Commission in Islamabad were expelled.[57] The Foreign Office of Pakistan stated that the members of the Indian High Commission were working undercover for their intelligence bureau, had contacts with TTP, and were involved in suspicious activities such as creating social unrest inside Pakistan.[58] India has also used a variety of pressure tactics against Pakistan. One example is the false flag operation in Pulwama in 2019 where India held Pakistan responsible for the killing of 40 CRPF personnel in an attack on an Indian convoy.

Evidence suggests that India orchestrated attacks like the Lahore blast (2001)[59] and the Dasu Bus Incident (2001) to disparage Pakistan's security environment. In addition, India was involved in attacks, including suicide bombing at the Confucius Institute of University of Karachi (2022) targeting Chinese workers in Pakistan in an attempt to undermine the Pakistan-China strategic partnership and China Pakistan Economic Corridor (CPEC). The arrest of the serving Indian Navy Officer Commander Kulbushan Yadhav in Pakistan in 2016 and investigation into his case revealed that his purpose was to destabilize Pakistan by supporting a separatist movement in Balochistan.[60] Kulbushan Yadhav has confessed to a series of terrorist activities planned and controlled by Indian operatives in Afghanistan.

EU Disinfo Lab report (2020) named 'Indian Chronicles' exposed India's massive disinformation campaign against Pakistan. Active Indian networks in Brussels and Geneva produced content to primarily target Pakistan.[61] According to the report, "Since 2005, for the following 15 years; India managed more than 750 fake media outlets in 116 countries and directly controlled 10+ NGOs accredited to the UN Human Rights Council."[62] In addition, India resurrected dead people's social media accounts and created fake media websites to propagate disinformation against Pakistan.[63] Moreover, 550 plus website

[57] Ibid.

[58] FO reveals details of eight Indian 'undercover agents', 3 Nov 2016, Dawn, https://www.dawn.com/news/1294023

[59] VoA, Pakistan Alleges India Plotted Recent Bombing; No Comment From Delhi, 4 June 2021, https://www.voanews.com/a/south-central-asia_pakistan-alleges-india-plotted-recent-bombing-no-comment-delhi/6207833.html

[60] Mir Sherbaz Khetran,"Indian Interference in Balochistan: Analysing the Evidence and Implications for Pakistan" *Strategic Studies*, 2017.

[61] EU Disinfo Lab, Dec 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/

[62] Ibid.

[63] Ibid.

domain names were registered by Indian malicious actors.[64] Pakistan also became the target of Indian cyberattacks. The *Pegasus Software* – a creation of the Israeli company *NSO group* – was used by India in an attempt to spy on Pakistan. The spyware, as claimed by the Amnesty group, was used to penetrate the mobile phones of journalists, politicians, leadership and political opponents of several states including Pakistan. In 2017, Pakistan's Senate Committee on Foreign Affairs warned the government that Pakistan was a prime target of cyber espionage – monitored extensively by foreign spies. In a statement given by ISPR in 2020, Indian intelligence agencies were stated to have targeted the cell phones and gadgets of military personnel and government officials.[65]

Conclusion

The emerging trends in modern warfare have pushed states towards defending their frontiers in every spectrum. The seriousness of the threat posed by hybrid warfare has pushed states to bolster their susceptibilities before irreversible damage is done. However, such type of warfare requires an early warning defense mechanism and a multi-pronged approach as a countermeasure. Defense against hybrid warfare includes measures for detecting, deterring, countering, and responding to hybrid threats meticulously.[66] The proposed solutions should adequately address the challenges posed by hybrid warfare where information, cognitive, and social domains play crucial roles. A holistic defense approach that embraces technological advancements, strategic partnerships, and proactive intelligence efforts is essential to safeguarding nations against the complexities of hybrid threats in the contemporary security landscape.

Additionally, fostering international cooperation and strengthening digital defenses will be pivotal in navigating the evolving landscape of hybrid warfare.[67] However, the role of strategic deterrence, both conventional and unconventional, should not be underestimated. Developing a versatile defense posture that combines traditional military strength with adaptive strategies for countering disinformation, cyberattacks, and social manipulation is essential.

---

[64] Ibid.

[65] Dawn, August 12, 2020, https://www.dawn.com/news/1574034

[66] Arslan Bilal, Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote, NATO Review, 2021 https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

[67] Yuriy Danyl et al., Hybrid War: High-tech, Information and Cyber Conflicts, Connections: The Quarterly Journal, 2017, https://www.jstor.org/stable/26326478?searchText=&searchUri=&ab_segments=&searchKey=&refreqid=fastly-default%3A26ff86a4e2746dfc8f26b57702131fba&seq=1

Importantly, smaller states should defend themselves against the strategies used by huge corporations and IFIs, which often resemble those employed in hybrid warfare. Governments, military forces, and intelligence agencies must remain vigilant, agile, and collaborative to effectively address the multifaceted challenges posed by hybrid threats. To fortify national strength, resilience and security, it is imperative to integrate measures that prioritize information warfare resilience, cognitive defense capabilities, and robust social resilience.